



SENSING THE SURVEILLANCE STATE

ARGENTINA'S EXPANDING POLICIES AND TECHNOLOGIES OF MASS
SURVEILLANCE

AMNESTY
INTERNATIONAL



Amnesty International is a movement of 10 million people which mobilizes the humanity in everyone and campaigns for change so we can all enjoy our human rights. Our vision is of a world where those in power keep their promises, respect international law and are held to account. We are independent of any government, political ideology, economic interest or religion and are funded mainly by our membership and individual donations. We believe that acting in solidarity and compassion with people everywhere can change our societies for the better.

Acknowledgement

Amnesty international is grateful to the partners including civil society organizations and activists who contributed to this research.

© Amnesty International 2026

Except where otherwise noted, content in this document is licensed under a Creative Commons (attribution, non-commercial, no derivatives, international 4.0) licence.

<https://creativecommons.org/licenses/by-nc-nd/4.0/legalcode>

For more information please visit the permissions page on our website: www.amnesty.org

Where material is attributed to a copyright owner other than Amnesty International this material is not subject to the Creative Commons licence.

First published in 2026

by Amnesty International Ltd

Peter Benenson House, 1 Easton Street

London WC1X 0DW, UK

Index: AMR 13/1104/2026

Original language: English

amnesty.org



Cover illustration: Amnesty International / Celina Hilbert

AMNESTY
INTERNATIONAL



CONTENTS

1. EXECUTIVE SUMMARY	10
CONTEXT: POLICIES TO CURTAIL AND REPRESS PROTEST	10
STRUCTURAL AND OPERATIONAL REFORMS	10
PROCUREMENT OF SURVEILLANCE TECHNOLOGIES	11
THE CHILLING EFFECT OF SURVEILLANCE	11
CLEARVIEW AI'S CORPORATE RESPONSIBILITIES	12
2. METHODOLOGY	14
2.1 CONTEXT, METHOD, AND SCOPE OF THIS STUDY	14
2.2 HISTORY OF SURVEILLANCE IN ARGENTINA AND IN THE REGION	17
2.3 MASS SURVEILLANCE WITH NO OVERSIGHT: FACIAL RECOGNITION OF FUGITIVES IN THE CITY OF BUENOS AIRES	18
2.4 REGIONAL EXPERIENCES: LATIN AMERICA AND THE SPREAD OF MASS SURVEILLANCE	19
3. LEGAL STANDARDS APPLICABLE TO THE USE OF SURVEILLANCE TECHNOLOGIES IN ARGENTINA	21
3.1 RIGHT TO PRIVACY AND PROTECTION OF PERSONAL DATA	22
3.2 FREEDOM OF EXPRESSION	22
3.3 FREEDOM OF PEACEFUL ASSEMBLY AND ASSOCIATION	23
3.4 RIGHT TO EQUALITY AND NON-DISCRIMINATION	23
3.5 TRANSPARENCY AND ACCESS TO PUBLIC INFORMATION	25
3.6 NON-BINDING INTERNATIONAL STANDARDS AND RECENT DEVELOPMENTS	25
4. HUMAN RIGHTS IMPACTS OF SURVEILLANCE TECHNOLOGIES	26
4.1 IMAGE RECOGNITION AND BIOMETRICS	26
4.2 CRIME PREDICTION AND DETERMINATION OF SURVEILLANCE AREAS	28
4.3 SOCIAL MEDIA REVIEW AND OPEN SOURCE INTELLIGENCE (OSINT)	29
5. SURVEILLANCE POLICIES AND TECHNOLOGIES: A NEW PARADIGM	30
5.1 EXPANDING THE SCOPE OF THE INTELLIGENCE SYSTEM AND FEDERAL LAW ENFORCEMENT	30
5.1.1 REFORM OF THE NATIONAL INTELLIGENCE SYSTEM	30

5.1.2 REFORM OF THE FEDERAL POLICE STATUTE	31
5.2 OPERATIONAL ELEMENTS FOR IMPLEMENTING DOMESTIC SURVEILLANCE	32
5.2.1 “ANTI-PICKET” PROTOCOL	32
5.2.2 ARTIFICIAL INTELLIGENCE UNIT FOR SECURITY (UIAAS)	32
5.2.3 “CYBER PATROLLING” PROTOCOL	33
5.2.4 <i>EX-POST</i> FACIAL RECOGNITION: PROTOCOL FOR FACIAL RECOGNITION AND COMPARISON	34
6. ANALYSIS OF PROCUREMENTS AND COMMISSIONING OF SURVEILLANCE TECHNOLOGIES	35
6.1 TECHNOLOGIES PROCURED BY THE NATIONAL GOVERNMENT	36
6.1.1 SOCIAL MEDIA AND OPEN-SOURCE SURVEILLANCE	36
6.1.2 IMAGE PROCESSING WITH FACIAL RECOGNITION TECHNOLOGY	37
6.1.3 DRONES, ROBOTS AND AERIAL SURVEILLANCE	39
6.1.4 PREDICTIVE ALGORITHMS: TOOLS FOR REINFORCING STEREOTYPES	40
6.2 SURVEILLANCE TECHNOLOGIES PROCURED BY THE CITY OF BUENOS AIRES: INCREASED VIDEO SURVEILLANCE CAPABILITIES AND NEW FACIAL RECOGNITION TECHNOLOGY	41
6.2.1 WHAT DOES THIS LOOK LIKE IN A REAL PROTEST SCENARIO IN BUENOS AIRES?	43
7. THE CHILLING EFFECT: WHEN THE PERCEPTION OF SURVEILLANCE TECHNOLOGIES AFFECTS PEOPLE’S RIGHTS	46
7.1 CHILLING EFFECTS AND BEHAVIOURAL ADJUSTMENTS RESULTING FROM SURVEILLANCE	47
7.2 SHRINKING OF CIVIC SPACE	48
7.3 SELF-CENSORSHIP AND LACK OF GUARANTEES FOR FREEDOM OF EXPRESSION	50
8. CONCLUSIONS AND RECOMMENDATIONS	52
8.1 TO THE NATIONAL GOVERNMENT AND THE CITY OF BUENOS AIRES:	53
8.2 TO THE NATIONAL GOVERNMENT AND THE MINISTRY OF SECURITY IN PARTICULAR:	54
8.3 TO THE NATIONAL CONGRESS:	55
8.4 TO REGIONAL AND INTERNATIONAL HUMAN RIGHTS BODIES:	55
ANNEX 1 – DETAILS OF PROCUREMENTS AND CONTRACTS	56
PROCUREMENTS AND COMMISSIONING BY THE NATIONAL GOVERNMENT	56
PROCUREMENTS AND COMMISSIONING BY THE GOVERNMENT OF THE CITY OF BUENOS AIRES	57
CAPTURE POINT ACQUISITION AMOUNTS UNDER CABA EXTENSION RESOLUTIONS	59

INDEX OF TABLES

TABLE 1: FREEDOM OF INFORMATION REQUESTS REGARDING SURVEILLANCE TECHNOLOGIES	15
TABLE 2: PROCUREMENT AND COMMISSIONING OF TECHNOLOGY BY THE MINISTRY OF NATIONAL SECURITY	35
TABLE 3: PROCUREMENT OF SURVEILLANCE INFRASTRUCTURE BY THE GOVERNMENT OF THE CITY OF BUENOS AIRES (GCABA)	41
TABLE 4: GCBA REQUIREMENTS FOR VIDEO SURVEILLANCE CAMERAS 2024-2025, AS PER TECHNICAL SPECIFICATIONS IN PROCUREMENT PROCESS 3202-0540-LPU24	42

ACRONYMS

WORD	DESCRIPTION
AAIP	Access to Public Information Agency (Acceso a la Información Pública)
AFC	Federal Cyberintelligence Agency (Agencia Federal de Ciberinteligencia)
AGCBA	Auditor General of the City of Buenos Aires (Auditoría General de la Ciudad de Buenos Aires)
AI	Artificial Intelligence
APN	National Public Administration (Administración Pública Nacional)
CCPR	United Nations Human Rights Committee
CNC	National Centre for Cybersecurity (Centro Nacional de Ciberseguridad)
CONARC	The National Wanted Persons and Arrest Warrants Database (Consulta Nacional de Rebeldías y Capturas)
CS5	Centre for Cyber Synergy of the Federal Police and the Security Forces (Centro de Sinergia Cibernética de las Fuerzas Policiales y de Seguridad Federales)
CSIRT-MINSEG	Computer Security Incident Response Team of the MINSEG (Equipo de Respuesta ante Incidentes de Seguridad Informática del MINSEG)
DPIA	Data Protection Impact Assessments
FRT	Facial Recognition Technology
GCABA	Government of the Autonomous City of Buenos Aires (Gobierno de la Ciudad Autónoma de Buenos Aires)
IACHR	Inter-American Commission on Human Rights
IAcHR	Inter-American Court of Human Rights
ICCPR	International Covenant on Civil and Political Rights
IFJ / FIP	International Federation of Journalists
MINSEG	Ministry of Security (Ministerio de Seguridad)
ODIA	Argentinian Observatory of Information Rights (Observatorio de Derecho Informático Argentino)

WORD	DESCRIPTION
PDPR	Personal Data Protection Regulation (Ley de Protección de Datos Personales)
RENAPER	National Registry of Persons (Registro Nacional de las Personas de la Nación)
SiPreBA	Buenos Aires Press Union (Sindicato de Prensa de Buenos Aires)
SRFP	Fugitive Facial Recognition System (Sistema de Reconocimiento Facial de Prófugos)
UIAAS	Artificial Intelligence Unit for Security (Unidad de Inteligencia Artificial Aplicada a la Seguridad)

GLOSSARY

WORD	DESCRIPTION
ALGORITHM	A set of instructions given to a computer to perform a task or solve a problem.
CHILLING EFFECT	When individuals or groups limit or modify their behaviour, particularly the exercise of rights such as freedom of expression, due to the fear of possible negative consequences, such as surveillance or reprisals.
FACIAL RECOGNITION	Computer vision technology used to identify human faces from images previously used to train an algorithm.
FRT TRAINING DATA	Images used to train a facial recognition algorithm, in order to allow comparison and identification of facial images in the future.
IMAGE RECOGNITION AND BIOMETRICS	Ability to process images and biometric data to identify or verify the identity of individuals, using technology such as facial recognition, image comparison, feature detection and real-time video analysis, facilitating the identification and authentication of identity.
MASS SURVEILLANCE TECHNOLOGY	A type of surveillance technology that allows the monitoring of large volumes of individuals and territories with greater precision and automation.
PREDICTIVE POLICING	Term used to describe policing systems based on data, profiles and risk assessments, the genuinely predictive nature of which is highly questionable. It refers to the use of algorithms and analysis of historical data to anticipate where crimes could occur. Predictive policing also includes techniques that analyse large volumes of heterogeneous data using machine learning algorithms to identify patterns, anomalies and trends, build risk profiles, establish links between events or individuals and generate predictions regarding potential future behaviours or risk scenarios.
PROFILING	The practice of collecting and analysing data on individuals or groups to identify characteristics, patterns of behaviour or levels of risk, in order to classify or make decisions about them.
SOCIAL MEDIA REVIEW AND OPEN-SOURCE INTELLIGENCE (OSINT)	Ability to collect, integrate and analyse information from digital open sources (social networks, websites, forums, public databases), allowing relationships between people to be mapped, patterns of behaviour to be identified, activities to be reconstructed and intelligence to be generated from dispersed data, through correlation techniques and visualization of links.
SOCIO-TECHNICAL APPROACH	An approach to analyzing technology that considers the context in which it is implemented, as well as all cross-cutting political and structural elements. In this report, the analysis includes the policies that enable the use of technology, the applicable regulatory framework, the mechanisms for protection against abuse,

WORD	DESCRIPTION
	the network of public and private actors involved, and the groups and rights affected by the deployment of such technology.
SURVEILLANCE	A set of practices by means of which the state produces, organizes, and uses information on individuals, for the stated purpose of the prevention and investigation of crime.
SURVEILLANCE TECHNOLOGIES	Technologies, including hardware, software and services which are designed to enable covert and non-covert surveillance by and of digital systems with a view to monitor, extract, collect and/or analyse data, including biometric surveillance technologies.
TECHNICAL SPECIFICATIONS (PET)	A document that is part of a purchase process and describes in a clear and detailed manner the technical characteristics, requirements, standards and conditions that the goods or services to be purchased must meet. The aim is to ensure that suppliers understand exactly what is required.

1. EXECUTIVE SUMMARY

CONTEXT: POLICIES TO CURTAIL AND REPRESS PROTEST

Between December 2023 and December 2025, the Argentinian government implemented a slew of security and intelligence reforms and expanded their use of surveillance technologies. This period coincided with the first two years of the administration of Javier Milei and the *La Libertad Avanza* political alliance.

Surveillance plays a central role in the government's agenda. Even during its electoral campaign,¹ the ruling party had proposed the use of tools such as databases linked to facial recognition and greater investment in technology for security purposes. These public commitments led to reforms of the security and intelligence system, as well as the implementation of new practices such as the creation of databases of protesters, monitoring of social media, and the use of facial recognition, drones and mobile cameras.

These reforms took place in the context of the implementation of severe austerity measures in key areas and an institutional restructuring marked by changes in legislation and budgetary measures that expanded the state's punitive, repressive and surveillance capabilities, without a corresponding strengthening of oversight and accountability mechanisms.

At the same time, polarized narratives and rhetoric around the “internal enemy” intensified, resulting in reprisals on women, LGBTI communities, migrants and other marginalized groups, as well as the discrediting and harassment of civic society actors, particularly journalists, the media, social and human rights organizations, unions, the academic community and feminist and other social and environmental movements.

In this environment, surveillance technologies are not neutral but operate as part of an infrastructure designed for social control, persecution of dissent, and a restriction of civic space. They serve to expand surveillance, profiling and reprisals, which in turn directly impact rights such as the rights to privacy, freedom of expression, freedom of peaceful assembly and association.

STRUCTURAL AND OPERATIONAL REFORMS

In just two years, the national government drove a set of institutional reforms designed to expand its surveillance and intelligence capabilities, implemented mainly through executive decrees and resolutions, with no legislative debate.

At the institutional level, the government carried out two reforms of the National Intelligence System to expand the role of intelligence and counterintelligence, including overly broad definitions of what constitutes a “threat”, strengthened justifications for secrecy, enabled greater access and exchange of information between agencies, and created a new specialist cyber intelligence agency. These changes increased the state's capacity to collect and process large volumes of data in a context of weak mechanisms of oversight.

¹ The security agenda included 47 items, far exceeding topics such as Health, Economic Reform, Labour Reform, among others. The platform presented in 2023 is available at: <https://www.electoral.gob.ar/nuevo/paginas/pdf/plataformas/2023/PASO/JUJUY%2079%20PARTIDO%20RENOVADOR%20FEDERAL%20-PLATAFORMA%20LA%20LIBERTAD%20AVANZA.pdf> Accessed in March 2026.

Simultaneously, reforms to the Federal Police statute established new investigative structures and formalized practices such as the monitoring of social media without a court order, and the establishment of “cyber patrolling” as an official function. In addition, specific protocols were adopted for the use of fictitious digital identities in investigations and the deployment of undercover agents in digital environments.

At the operational level, the government set up key instruments such as the “anti-picket” protocol, which allows the federal forces to disperse protests without a warrant and to identify, register and collect information on protesters, organizations and vehicles. It also created the Artificial Intelligence Unit for Security (UIAAS – Unidad de Inteligencia Artificial Aplicada a la Seguridad), with broad responsibilities linked to data analysis, digital monitoring, facial recognition, and crime prediction, again with no specific oversight or accountability mechanisms.

Finally, protocols were adopted to regulate the *ex post facto* use of specific technologies, such as cyber patrolling and facial recognition, thereby expanding operational surveillance in digital environments. Together, these measures constitute an intensification of state monitoring capacities, the incorporation of advanced technologies and the absence of robust oversight and accountability, in a context of growing state actions aimed at controlling and deterring protest and increasing authoritarian practices.

PROCUREMENT OF SURVEILLANCE TECHNOLOGIES

Between 2024 and 2025, the Ministry of National Security acquired mass surveillance technologies worth at least USD 1.2 million. The contracts reviewed show sustained investment in tools designed for open-source monitoring, facial recognition and aerial surveillance. These acquisitions happened in a context of economic austerity, and a lack of sufficient information on oversight, impact assessments or human rights safeguards, barring minimum public procurement information.

Notable procurements among those analysed in this report are:

- a licence for the Maltego open-source investigation platform, which is designed for the collection, cross-checking and visualization of large volumes of data from social media, websites, the dark web, personal data, technical infrastructure and other open sources;
- a licence for Clearview AI facial recognition, a company with a widely known track record of mass exploitation of biometric data without sufficient legal grounds across many contexts globally;
- and the procurement of drones and ground control stations, with automated tracking capabilities, thermal cameras and real-time transmission of images.

These purchases were made possible by the institutional reforms and newly established protocols and provide concrete means for new surveillance activities to be carried out in digital and physical environments. In particular, they expand state capacity to collect and process information on individuals, carry out facial recognition, track movements, and reinforce monitoring activities in public spaces, including during protests.

These procurements must also be analysed in conjunction with the expansion of the video surveillance infrastructure carried out by the Government of the Autonomous City of Buenos Aires, which has significantly increased its territorial coverage through the installation of cameras, image processing systems and associated services. While the national government is strengthening its data analysis, identification and processing capabilities, Buenos Aires is increasing its ability to collect information in public spaces at the same time, with the city government pursuing the installation of expansive surveillance equipment and pursuing contracts for further tools allowing them further surveillance powers. Together, these developments create an integrated surveillance apparatus and increase the state's citywide monitoring and surveillance capacity.

THE CHILLING EFFECT OF SURVEILLANCE

This report shows that, based on interviews conducted in the City of Buenos Aires, that the deployment of surveillance policies and technologies in Argentina has direct impacts on human rights, while also having significant indirect effects on the exercise of human rights, through what is known as the *chilling effect*. This occurs when the mere perception or fear of being monitored causes individuals to modify their behaviour and leads them to limit their participation in the exercise of their human rights, including the right to freedom of speech, association, or peaceful assembly.

Based on interviews with 21 people from a range of backgrounds, including journalists, activists, pensioners, young people and human rights defenders, we conclude that there is a widespread belief of state surveillance in both the physical and digital spheres. This perception is linked to the visible presence of technologies (such as drones and cameras), the monitoring of social media, the collection of information during protests, and a previous track record of state surveillance.

Importantly, this perception translates into concrete changes in behaviour that impact the exercise of basic rights, including:

- Reduced or selective participation in protests, in some cases linked directly to fear of subsequent repression or identification.
- Changes in organizational strategies by activists, protestors, and civil society at-large, including reduced public exposure, greater caution in the planning of activities and a drop in groups' operational capacity.
- Adjustments to communication practices, such as using safer platforms or avoiding channels considered vulnerable.
- Self-censorship on social media and in public spaces, by moderating narratives or reducing participation.
- In the case of journalists, limiting reporting practices and source protection, due to the risks of identification and surveillance.

This report includes specific impacts on particular groups, particularly the press, activists and migrants, and analyses the consequences for young people. In these cases, surveillance is often accompanied by other repressive or punitive measures, such as repression in public spaces or reporting to immigration authorities, which intensifies the chilling effect and leads to higher levels of self-censorship.

Furthermore, our research finds that surveillance does not operate in isolation but is compounded by other security policies to create an environment in which the perception of constant state control undermines trust between individuals and organizations, hinders collective action and increases reluctance to participate in political or social activities. These findings show that surveillance, even when not resulting in direct reprisals, can lead to substantial indirect restrictions on the rights to freedom of expression, assembly and association, in line with warnings issued previously by international human rights bodies. Thus, the impact of such technologies extends beyond their operational use and affects the very nature of civic space.

While surveillance technologies and surveillance policies have been introduced as tools to ostensibly address specific forms of criminal activity, Amnesty International's conclusions demonstrate that broadly drafted legal provisions and the documented history of abuses and misuse of such technologies in Argentina, violate the rights to privacy, equality and non-discrimination, freedom of expression and peaceful assembly, while also stifling transparency and freedom of information.

CLEARVIEW AI'S CORPORATE RESPONSIBILITIES

Amnesty International has found that Clearview AI should have been aware of the human rights risks arising from its business operations more broadly, including in Argentina. Under the UN Guiding Principles on Business and Human Rights (UN Guiding Principles), companies must promptly address adverse human rights impacts with which they are involved, no matter where they operate. This corporate responsibility to respect human rights exists independently of a state's ability or willingness to fulfil its own human rights obligations and over and above compliance with national laws and regulations protecting human rights. To meet this corporate responsibility, a company must take early, proactive and ongoing steps to identify and respond to its potential or actual human rights impacts by conducting due diligence to identify, prevent, mitigate and account for any negative human rights impacts resulting from their operations or as a result of their business relationships with other actors.

Amnesty International has found that Clearview AI has not to date carried out a public, transparent and ongoing human rights impact assessment, nor demonstrated that the company has addressed any potential or actual adverse human rights impacts that their business products or activities may cause, contribute or be directly linked to in Argentina. As such, Clearview AI must cease the development, sale, deployment and

export of FRT in Argentina, or risk that the company contributes to or becomes directly linked to the increasingly hostile environment faced for human rights in the country.

In advance of the publication of this report, Amnesty International wrote to the national and city-level (Buenos Aires) authorities in Argentina to seek their responses to the findings of this research. Amnesty International also wrote to the FRT company Clearview AI outlining human rights concerns related to their products and seek their responses to the information and human rights concerns mentioned regarding the company's product in this report. However, Amnesty International have not received responses from the company at the time of publication of this report.

This report analyses the regulatory reforms and technology procurements made by the Argentinian national government and the city of Buenos Aires. It does not seek to provide a comprehensive analysis of how the corporate actors involved comply with human rights. In this regard, allegations are made against Clearview AI only.

Amnesty International furthermore informed companies that were mentioned in contracts and procurement documents analysed within this report—which included Maltego, DJI, and NOSIS—about its forthcoming publication but did not carry out analysis of the onward implications of their value chains. Amnesty International is not making any allegations against these companies. At the time of publication, Amnesty International has only received a response from Maltego.

Amnesty International makes the following key recommendations to end these violations:

- The national government and the government of the City of Buenos Aires should:
 - Ban the development, production, sale, and use of biometric technologies by all public and private actors that enable mass surveillance and discriminatory targeted surveillance;
 - Ban the development, production, sale, and use of AI systems that create or expand facial recognition databases through the untargeted scraping of facial images from the internet or CCTV footage;
 - Ban automated risk assessment and profiling systems in the context of migration, when used to determine whether people on the move present a 'risk' of unlawful activity or security threats;
 - Immediately suspend the use of all surveillance technologies acquired or deployed without specific legal grounds, human rights and data protection impact assessments (DPIA), or external oversight mechanisms. This includes, in particular, open-source monitoring and aerial surveillance tools.
- The national government, and the Ministry of Security in particular, should:
 - Immediately publish substantive information on the structure, budget, suppliers and technical criteria of all the functions assigned to the UIAAS, as a minimum requirement for transparency and accountability;
 - Set up an intersectoral working group comprising oversight bodies, civil society, and experts in technology and human rights, with a defined mandate, deadlines and expected results, for the purpose of reviewing the scope of the UIAAS and establishing agreed criteria for its regulation;
- The National Congress should:
 - Set up and ensure the effective functioning of the Bicameral Commission for the Oversight of Intelligence Bodies and Activities, pursuant to Article 31 of Law 25.520, providing the resources and powers required to carry out specific oversight of surveillance technologies.
- Regional and International Human Rights bodies should:
 - Enact legislation to ban the use, development, production, sale and export of remote biometric recognition technology for mass surveillance as well as remote biometric or facial recognition technology used for identification purposes used within their own jurisdictions by both state agencies and private sector actors, as technologies that are fundamentally incompatible with international human rights law

2. METHODOLOGY

2.1 CONTEXT, METHOD, AND SCOPE OF THIS STUDY

This report adopts a socio-technical approach that examines not only the technologies used, but also the policies that enable their use, the applicable regulatory framework, the mechanisms for protection against abuse, the network of public and private actors involved, and the groups and rights affected by their deployment.

This report focuses on the period between December 2023 and December 2025, which includes the first two years of the presidency of Javier Milei at the national level and the tenure of Jorge Macri as head of government of the city of Buenos Aires. This report focuses on three types of surveillance technologies that have been acquired by the national government and the Government of the City of Buenos Aires. These technologies can be broadly grouped into the following categories:

- Social media review and open-source intelligence (OSINT).
- Image recognition and biometrics.
- Crime prediction and determination of areas for heightened surveillance and policing.

In terms of methodology, the purpose of this report is to analyse the human rights impact of the use of surveillance technologies by Argentina's national government. Given that this is a phenomenon that is still evolving, this report provides a snapshot of the human rights impact and is not meant to be exhaustive in its analysis. It combines an analysis of the international, regional and local human rights legal frameworks applicable to the use of surveillance technologies in Argentina with a detailed study of the national regulations that led to the reforms of the national security and intelligence systems. In addition, the report also draws on local and regional examples to build an understanding of the international context surrounding the use of this type of technology.

Research also examines the surveillance technologies acquired by the state, based on a review of the relevant public procurement processes, in order to accurately identify the tools currently being used. Finally, the report analyses the impact of this surveillance on individuals, including a chilling effect on the exercise of human rights.

The research does this through:

ANALYSIS OF PROCUREMENT AND COMMISSIONING OF SURVEILLANCE TECHNOLOGIES.

In order to analyse the technologies described earlier, a study of the relevant procurement processes in the publicly accessible official platforms of the national government and the city of Buenos Aires (ComprAR and BA Compras, respectively) was carried out. Using the information published on such platforms and the search functionalities available, databases were generated to filter the purchases of the relevant national and local (Buenos Aires) security ministries and law enforcement agencies for the 24-month period covered in this report. However, this provides merely a snapshot of the true scale of the problem, as any procurement information that is not publicly available due to secrecy clauses cannot be included in the analysis. From this analysis, 11 procurements were selected, 5 at the national level, and 6 for the City of Buenos Aires, to obtain a sample that provides a snapshot of the diversity of technologies acquired.

For each case analysed, the procurement process followed by the authorities was tracked in order to examine aspects such as the type of procedure (direct procurement, public tender and so on), the procurement method (open order, EPC/turnkey and so on), duration, object and amount, among other relevant data. The analysis is based on the information contained in the procurement files themselves, as well as the corresponding purchase orders and resolutions providing institutional authorization. To more accurately identify the purpose of each procurement and the expected functionalities of the acquired technologies, the Technical Specifications (PET) document attached to each public procurement process was examined. Similarly, the resolutions provide information on the government departments involved, which in turn provides an indication of the policies in respect of which these acquisitions were made.

FREEDOM OF INFORMATION REQUESTS

With respect to official sources of information, as previously mentioned, the analysis contained in this report is based on information published on procurement and commissioning platforms, official gazettes publishing legislation, official newsletters and other publications issued by both the national and the autonomous Buenos Aires governments.

However, a significant part of the information is not available on such platforms or publications and was obtained through formal freedom of information (FOI) requests. At the national level, this right is regulated by Law 27.275 on Access to Public Information² (published in 2016), whereas the Autonomous City of Buenos Aires has its own Law 104 on Access to Public Information³ (modified and updated in 2016).

Some of the information analysed in this report was obtained through FOI requests made by Amnesty International between April 2025 and January 2026. During that period, the organization submitted four FOI requests relating to various aspects of the use of surveillance technologies by both governments. Table 1 provides a list of these requests.

TABLE 1: FREEDOM OF INFORMATION REQUESTS REGARDING SURVEILLANCE TECHNOLOGIES

SUBMITTED TO	INFORMATION REQUESTED (SUMMARY)	DATE	REPLY RECEIVED
MINISTRY OF NATIONAL SECURITY	Information on the operation, regulation, budget and activities of the Artificial Intelligence Unit for Security (UIAAS); use of facial recognition by security forces (technology, databases, contracts, evaluations and impact); and cyber patrolling on social media (monitoring, tools, personal data and agreements with companies).	8 May 2025	26 June 2025
MINISTRY OF NATIONAL SECURITY	Legislation, protocols, equipment and use of video recordings by security forces at demonstrations, including cameras and drones, access to footage, purposes of use, controls, storage and departments responsible.	17 December 2025	3 February 2026
MINISTRY OF NATIONAL SECURITY	Operational status of the UIAAS (structure, activities, legislation, recruiting, procurement, and international cooperation); implementation of the facial recognition protocol (software, procurements and use of databases); and application of the cyber patrolling protocol (implementation, tools, monitoring and processing of personal data).	19 December 2025	2 February 2026
MINISTRY OF SECURITY OF THE CITY OF BUENOS AIRES	Information on contracting, technical specifications and implementation of video surveillance systems, digital forensics, facial recognition and fugitive detection in the GCABA, including cameras,	4 February 2026	16 and 17 March 2026 ⁴

² Available at: <https://servicios.infoleg.gob.ar/infolegInternet/anexos/265000-269999/265949/norma.htm>

³ Available at: <https://boletinoficial.buenosaires.gob.ar/normativaba/norma/982>

⁴ Due to a technical issue preventing access to the information, A was only able to access the content of the responses submitted by the GCABA on 27 May 2026.

SUBMITTED TO	INFORMATION REQUESTED (SUMMARY)	DATE	REPLY RECEIVED
	software, licences, audits, institutional controls and integration with other systems.		

Source: Summarized by Amnesty International

While the authorities responded to these requests, they were mostly partial responses. In the case of the first request submitted, for example, the questions on the use of facial recognition were only partially answered, with the omissions being justified on grounds of reservations for reasons of national security set out in Article 8(A) of Law 27.275 and its corresponding regulatory decrees. In the same request, questions on the monitoring of social media (or *cyber patrolling*) were not responded to on the grounds of the confidentiality of the activities of the National Intelligence System, as set out in Articles 16 and 16(bis) of the National Intelligence Law (Law 25,520).

INTERVIEWS: ANALYSIS OF THE CHILLING EFFECTS OF SURVEILLANCE TECHNOLOGIES

To analyse the chilling effects of surveillance for this research, the methodology adopted was that used by Murray and others,⁵ who consider this phenomenon as a set of behavioural changes arising from fear, awareness or anticipation of surveillance, including self-censorship, reluctance to engage with individuals or organizations believed to be subject to surveillance, and an erosion of interpersonal trust that undermines collective action.⁶

Between October and December 2025, 21 people from a range of backgrounds were interviewed, including media professionals (designers, photographers, journalists, content creators for streaming channels and trade union representatives), students and young people,⁷ human rights activists and pensioners. All of them are residents of the city of Buenos Aires, given that one of the goals of this report is to analyse the experiences of individuals and communities who participated in the mobilizations near the National Congress, driven by opposition to the current administration's economic reforms, including sweeping austerity measures, deregulation, and reductions in public spending. Thirteen people were interviewed individually and remotely, with the remaining eight being interviewed in face-to-face group meetings.

The following aspects were discussed in the interviews:

1. Perceptions of surveillance

- Knowledge/awareness of surveillance technologies.
- Distinction between actual and perceived surveillance.
- Influence of traditional (cameras, police) versus digital tools (telephone surveillance, data collection).

2. Freedom of assembly and political participation

- Erosion of trust within groups.
- Reluctance to attend or organize protests/meetings.
- Avoidance of individuals or organizations perceived as being subject to surveillance.

3. Freedom of speech

- Self-censorship practices.
- Chilling effects (direct or indirect).
- Online versus offline speech.

⁵ Murray, D., Fussey, P., Hove, K., Wakabi, W., Kimumwe, P., Saki, O., & Stevens, A., 2024 "The chilling effects of surveillance and human rights: Insights from qualitative research in Uganda and Zimbabwe", 2024, *Journal of Human Rights Practice*, 16(1), <https://doi.org/10.1093/jhuman/huad020>, pp. 397-412.

⁶ Murray, D., Fussey, P., Hove, K., Wakabi, W., Kimumwe, P., Saki, O., & Stevens, A., 2024 "The chilling effects of surveillance and human rights: Insights from qualitative research in Uganda and Zimbabwe", 2024, *Journal of Human Rights Practice*, 16(1), <https://doi.org/10.1093/jhuman/huad020>, Chapter 6: Conclusion.

⁷ Four of the people interviewed in group meetings were from the Amnesty International youth group, a space where young people aged 15 to 25 volunteer for human rights campaigns. For privacy reasons, the group's responses will be discussed as a whole. No children were interviewed for this report.

These aspects were incorporated into a semi-structured questionnaire consisting of fourteen questions, which served as a framework for both the individual and group interviews. The questions were designed to engage participants in their role as members of groups or organizations, rather than as individuals acting in isolation.

In advance of the publication of this report, Amnesty International wrote to the national and city-level (Buenos Aires) authorities in Argentina to seek their responses to the findings of this research. At the time of publication, the authorities have not responded. Amnesty International also wrote to the FRT company Clearview AI to seek their responses to the information mentioned about the company in this report. At the time of publication, the company has not responded.

Amnesty International furthermore informed companies that were mentioned in contracts and procurement documents analysed within this report—which included Maltego, DJI, and NOSIS—about its forthcoming publication, but did not carry out analysis of the onward implications of their value chains. Amnesty International is not making any allegations against these companies. At the time of publication, Amnesty International has only received a response from Maltego.

VIDEO SURVEILLANCE CAMERAS: COLLABORATIVE CONSTRUCTION OF INFORMATION

The government of the city of Buenos Aires (GCABA – Gobierno de la Ciudad Autónoma de Buenos Aires) has not published any information on the specific location of the cameras for the city's video surveillance system, something that is of utmost importance when analysing respect for the privacy of those seeking to demonstrate, and their right to peaceful protest.

In this regard, Amnesty International, together with local human rights organizations, held a “hackathon” in October 2025. The purpose of the event was to collaboratively map the coverage of surveillance cameras located in the vicinity of the National Congress using Google Street View imagery. The location was identified as one frequented by civil society during protests in particular and was the reference for establishing the scope and exposure to possible mass surveillance. As Amnesty International has previously documented, through mapping the locations of CCTV cameras, the potential reach of facial recognition exposure can be established, as the technology is frequently paired as software used with cameras. This method did not make a distinction between facial recognition exposure by whether it is real time or through subsequent processing by the GCABA or the national authorities in that area. Rather, participants browsed the streets in a radius of eight blocks within the National Congress looking for cameras mounted to building and other public infrastructure (e.g. lamp posts, traffic signals, etc.), generating a list of coordinates of discovered cameras. The list was subsequently peer reviewed by participants, and a map generated from the coordinated.

As a result of this event, a map was created and a space for discussion and exchange between the participating organizations was set up.⁸

2.2 HISTORY OF SURVEILLANCE IN ARGENTINA AND IN THE REGION

Between December 2023 and December 2025, the national government introduced a series of reforms to the roles of the security forces and began acquiring a range of technologies to increase their surveillance capabilities. This period represents the first two years of the administration led by La Libertad Avanza, an alliance that stood for election for the first time in 2021. In 2023, during its second electoral campaign, the alliance won the presidential elections, resulting in the then member of parliament Javier Milei becoming president. The election campaign was characterized by proposals for economic cuts, which the candidate enacted by taking a chainsaw to election rallies.

In addition to the economic agenda, the security agenda also featured prominently in La Libertad Avanza's electoral manifesto. The use of surveillance technologies has been a government priority since its inception, as reflected in the manifesto submitted to the national electoral authority.⁹ The section on “National security”

⁸ The results of the hackathon are available in section 6.2.

⁹ Points 10 and 14, respectively. Link to the full electoral platform: <https://www.electoral.gob.ar/nuevo/paginas/pdf/plataformas/2023/PASO/JUJUY%2079%20PARTIDO%20RENOVADOR%20FEDERAL%20-PLATAFORMA%20LA%20LIBERTAD%20AVANZA.pdf>

of the manifesto included proposals to create a national database of individuals wanted by the police linked to security cameras with facial recognition, and to invest in technology for all security forces. This shows the importance placed on surveillance activities and the use of technology in the agenda of the candidates who were running for government at the time.

The new administration delivered on both its economic and its surveillance promises. On economic issues, the government introduced adjustments in areas such as social security, healthcare, education, and productive development.¹⁰ On issues of surveillance, reforms were introduced in the national security and intelligence systems during the first two years of the administration, which were subsequently complemented with new units and protocols for tasks such as the compilation of databases of protesters, the monitoring of social media and open-source information, the use of facial recognition technologies, and the deployment of drones and mobile cameras, among others.¹¹

Threats to economic and social rights were exacerbated by an accelerated process of institutional restructuring, marked by the spread of authoritarian practices, overt attacks on the gender and diversity agendas, and a fundamental shift in foreign policy. The government pushed through reforms that expanded its enforcement capacity without strengthening oversight and accountability mechanisms, placing surveillance technologies centre stage. These are not neutral tools, but devices that serve to reinforce social control and the persecution of dissent and restrict civic space, particularly in environments with a lack of transparency and weak institutional controls. The impact of technology on human rights must therefore be analysed in the context of this authoritarian trend, as part of an infrastructure of power that amplifies the surveillance, profiling and reprisals against individuals and groups and affects the right to privacy, freedom of expression, association and assembly, and is integral to the sociotechnical approach of this research.

2.3 MASS SURVEILLANCE WITH NO OVERSIGHT: FACIAL RECOGNITION OF FUGITIVES IN THE CITY OF BUENOS AIRES

The Autonomous City of Buenos Aires, Argentina's capital, has a track record of misuse of mass surveillance technologies. The Fugitive Facial Recognition System (SRFP – Sistema de Reconocimiento Facial de Prófugos), implemented by the Government of the City of Buenos Aires (GCABA) between 2019 and 2020 and subsequently suspended by the courts in 2022,¹² is a representative case of one of the first instances of artificial intelligence applied to policing in the country, and one that showed serious impacts on human rights.¹³ Many of the actors, technologies and infrastructures involved in that system remain in place currently, and could play a key role in potential collaboration between the national and city governments vis-à-vis the surveillance policies promoted by the government of Javier Milei.

The SRFP involved the use of facial recognition algorithms to analyse images captured by video surveillance cameras in public spaces and automatically cross-referenced with the CONARC databases (National Wanted Persons and Arrest Warrants Database or *Consulta Nacional de Rebeldías y Capturas*) and the SIBIOS (*Sistema Federal de Identificación Biométrica para la Seguridad*) biometrics database of the RENAPER (National Registry of Persons – Registro Nacional de las Personas de la Nación).¹⁴ Although Resolution 398/2019¹⁵ of the GCABA Ministry of Justice and Security imposed strict limits on the use of the system and the obligation to destroy the data once the court order ceased to be valid, its implementation exceeded the limits set, causing its suspension by the courts. As became evident during the court proceedings, one of the main problems of the SRFP was the low quality of the data from the CONARC database, which resulted in

¹⁰ According to data analyzed by CEPA (Centre for Argentine Political Economy), based on official budget execution data. The report is available at: <https://centrocepa.com.ar/informes/735-la-ejecucion-presupuestaria-de-la-administracion-publica-nacional-datos-a-diciembre-2025> (accessed March 2026).

¹¹ The reforms introduced by the national government in this respect are analysed in depth in Chapter 5 of this report.

¹² For further information, see this article by the Centre for Legal and Social Studies (CELS), one of the organizations in the legal proceedings against the system: <https://www.cels.org.ar/web/2023/04/confirman-la-inconstitucionalidad-del-uso-del-sistema-de-reconocimiento-facial/> (accessed March 2026).

¹³ Amnesty International, together with other human rights organizations, requested the suspension of the SRFP due to its high potential of violating human rights. See statement released in October 2020: <https://amnistia.org.ar/noticias/la-legislatura-portena-debe-rechazar-el-uso-de-la-tecnologia-de-reconocimiento-facial-para-la-vigilancia-del-espacio-publico>

¹⁴ As stated in the Annex to Resolution 398/19, establishing the system operation guidelines, <https://documentosboletinoficial.buenosaires.gob.ar/publico/PE-RES-MJYSGC-MJYSGC-398-19-ANX.pdf>

¹⁵ Resolution 398/2019. Available at: <https://boletinoficial.buenosaires.gob.ar/normativaba/norma/464360> (accessed December 2025).

multiple cases of individuals being wrongly detained. Added to this was a lack of public information on the operation of the algorithm system and the reliance on proprietary software with no independent audits, which limited the state's ability to exercise control.¹⁶

Although the SRFP remains suspended at the time of writing of this report, the GCABA has made significant investments in video surveillance infrastructure, expanding and renewing the system, including fixed and mobile cameras, drones, aerostat systems and devices in patrol cars. However, there is no public information on the location of these devices, and the government has refused to respond to FOI requests on grounds of public safety.¹⁷

The legal challenge against the SRFP, which began in 2020 with a collective *amparo* action,¹⁸ brought by the Centre for Legal and Social Studies (CELS) and the Argentine Observatory of Information Rights (ODIA – Observatorio de Derecho Informático Argentino), has helped to more clearly understand the extent of the irregularities in its operation. The GCABA carried out approximately ten million retrievals of biometric data from the RENAPER, in a context where the data universe required for the system's operation, the CONARC database, did not exceed forty thousand people.¹⁹ Furthermore, an IT analysis confirmed that 15,459 individuals had been uploaded to the SRFP search engine despite not being registered in the CONARC database; in other words, without a court order authorizing their identification through facial recognition. Added to this was the absence of effective institutional oversight mechanisms and prior impact assessments, as well as a lack of transparency in the system's operation.

The SRFP case should not be viewed in isolation or as a resolved incident, but rather as a warning of the potential risks involved in strengthening surveillance and control policies in the absence of robust regulatory frameworks, effective oversight and adequate safeguards for the protection of human rights. The deployment of these technologies in Argentina raises critical questions about limits on state power, the impact on political participation and protest, and the need to assess these practices in light of international human rights standards.

2.4 REGIONAL EXPERIENCES: LATIN AMERICA AND THE SPREAD OF MASS SURVEILLANCE

The use of surveillance technologies by governments in Latin America is steadily increasing. This is taking place through a combination of traditional tools, such as video surveillance cameras, with automated facial recognition systems, mass data monitoring, cyber patrolling, interception of communications and predictive analytics using artificial intelligence.

One of the most visible examples of this trend is the expansion of video surveillance systems in large cities. In Mexico City, for example, the C5 system comprises hundreds of thousands of cameras connected to command centres that use automated image analysis. Civil society organizations have highlighted the absence of safeguards, lack of transparency and lack of legal certainty regarding its operation.²⁰

Brazil is a prime example of the use of facial recognition technologies at mass gatherings, such as at sporting and other major events, where the authorities have reported arrests based on biometric matches.²¹ These actions have been presented as successful in terms of security, but human rights organizations have warned of structural bias and systematic identification errors inherent in these technologies, resulting in a well-

¹⁶ As stated in the ruling ordering suspension of the SRFP, the database was updated in 2020, resulting in a reduction from 46,000 to 33,000 records. The head of the department responsible for managing the database stated that its use within the framework of the SRFP could lead to false positives, given various internal management issues or errors in data provision. *Fallo del Juzg. CAyT N.º 4, Sec. 7, Observatorio de Derecho Informático Argentino (ODIA) y otros c/ GCBA s/ amparo – otros, Expte. N.º 182908/2020-0* [Ruling of CAyT Court No. 4, Sec. 7, ODIA and others v. GCBA s/ amparo – others, Case. No. 182908/2020-0]. (September 2022). Available at: <https://repositorio.mpd.gov.ar/jspui/handle/123456789/4658>

¹⁷ The surveillance infrastructure is largely integrated within the nationwide “Safe Trains” Programme, through which cameras and monitoring centres were installed in multiple train stations under the jurisdiction of the national government. See: <https://www.argentina.gob.ar/viajaseguro/si-viajas-en-tren> (accessed March 2026).

¹⁸ Expedited judicial remedy proceedings to protect basic rights.

¹⁹ From the proceedings in the case *Observatorio de Derecho Informático Argentino (ODIA) y otros c/ GCBA s/ amparo – otros* [ODIA and others v. GCBA s/ amparo – others]. Ruling of the CAyT Court of the CABA of 7 September 2022. Available at: <https://www.saij.gob.ar/FA22370014> (accessed December 2025).

²⁰ For more information, see: <https://r3d.mx/2025/08/26/ojos-que-vigilan-ciudad-de-mexico-sera-la-ciudad-mas-videovigilada-de-america-latina/> (accessed February 2026).

²¹ The *O Panóptico* project tracks the use of facial recognition in different regions of the country. Available at: <https://www.opanoptico.com.br/> (accessed February 2026).

documented perpetuation of inequalities and discrimination against Black and Indigenous communities and other population groups.²²

Another key area is targeted digital surveillance and the interception of communications. In Mexico, the use and documentation of the Pegasus spyware against journalists,²³ activists and public figures, has revealed the acquisition of cyber intelligence tools by state agencies.²⁴ In El Salvador, international organizations have pointed to the use of technologies to monitor communications in the context of the state of exception.²⁵ These cases show that surveillance is not limited to physical spaces, but extends to the digital environment.

The creation of biometric databases and national identification systems is also significant. Countries such as Argentina and Chile have modernized their civil registries by incorporating fingerprint and facial recognition technology, as well as remote verification of identity for public procedures, a trend that increased following the Covid-19 pandemic in 2020. While these innovations purport to improve administrative efficiency, they also enhance the state's ability to track people's movements and activities at an unprecedented scale.

Human rights organizations have been monitoring this trend. All these processes, to cite a few examples, were recently analysed in a report by the AI Sur consortium,²⁶ where it is argued that the use of these technologies not only increases in the absence of specific regulation but is also part of a regional trend to legitimize mass and indiscriminate surveillance measures that are incompatible with international human rights standards. The organization Access Now also analysed in detail²⁷ the procurement of technologies used for surveillance in the region, stating that the companies supplying them are flying under the radar, selling surveillance technology that is being deployed across Latin America "without sufficient transparency or public scrutiny", and yet, according to the study, their tools are frequently involved in human rights violations perpetrated against civil society.

There are common patterns in the trend across the region, specifically a rapid expansion in the roll-out of surveillance technologies, aggravated by inadequate regulatory frameworks and weak or non-existent mechanisms for public oversight.

²² The "Tire Meu Rosto da Sua Mira" project calls for the suspension of facial recognition systems in Brazil, due to their "abusive and non-transparent" use. The campaign is available at: <https://tiremeurostodasuamira.org.br/> (accessed February 2026).

²³ Amnesty International's Security Lab played an important role in exposing the relevant forensic evidence. See: <https://www.amnesty.org/en/latest/news/2022/03/the-pegasus-project-how-amnesty-tech-uncovered-the-spyware-scandal-new-video/>

²⁴ Mexico was the state with the most documented victims of the Pegasus system, with 456 people surveilled. See: <https://r3d.mx/2025/04/14/gobierno-mexicano-uso-pegasus-para-espiar-al-menos-a-456-personas-en-2019/> (accessed February 2026).

²⁵ See: <https://articulo19.org/investigaciones-periodisticas-revelan-estrategias-hechas-por-funcionarios-allegados-a-bukele-para-espiar-y-vigilar-a-funcionarios-del-gobierno-y-periodistas-con-voces-criticas/> (accessed February 2026).

²⁶ AI Sur (2025), *Surveillance Trends and Practices in Latin America. Case studies from Brazil, Chile, Colombia, El Salvador, Mexico, Peru and Paraguay*, <https://www.alsur.lat/en/report/surveillance-trends-and-practices-latin-america-case-studies-brazil-chile-colombia-el-salvador-mexico-peru-paraguay>

²⁷ Access Now (2021), *Surveillance Tech in Latin America: Made abroad, deployed at home*, <https://www.accessnow.org/surveillance-tech-in-latin-america-made-abroad-deployed-at-home/>

3. LEGAL STANDARDS APPLICABLE TO THE USE OF SURVEILLANCE TECHNOLOGIES IN ARGENTINA

The regulatory framework applicable to the use of surveillance technologies in Argentina is part of a set of human rights obligations that includes international human rights law with constitutional status and specific national legislation on the protection of personal data and access to public information.²⁸ These regulations establish clear limits on the deployment of surveillance technologies, particularly where these may affect human rights such as privacy, freedom of expression, freedom of association, freedom of assembly, and political participation, which are the subject of analysis in this report.

In this chapter, a structured analysis of the specific rights considered, based on the different regulatory frameworks, is carried out. Firstly, international instruments, in particular the International Covenant on Civil and Political Rights (ICCPR),²⁹ as the primary benchmark for respect for privacy, freedom of expression and freedom of association in the face of surveillance practices. Secondly, the treaties and standards of the inter-American human rights protection system are analysed, given their central role in the region and the specific design of criteria applicable to contexts of protest, journalism and political participation. Finally, the report considers relevant regulatory and public policy developments at the national and local levels, in particular legislation on the protection of personal data, access to public information and other regulations governing state action, which establish specific limits and obligations regarding the use of surveillance technologies.

²⁸ The constitutional reform of 1994 incorporated various international human rights treaties into the Argentinean constitution, thereby affording them constitutional status and becoming directly applicable and binding for all state authorities (Article 75(22), Constitution of the Argentine Nation). Available at: https://www.argentina.gob.ar/sites/default/files/derechoshumanos_publicaciones_colecciondebolsillo_01_constitucion_nacion_argentina.pdf

²⁹ Office of the High Commissioner of Human Rights, the International Covenant on Civil and Political Rights: <https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights>

3.1 RIGHT TO PRIVACY AND PROTECTION OF PERSONAL DATA

At the international level, the International Covenant on Civil and Political Rights constitutes the main binding instrument for the analysis of the use of surveillance technologies. In particular, Article 17 protects all persons against arbitrary or unlawful interference with their privacy, family, home or correspondence, and against unlawful attacks on their honour and reputation. This human right is especially relevant in the face of surveillance practices that involve systematic collection, storage and analysis of personal data, in both digital and physical environments.

At the regional level, the American Convention on Human Rights (American Convention)³⁰ reinforces and complements the obligations of the Argentinian state to protect the right to private life and honour (Article 11).

At the domestic level, the National Constitution guarantees the protection of privacy (Article 19) and recognizes the inviolability of correspondence and private documents. Likewise, the 1994 constitutional reform expressly incorporated the right to the protection of personal data, recognizing the right of all persons to access, update and suppress information held about them in public or private registers or data banks (Article 43). This recognition takes on particular significance in the context of technological surveillance, where the collection and processing of personal data can take place on a mass scale and in a systematic manner, with little public scrutiny.

National legislation on the protection of personal data³¹ establishes the principles that must govern how the state processes data, including those of legality, purpose, proportionality and data quality and security. These principles are directly applicable to surveillance systems and technologies used for the identification, tracking or profiling of individuals. In particular, the requirement for a specific and explicit purpose, as well as the prohibition of processing that is excessive or incompatible with the stated objectives (Article 4), significantly limits surveillance practices that may lead to political, trade union or labour persecution, or the criminalization of social protest and the work of journalists. Similarly, Argentina has acceded to Convention 108+ of the Council of Europe,³² thereby undertaking significant international commitments on the protection of personal data, although these have not been fully reflected in current domestic legislation. This convention sets out a standard of protection aimed specifically at safeguarding against automated data processing.

3.2 FREEDOM OF EXPRESSION

The International Covenant on Civil and Political Rights (Article 19) and the American Convention (Article 13) guarantee freedom of expression. Domestically, the National Constitution guarantees freedom of expression in Articles 14 and 32.

In the inter-American system, the Special Rapporteur for Freedom of Expression (RELE) of the Inter-American Commission on Human Rights (IACHR) has developed specific standards on surveillance, criminalization of protest and indirect restrictions on the exercise of rights that are directly applicable to the analysis of technologies that monitor, identify or register individuals during public protests.

In June 2024, the IACHR and its RELE expressed concern about the disproportionate use of force against individuals and journalists during protests in Argentina, reiterating that the state must treat peaceful protest as a legitimate exercise of rights, refrain from criminalizing or stigmatizing it, and guarantee safe conditions for journalists.³³

The link between freedom of expression and technological surveillance was made explicit in 2025, in a joint statement by the UN Special Rapporteur on the rights to freedom of assembly and association, the RELE

³⁰ Organization of American States, American Convention on Human Rights: https://www.oas.org/dil/treaties_b-32_american_convention_on_human_rights.pdf

³¹ Law 25.326. Available at: <https://servicios.infoleg.gob.ar/infolegInternet/anexos/60000-64999/64790/texact.htm> (accessed December 2025).

³² Through Law 27.699, of November 2022. Available at: <https://www.boletinoficial.gob.ar/detalleAviso/primera/276783/20221130>. Accessed December 2025; Council of Europe, Convention 108+, https://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/LIBE/DV/2018/09-10/Convention_108_EN.pdf

³³ Inter-American Commission on Human Rights (IACHR), Argentina Must Respect Rights to Freedom of Association and Peaceful Assembly While Keeping Its Citizens Safe, Say IACHR and Its Special Rapporteur for Freedom of Expression, 4 July 2024, https://www.oas.org/en/iachr/jsForm?File=/en/iachr/media_center/preleases/2024/158.asp

and other regional rapporteurs.³⁴ The statement warned that arbitrary and unlawful use of surveillance technologies, such as spyware and facial recognition using AI, amplifies the criminalization of protest and of civil society, and noted that such tools enable preventive detentions long after a demonstration and have a chilling effect on organization, participation and journalistic coverage. Accordingly, it calls for a ban on the use of arbitrary mass surveillance during protests and for robust safeguards, including case-by-case decisions, transparency, independent oversight and redress mechanisms.

3.3 FREEDOM OF PEACEFUL ASSEMBLY AND ASSOCIATION

The International Covenant on Civil and Political Rights recognizes freedom of association (Article 22) and the right to peaceful assembly (Article 21). The American Convention protects freedom of peaceful assembly (Article 15) and freedom of association (Article 16), rights that the inter-American system has interpreted as being interdependent. Domestically, the National Constitution guarantees the right to association and assembly in Article 14 bis.

Both the UN Human Rights Committee and the IACHR have recognized that the mere existence of unlawful or disproportionate surveillance practices can have a chilling effect on political participation, collective organization, trade union activity, social protest or the exercise of journalism, even in the absence of explicit sanctions or formal restrictions. This is addressed in detail in the Human Rights Committee General Comment 37 (2020) on the right of peaceful assembly. The Committee establishes that this right is not limited to physical public spaces but extends to digital environments and warns that while surveillance technologies can be legitimately used to detect threats of violence, they may violate the privacy of participants and bystanders and discourage the exercise of the right they purport to protect.³⁵

At the regional level, the IACHR has also documented this specific issue. In its observations following a visit to Colombia in June 2021, it identified that the profiling of social media users and the stigmatization of protesters through labels such as “terrorism” or “vandalism” build a hostile environment that deters protest and freedom of expression, particularly in digital spaces.³⁶ This is a relevant regional precedent for analysing similar practices in Argentina.

3.4 RIGHT TO EQUALITY AND NON-DISCRIMINATION

The right to equality and non-discrimination is a cross-cutting principle of international human rights law and a key interpretative framework for analysing the use of surveillance technologies. Articles 2 and 26 of the International Covenant on Civil and Political Rights establish the obligation of states to guarantee to all persons the enjoyment of the rights recognized in the covenant without distinction, as well as the autonomous right to equality before the law and to protection against all forms of discrimination.

At the regional level, the American Convention enshrines this principle in Articles 1.1 and 24, establishing the obligation to respect and guarantee rights without discrimination and recognizing the right to equality before the law.

Applied to the use of surveillance technologies, this regulatory framework is particularly relevant to the risks of algorithm bias or automatic profiling. A recent report³⁷ by the Office of the United Nations High Commissioner for Human Rights (OHCHR), analyses the role of data as a source of discrimination and inequality in key sectors, warning that automated and biometric recognition systems can embed bias and disproportionately affect certain groups, as well as facilitate profiling based on protected characteristics and the identification of protesters and dissidents, which can constitute a form of discrimination.³⁸

³⁴ Inter-American Commission on Human Rights (IACHR), Joint declaration on protecting the rights to freedom of peaceful assembly and of association from criminalization amid intensified existential threats, 19 September 2025, https://www.oas.org/en/iachr/jsForm?File=/en/iachr/expression/basic_documents/declarations/2025.asp (accessed on 10 July 2026).

³⁵ United Nations Human Rights Committee, CCPR/C/GC/37, available at: <https://docs.un.org/en/ccpr/c/gc/37> (accessed December 2025).

³⁶ The IACHR's observations and recommendations are available at: https://www.oas.org/es/cidh/informes/pdfs/ObservacionesVisita_CIDH_Colombia_SPA.pdf (accessed December 2025).

³⁷ The right to privacy in the digital age: Report of the Office of the United Nations High Commissioner for Human Rights A/HRC/60/45 (2025). Available at: <https://docs.un.org/en/A/HRC/60/45>.

³⁸ A/HRC/56/68 (2024). Available at: <https://docs.un.org/en/A/HRC/56/68>

In light of these risks, international standards have begun to require human rights impact assessments that specifically address the risks of discrimination in the design and implementation of technology systems. This implies transparency in operating criteria, auditability of algorithms, data quality and representativeness, and effective oversight and accountability mechanisms.³⁹

THE THREE-PART TEST: LEGALITY, LEGITIMACY AND PROPORTIONALITY

The ICCPR (Articles 17, 19, 21 and 22) and the American Convention (Articles 11, 13, 15 and 16) share a common structure in that they expressly recognize the protection of private life, freedom of expression, freedom of peaceful assembly and freedom of association and prohibit arbitrary interference, but at the same time allow restrictions under strict conditions.

Any measures of state surveillance, including those carried out using digital technologies or automated systems, must meet three requirements: they must be provided by law, pursue a legitimate aim, and be necessary and proportional to the objective stated. In international human rights law, this is known as the three-part test.⁴⁰ The three requirements operate jointly and cumulatively: failure to comply with any one of them renders the measure incompatible with international law, regardless of whether the other requirements are met.

Legality: Surveillance must be accompanied by legislation that is accessible, precise and predictable. It is not enough for a law to exist: it must clearly define who may impose surveillance, under what conditions, within what scope and for how long. As it relates to technology, this means systems must not be deployed without explicit legal grounds, authorizations that are ambiguous and enable discretion, and regulatory frameworks that do not consider the specific capabilities of the tools used. Examples of technologies falling into this category include facial recognition or predictive analytics based on mass surveillance.

Legitimacy: Measures must pursue an aim recognized as legitimate under international law, such as national security, public order, public health or protection of the rights of third parties. This element acts as a filter for the purpose of the measure: surveillance aimed at monitoring political, trade union or journalist activity or at identifying participants in social protests, does not meet this requirement, even if formally authorized. If the stated aim is security but the effective use is controlling dissent, the measure fails to meet this threshold.

Necessity and proportionality: Measures must be the least restrictive available to achieve the legitimate aim, and the extent to which rights are affected must not exceed what is strictly necessary. Applied to digital surveillance, this means that mass arbitrary surveillance is incompatible with this standard by definition: if the objective can be achieved through targeted surveillance under a court order, the deployment of facial recognition systems in public spaces or the monitoring of social networks at scale does not pass this test. Proportionality also requires that collateral impact for bystanders, journalists and individuals not under investigation is minimal and justified.

Within this framework, the three-part test serves as a key tool for assessing not only express restrictions, but also instances of state interference which, due to their scope, lack of transparency or intensity, are incompatible with regional and international human rights standards.

³⁹ For example, the Methodology for assessing the risks and impacts of artificial intelligence systems from the perspective of human rights, democracy and the rule of law (HUDERIA) promoted by the Council of Europe. Available at: <https://www.coe.int/en/web/artificial-intelligence/huderia-risk-and-impact-assessment-of-ai-systems>.

⁴⁰ This standard has been developed and clarified by international bodies of authoritative interpretative powers, in particular by the United Nations Human Rights Committee (CCPR), which in its General Comment 34 of 2011 held that any restriction on freedom of expression must strictly and cumulatively comply with the requirements of legality, legitimacy and necessity and proportionality, and that failure to comply with any of them renders the measure incompatible with the ICCPR. Available at: <https://docs.un.org/en/ccpr/c/gc/34> (accessed December 2025). Similarly, the Inter-American Court of Human Rights (IACtHR) has reiterated that restrictions on the rights protected by the American Convention must be exceptional, clearly defined and must not render the right in question meaningless. See, for example, Advisory Opinion OC-5/85. Available at: https://www.corteidh.or.cr/docs/opiniones/seriea_05_ing.pdf (accessed December 2025).

3.5 TRANSPARENCY AND ACCESS TO PUBLIC INFORMATION

National legislation on access to public information⁴¹ establishes obligations regarding active and passive transparency that are central to the oversight of surveillance policies, as they enable scrutiny of the technologies being procured, their purposes, and the regulatory frameworks and institutional safeguards under which they fall. However, the current Argentinian administration has taken a step backwards in this regard by introducing regulations that restrict the scope of the law by extending the scope of exceptions and allowing information to be withheld on broader grounds.⁴²

3.6 NON-BINDING INTERNATIONAL STANDARDS AND RECENT DEVELOPMENTS

In addition to legally binding instruments, there are other non-binding international standards relevant to the analysis of surveillance technology use. In this respect, UNESCO has driven multilateral processes aimed at promoting the ethical use of automated technologies and artificial intelligence with a rights-based approach. Argentina has not only actively participated in these processes in recent years but has also developed guidelines and regulatory resources that align with UNESCO's Recommendation on the Ethics of Artificial Intelligence.⁴³ The Argentinian state was also a signatory to the Declaration of Santiago,⁴⁴ adopted at the Forum of High Authorities on the Ethics of Artificial Intelligence in Latin America and the Caribbean, held in October 2023, just a few months before the change of government. However, the government of Javier Milei did not subscribe to the Declaration of Montevideo, the document resulting from the second ministerial meeting held in Montevideo in October 2024.⁴⁵

Building on the above, the following chapter provides an analysis of the policies implemented by the new government, with particular attention to the use of surveillance technologies, the regulations governing them and the impact of these technologies on the exercise of human rights.

⁴¹ Law 27.275, available at: <https://www.saij.gob.ar/LNS0006235> (accessed in December 2025).

⁴² Decree 780/2024. For more information on the regressive exceptions contained in the Decree, see, for example: Civil Association for Equality and Justice (ACIJ): <https://acij.org.ar/el-poder-ejecutivo-reglamento-de-forma-restrictiva-y-regresiva-el-derecho-de-acceso-a-la-informacion-publica/> (accessed December 2025).

⁴³ UNESCO, Argentina implementa normativa en base a la Recomendación sobre la, 19 June 2023, <https://www.unesco.org/es/articles/argentina-implementa-normativa-en-base-la-recomendacion-sobre-la-etica-de-la-inteligencia-artificial> (accessed on 10 July 2026).

⁴⁴ Available at: https://minciencia.gob.cl/uploads/filer_public/40/2a/402a35a0-1222-4dab-b090-5c81bbf34237/declaracion_de_santiago.pdf (accessed December 2025).

⁴⁵ See: https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-conocimiento/sites/agencia-gobierno-electronico-sociedad-informacion-conocimiento/files/documentos/noticias/ENG_Montevideo_Declaration_approved_0.pdf (accessed December 2025).

4. HUMAN RIGHTS IMPACTS OF SURVEILLANCE TECHNOLOGIES

In light of the international human rights principles and standards set out above, it is necessary to address a number of the structural characteristics of these technologies that raise specific human rights concerns, particularly when they enable the collection, integration and processing of large volumes of personal data, the automation of identification or classification procedures, the establishment of links or behaviours, and the enhancement of the state's ability to monitor the population.

These technologies are not neutral. Their design, the data sources they use, the criteria applied in their operation and the contexts in which they are deployed can directly or indirectly affect rights such as privacy, freedom of expression, freedom of peaceful assembly and association, equality and non-discrimination, as well as access to information and guarantees vis-à-vis the arbitrary exercise of power by the state. Furthermore, their use is often characterized by a lack of transparency, difficulties in supervision, reliance on private providers and limited opportunities for the individuals affected to control or challenge them.

Before examining the technologies acquired or used by the national government in detail, the main human rights risks potentially posed by the deployment of the three types of technology relevant to this analysis are outlined.

4.1 IMAGE RECOGNITION AND BIOMETRICS

Image recognition and biometrics technologies can process people's physical or behavioural traits, such as their face, fingerprints, voice or certain body patterns, with the aim of identifying individuals, verifying their identity or tracking their movements in different environments. Facial recognition technology applied to video surveillance cameras can convert visual records of public spaces into individualized identification and tracking mechanisms, enabling persistent and large-scale surveillance of groups and individuals.

It is important to distinguish between the different types of facial recognition, which typically come in the form of 1:n (facial recognition for *identification*, or *one-to-many*), or 1:1 (facial recognition for *authentication* or *verification*, or *one-to-one*). Amnesty International's research, including this briefing, focuses on facial recognition for identification. This is because facial recognition technology for identification is built upon mass surveillance by design (as previously established by Amnesty International), and its use creates

impermissible violations of the rights to privacy, equality and non-discrimination, as well as associated human rights, including freedom of peaceful assembly and association.⁴⁶

Facial recognition for identification can be either real-time or used retrospectively. The former operates simultaneously with image capture, identifying or verifying the identity of individuals as they move through public spaces and enabling the security forces to respond immediately. Retrospective systems (or *ex post* systems) analyse previously captured images or audiovisual records, such as security camera footage or photographs and videos from social media, to identify individuals after an event has occurred. While often presented as forensic investigative tools, these systems also significantly expand the state's identification and retrospective tracing capabilities, particularly when combined with mass biometric databases or facial search engines created using images scraped from the internet.

These technologies are particularly sensitive because they are based on the use of biometric data, which is intimately linked to a person's identity. Using this data can seriously affect the right to privacy and personal data protection, as well as freedom of movement, freedom of expression and the right to protest, particularly when it enables individuals to be identified at demonstrations, meetings or other political activities. In addition, there are issues around lack of transparency, wrongful identification, algorithmic bias and the risk of discrimination, particularly when the systems are trained with data that is not representative of the people they are targeting, or when they are used on groups that have historically been subject to practices of selective surveillance. Even when the technology "works" on a technical level, Amnesty International's research has shown that law enforcement officers can be quick to target and harass protestors, and the technology risks reinforcing existing patterns of discriminatory policing.⁴⁷

The case of the Fugitive Facial Recognition System in the city of Buenos Aires is a clear example of the potential for abuse by government in the absence of effective safeguards or clear regulations on audit and reparation measures. As detailed in section 2.2, the system operated with low-quality data that was not up to date, and the government used it to track individuals for whom no arrest warrant had been issued, while not having implemented the necessary control mechanisms.

As for case studies outside Latin America, Amnesty International has documented a number of contexts within its *Ban the Scan* campaign.⁴⁸ Investigations show that facial recognition not only expands state surveillance capacity, but has been used in specific contexts to identify, track and arrest individuals, including protesters and activists. In cities such as New York, the repeated large-scale use of these tools by the police has been documented in investigations which revealed that the technology was frequently used arbitrarily on protestors.⁴⁹ The investigation also revealed that facial recognition exposure is asymmetrically centred on historically marginalized, and in particular, racialized communities.⁵⁰ In other cases, such as Hyderabad,⁵¹ the deployment of mass video surveillance infrastructures integrated with real-time facial recognition has been carried out in the absence of adequate regulatory frameworks, significantly expanding the state's monitoring capacity without sufficient guarantees. The Command-and-Control Centre in Hyderabad supports the processing of data from up to 600,000 cameras at once, with the possibility to increase this scope much further across the region. These cameras can be used in combination with Hyderabad Police's existing facial recognition software to track individuals.⁵² Finally, in contexts such as the Occupied Palestinian Territories, these technologies have been used as part of broader systems of population control, facilitating forms of permanent and differentiated surveillance that directly impact the rights of Palestinians, including through arbitrarily restricting the right to freedom of movement, and violating the rights to privacy and equality and non-discrimination.⁵³

⁴⁶ Amnesty International, Ban the Scan, <https://banthescan.amnesty.org/>

⁴⁷ Amnesty International, USA: Facial recognition technology reinforcing racist stop-and-frisk policing in New York – new research, 15 February 2022, <https://www.amnesty.org/en/latest/news/2022/02/usa-facial-recognition-technology-reinforcing-racist-stop-and-frisk-policing-in-new-york-new-research/> (accessed on 17 July 2026)

⁴⁸ See: <https://banthescan.amnesty.org/nyc/index.html>

⁴⁹ Amnesty International, USA: Facial recognition technology reinforcing racist stop-and-frisk policing in New York – new research, 15 February 2022, <https://www.amnesty.org/en/latest/news/2022/02/usa-facial-recognition-technology-reinforcing-racist-stop-and-frisk-policing-in-new-york-new-research/> (accessed on 17 July 2026)

⁵⁰ Amnesty International, Amnesty International, S.T.O.P. Lawsuit Reveals NYPD Surveillance Abuses, 13 November 2025, <https://www.amnesty.org/en/latest/news/2025/11/amnesty-and-s-t-o-p-reveal-nypd-surveillance-abuses/> (accessed on 17 July 2026)

⁵¹ Amnesty International, "India: Hyderabad 'on the brink of becoming a total surveillance city'", 9 November 2021, <https://www.amnesty.org/en/latest/news/2021/11/india-hyderabad-on-the-brink-of-becoming-a-total-surveillance-city/> (accessed on 10 July 2026).

⁵² Amnesty International, India: Hyderabad 'on the brink of becoming a total surveillance city', 9 November 2021, <https://www.amnesty.org/en/latest/news/2021/11/india-hyderabad-on-the-brink-of-becoming-a-total-surveillance-city/> (accessed on 17 July 2026)

⁵³ Amnesty International, *Automated Apartheid: How facial recognition fragments, segregates and controls Palestinians in the OPT*, 2 May 2023, <https://www.amnesty.org/en/documents/mde15/6701/2023/en/>

Amnesty International has concluded that facial recognition technologies for identification and mass surveillance are fundamentally incompatible with international human rights law and must therefore be banned.⁵⁴

4.2 CRIME PREDICTION AND DETERMINATION OF SURVEILLANCE AREAS

Technologies used for crime prediction and the determination of areas to surveil and police, rely on large volumes of data and algorithmic techniques to identify patterns, establish correlations and predict potential future behaviours, areas considered at risk, and individuals who could be of interest to law enforcement. Although usually presented as tools aimed at optimizing resources and preventing crime, they introduce classification and anticipation mechanisms that can influence state decisions with significant human rights impacts on individuals and territories.

Police forces have been recording information for decades, such as where arrests are made, who is arrested, and which neighbourhoods are subject to the most patrols. A crime prediction algorithm processes this historical data to identify patterns and produces two types of results: maps showing “at-risk” areas, where the system estimates there is a higher probability of a crime occurring, and individual risk scores showing the probability of a person committing or being the victim of a crime. However, the critical problem is that historical data is not neutral but reflects law enforcement agencies’ own past decisions. For example, if more patrols were historically carried out in poor neighbourhoods or if more people from certain groups were arrested, the system would register these areas or these population groups as “risk zones” or “risk profiles”, and not the areas where more crime actually occurs. The algorithm learns from this history and predicts more crime in the same places and from the same people. More police are deployed there, leading to more arrests and generating new data that feeds the next prediction. Thus, the system creates a negative feedback loop that detects not where crime is occurring but rather consolidates and amplifies areas where the police were already intervening.

From a human rights perspective, these technologies are cause for concern because they tend to be based on historical data that is institutionally biased, which in turn reinforces previous practices of police discrimination, area-based stigmatization and structural discrimination. In this way, they perpetuate and exacerbate inequality, particularly when they associate risk with specific neighbourhoods, social groups or personal characteristics. Furthermore, their operation is often difficult to audit and explain due to opacity in terms of information related to precisely what systems are used, their technical specification, their legal justification, and their ingestion of sensitive databases. This is typically a result of exemptions used by law enforcement to undercut data protection law. This hinders oversight, accountability and the ability to challenge decisions that affect rights. Their use, therefore, requires particularly strict scrutiny, as such systems have been documented to violate the principles of legality, necessity and proportionality, in perpetuating discrimination. Amnesty International has previously called for a prohibition on predictive policing.⁵⁵

In the report “Automated Racism”,⁵⁶ published in 2025, Amnesty International has documented the impacts of these systems and shows that at least 33 police forces in the United Kingdom have used prediction, profiling or risk assessment systems that are based on data from the police and criminal justice system itself. Such data reflects structural practices of discrimination and institutional bias. For example, police intelligence records and information on arrests, checks or searches tend to overrepresent certain groups and territories as a result of prior selective surveillance practices. As a result, algorithmic systems developed using this data tend to predict a higher probability of crime in the same areas or assign a higher risk to individuals belonging to specific groups, in particular racialized groups and historically marginalized communities, directing new police interventions towards them. This creates feedback loops in which the data produced by the actual police activity reinforces new biased predictions, structurally exacerbating discrimination and criminalization.

A particularly relevant precedent of these policies in the region is the Urban Crime Prediction System, implemented in Chile. A recent study by a local NGO shows how the adoption of crime prediction

⁵⁴ Amnesty International, Ban the Scan, <http://banthescan.amnesty.org>

⁵⁵ Amnesty International, *Automated Racism: How police data and algorithms code discrimination into policing*, 1 February 2025, <https://www.amnesty.org.uk/knowledge-hub/all-resources/automated-racism-report/> (accessed on 10 July 2026).

⁵⁶ See Amnesty International, *Automated Racism*.

technologies can reinforce existing inequalities.⁵⁷ The study found that the system was built mainly on two data sources: police cases linked to crimes of major social significance and information from the AUPOL digital database, operated by the *Carabineros* (Chilean national police), which contains the personal data of victims, witnesses and whistle-blowers (including name, identification number, address, gender and profession). However, this data is not neutral, as it reflects institutional and social considerations that may incorporate errors, arbitrary practices or systematic bias. The result is the construction of a system that tends to reinforce patterns of surveillance in already stigmatized areas, perpetuating preventive identity checks and other discriminatory practices without clear independent audit or impact assessment mechanisms.

4.3 SOCIAL MEDIA REVIEW AND OPEN-SOURCE INTELLIGENCE (OSINT)

Social media review and open-source intelligence (OSINT) tools enable the collection, combination and processing of information from online sources, including social media posts, websites, forums, public databases and other open digital resources. While this information is already publicly available, its automated processing on a mass scale qualitatively changes its scope, by making it possible to trace movements, map connections between individuals, identify patterns of behaviour and generate profiles or assumptions regarding activities, opinions, interests or social relationships.

These capabilities are concerning because they greatly enhance the state's ability to intrusively monitor people's social and political lives without the need to resort to traditional measures. In particular, they can affect the right to privacy, freedom of expression and freedom of peaceful assembly and association, as well as facilitate the profiling or targeted surveillance of journalists, activists or those critical of the government. In this regard, the Special Rapporteur for Freedom of Expression of the IACHR has warned, in their report "The Impact of Digital Surveillance on Freedom of Expression in the Americas", that states in the region are increasingly relying on "cyber patrolling" and online profiling using advanced open-source intelligence tools to create new forms of mass surveillance aimed at monitoring and, in some cases, repressing critical voices. According to the information compiled, these practices include the contracting of private services to provide social media monitoring, the characterization of individual users based on their views of the government, and the use of fake profiles by security forces to engage with users of digital platforms.⁵⁸

⁵⁷ Derechos Digitales, Sistema predictivo del delito urbano – Inteligencia artificial e Inclusión en América Latina, <https://ia.derechosdigitales.org/en/casos/chile-sistema-predictivo-del-delito-urbano/> (accessed on 10 July 2026).

⁵⁸ Inter-American Commission on Human Rights, The Impact of Digital Surveillance on Freedom of Expression in the Americas, September 2025, <https://www.oas.org/en/iachr/expression/reports/vigilanciarelecidh.pdf>

5. SURVEILLANCE POLICIES AND TECHNOLOGIES: A NEW PARADIGM

Since taking office in December 2023, the current government in Argentina has created an infrastructure aimed at increasing its capacity for surveillance and control over public spaces –both physical and digital – implemented through executive decrees and resolutions without the participation of the National Congress. This infrastructure has been established through the creation of new government agencies, the publication of specific protocols for federal law enforcement, the restructuring of the National Intelligence System, budget allocations, and a series of procurements and contracts aimed at implementing these new functions and objectives.

These government actions can be divided into two categories. On the one hand, the institutional reforms necessary to provide the foundations on which the surveillance system will operate; on the other, the creation of the operational and material conditions needed to carry out surveillance and control activities effectively.

5.1 EXPANDING THE SCOPE OF THE INTELLIGENCE SYSTEM AND FEDERAL LAW ENFORCEMENT

The government pushed through reforms of two of the main institutions involved in investigating federal crimes: the intelligence systems and the federal security forces. A detailed analysis follows of what these reforms entailed and how they expanded and enabled new powers for internal surveillance.

5.1.1 REFORM OF THE NATIONAL INTELLIGENCE SYSTEM

In July 2024, the government carried out a comprehensive reform of the National Intelligence System (SIN),⁵⁹ the official name for Argentina's intelligence community. The SIN was created in 2001, and its current structure is the result of amendments introduced by decrees 614 and 615 of 2024,⁶⁰ and 941 of

⁵⁹ Law 25.520 on National Intelligence. Available at: <https://servicios.infoleg.gob.ar/infolegInternet/anexos/70000-74999/70496/norma.htm> (accessed December 2025).

⁶⁰ Decrees 614/2024 and 615/2024. Available at: <https://www.boletinoficial.gob.ar/detalleAviso/primera/310495/20240716> and <https://www.boletinoficial.gob.ar/detalleAviso/primera/310496/20240716> (accessed December 2025).

December 2025.⁶¹ In just two years in office, the new government carried out two structural reforms of the SIN.

Decree 941/2025 is critical in establishing the groundwork for internal surveillance by separating cybersecurity, which no longer falls under the SIN,⁶² from cyber-intelligence, which remains under the SIN.⁶³ In addition, it (i) significantly expands the scope of intelligence and counterintelligence functions through the use of broad and ambiguous definitions that could lead to the surveillance of individuals or organizations under an expansive framework; (ii) establishes secrecy as the general rule for intelligence activities, undermining transparency and accountability; (iii) strengthens the institutional capacity to access information held by other public agencies and centralize large volumes of personal data without robust judicial oversight; (iv) enables information transfers between agencies, potentially including foreign agencies, thereby increasing the risk of onward transfers and gaps in accountability; (v) authorizes the “apprehension” of individuals by intelligence agents without judicial control; and (vi) expands the role of the armed forces in intelligence operations. These measures have been enacted through an emergency decree (DNU) without legislative debate, raising serious constitutional objections and concerns regarding the rule of law.⁶⁴

This reform established the Federal Cyber-intelligence Agency (AFC – Agencia Federal de Ciberinteligencia), a new agency specifically dedicated to intelligence in the digital sphere. As provided in Article 9 of Decree 941/2025, this agency will be responsible for “the production of National Intelligence concerning actors, events, risks, opportunities, and threats arising in the cyberspace and radio spectrum domains that may affect national security, critical digital infrastructure, the assets of the National State, technological sovereignty, and/or the integrity of public and private information”.⁶⁵ The broad definitions of the agency’s functions, added to the general reforms detailed in the previous paragraph, raise concerns that a wide range of activities will be enabled, including the surveillance of the population through digital means.

5.1.2 REFORM OF THE FEDERAL POLICE STATUTE

A second legislative initiative also contributed hugely to laying the groundwork for state surveillance in Argentina. In June 2025, the Federal Police statute was amended to,⁶⁶ among other things, create a new investigative division known as the Federal Department of Investigations (DFI). The reform contains provisions enabling the Federal Police to monitor social media and other open digital sources without judicial authorization, enshrining “cyber patrolling” as an official function.⁶⁷ The decree also establishes processes for updating the police force, based on “modernizing protocols, processes and structural mechanisms, in particular those related to investigations” and “acquiring and using Information and Communication Technologies and Forensic Technology effectively” (Articles 2d and 2e). This reform, like most of the initiatives analysed, was carried out by decree, without parliamentary debate, under the special powers granted to the executive through Law 27.742 on the Foundations and Starting Points for the Freedom of the Argentinian People of July 2024.

To complement this reform, in July 2025, the Ministry of National Security issued Resolution 828/2025,⁶⁸ establishing the Protocol for the Operation of Digital Undercover and Revealing Agents, a specific framework for the selection, operation and protection of federal law enforcement officers carrying out criminal investigations through fictitious identities in digital environments. The protocol, published in Annex 1 of Resolution 828/2025 of the Ministry of National Security, details a procedure for creating, safeguarding and

⁶¹ Decree 941/2025. Available at: <https://www.boletinoficial.gob.ar/detalleAviso/primera/337032/20260102> (accessed December 2025).

⁶² Decree 941/2025, Article 31.

⁶³ Decree 941/2025, Article 9.

⁶⁴ Decree 941/2025: (i) the concept of “threat” lacks a clear definition in the text. For example, Articles 8 and 9, respectively, provide that the National Counterintelligence Agency and the Federal Cyberintelligence Agency are responsible for conducting intelligence tasks in the face of potential “threats to national security”; (ii) Article 2 of the decree establishes that “All National Intelligence activities carried out are covert by definition...”; (iii) Article 14 creates the National Information Community (CIFN), comprised by bodies from the National Public Administration (NPA – Administración Pública Nacional) and other jurisdictions, which must provide information according to criteria to be established by the State Intelligence Secretariat (Article 17); (iv) the decree, reforming the text of the National Intelligence Law, establishes that “in the course of intelligence activities, or activities to provide assistance or carry out judicial orders, and/or crimes committed in flagrante delicto, intelligence agents may apprehend individuals, in which case they must immediately notify the competent police and security forces” (Article 9).

⁶⁵ Decree 941/2025. Available at: <https://www.boletinoficial.gob.ar/detalleAviso/primera/337032/20260102>. (accessed December 2025).

⁶⁶ Decree 383/2025. Available at: <https://www.boletinoficial.gob.ar/detalleAviso/primera/326993/20250617> (accessed December 2025).

⁶⁷ Article 6 of the new Statute, on the powers of the Argentinean Federal Police, includes: “To carry out, without the need for judicial authorization, crime prevention tasks in digital public spaces, such as open social media platforms, public websites and other open sources, in accordance with the guidelines and guiding principles established for such activities by the corresponding authority.” Article 6.11, Annex to Decree 383/2025, available at: <https://www.boletinoficial.gob.ar/detalleAviso/primera/326993/20250617>

⁶⁸ Available at: <https://www.boletinoficial.gob.ar/detalleAviso/primera/328352/20250715> (accessed December 2025).

ultimately eliminating the fictitious identities and digital “avatars” used during their investigations. Once an agent is appointed, a fictitious biography is created, registered under a unique code and filed as classified (Article 4); if necessary, physical or digital documents are processed through the National Registry of Persons, at the request of the Special Unit (Article 5). The protocol also mandates law enforcement and the Centre for Cyber Synergy (CS5 – Centro de Sinergia Cibernética de las Fuerzas Policiales y de Seguridad Federales) to create and register fictitious digital identities (“avatars”) (Article 11), making them available to digital undercover and revealing agents for use in their investigations. It also provides for a system of regular certification of “highly qualified agents” who could potentially perform these roles in investigations requiring this special technique (Article 12).

5.2 OPERATIONAL ELEMENTS FOR IMPLEMENTING DOMESTIC SURVEILLANCE

The expansion of surveillance capabilities was enabled through measures such as the creation of new departments, the procurement of technology, and the enactment of specific protocols. These measures are driven by a common objective, namely, to build institutional capacity for monitoring protest and digital environments. They are described in detail below.

5.2.1 “ANTI-PICKET” PROTOCOL

One of the first actions of the new government was the publication of the “Protocol for maintaining public order in the face of road blockades” through Resolution 943/2023 (known as the “Anti-picket” Protocol).⁶⁹ Under the pretext of preventing roadblocks during protests, this protocol has served as an instrument to enable federal forces to intervene in protests without the need for a prior court order, by considering these situations to be flagrant crimes by default.⁷⁰

The protocol not only regulates the control of public spaces, but also explicitly incorporates provisions to identify, register and process information. More specifically, it enables: (i) the identification of “perpetrators, accomplices and instigators” through video footage and other digital or manual means, with a priority to register information on leaders and their organizations, and the collection of information on the vehicles used for the transfer of protesters and, (ii) in the case of foreign nationals with temporary residence, the sending of their data to the immigration authority. Finally, (iii) the protocol provides for the creation of a specific register of organizations involved, whether formal or informal, and the number of offenders identified, consolidating an approach aimed at compiling and processing information for purposes that go beyond the immediate management of public order.⁷¹

Published on 15 December 2023, just five days after the government took office, this protocol set the course for the government’s approach to dissent and social protest: using surveillance technologies and deploying federal forces to suppress protests on the streets. Following this initial step, the regulatory framework took on more specific forms in both areas. With regard to surveillance technologies, the government introduced a number of specific measures that are examined in greater detail below. These unprecedented measures will be analysed in terms of how they complement measures for compiling and systematizing information, and how such information is processed.

5.2.2 ARTIFICIAL INTELLIGENCE UNIT FOR SECURITY (UIAAS)

In 2024, the government created the UIAAS,⁷² with the stated aim of preventing, detecting, investigating and prosecuting crime through the use of AI-based technologies.⁷³ This unit falls under the Directorate of Cybercrime and Cyber Affairs (DCAC), and is staffed by officers from the federal police and security forces.

⁶⁹ Available at <https://www.boletinoficial.gob.ar/detalleAviso/primera/300917/20231215> (accessed December 2025).

⁷⁰ Since 10 December 2023, the Ministry of National Security has issued a number of resolutions that violate basic rights. Amnesty International has created a platform to register these government initiatives that serve as a regulatory framework for the government’s repressive system: <https://amnistia.org.ar/disenso-en-riesgo/marco-normativo>

⁷¹ (i) Articles 6 and 7, complemented by Article 8, which provides that the information collected must be sent to the Ministry of National Security; (ii) Article 11; (iii) Article 12 of the Decree.

⁷² Created by Resolution 710/2024 of the Ministry of National Security. Available at: <https://www.boletinoficial.gob.ar/detalleAviso/primera/311381/20240729> (accessed December 2025).

⁷³ Resolution 710/2024 of the Ministry of National Security, Article 3.

The DCAC operates under the supervision of the Advisory Cabinet Unit of the Ministry of National Security (MINSEG – Ministerio de Seguridad) and is one of the most important actors in the system. Its primary responsibility lies in the design of policies and programmes for fighting cybercrime, as well as in coordinating with the federal police and security forces. The responsibilities assigned to the DCAC pursuant to Annex 2 of MINSEG Administrative Decision 340/2024,⁷⁴ reinforce its role in providing technical assistance, planning and inter-institutional coordination, with no direct involvement in operations or investigations. The DCAC participated in the procurement processes for some of the most relevant technologies acquired by MINSEG in 2024 and 2025, such as open-source intelligence (OSINT) tools and facial recognition technologies (FRT).

The resolution creating the UIAAS lists a wide range of functions,⁷⁵ including the use of different technologies for monitoring open social media platforms, applications and websites, analysing big data and online activity, use of facial recognition and real-time image analysis, surveillance using CCTV cameras, drones and other technologies, use of machine learning algorithms to predict crime and detect cyber threats, as well as information processing for criminal investigations and coordination between security forces. Thus, the UIAAS seems to have been conceived as a cross-cutting operational body, but without any mention of external oversight or human rights impact assessments.

Amnesty International submitted two freedom of information requests to the Ministry of National Security in May and December 2025, requesting details regarding UIAAS internal regulations and cooperation with the security forces. The Ministry provided no substantive details in response to the first request other than to state that the regulations were being drawn up, and that the work was being carried out in a coordinated manner with the security forces; the Ministry further stated that the unit was working with the security forces on a strategic evaluation to “optimize the functional dynamics and organizational structure of the UIAAS”.⁷⁶ In response to the second FOI request, the Ministry of National Security stated that the Naval Prefecture, the Prison Service, the Airport Security Police and the National Gendarmerie (four of the five national security forces) “have no active systems or records relating to UIAAS”.⁷⁷ Simply clarifying that agencies do not have active systems linked to the UIAAS does not dispel concerns regarding the unit’s compliance with human rights standards.⁷⁸

5.2.3 “CYBER PATROLLING” PROTOCOL

In May 2024, the Ministry of National Security published the “General Protocol for the Police Prevention of Crime with the Use of Open Digital Sources”,⁷⁹ popularly known as the “Cyber patrolling” Protocol, which formalizes the use of open sources for investigation by federal law enforcement agencies. The protocol grants powers to investigate a wide range of crimes in cyberspace, including threats, harassment, sexual offences, human trafficking, money laundering, terrorism, and the sale of illicit goods. It also covers the search for disappeared persons or individuals wanted by the authorities.⁸⁰ While it refers to the Constitution and the Personal Data Protection Law and the need to uphold both, it includes a vague clause that allows intervention in “any other offence intelligence which may come to light via cyber sphere”,⁸¹ introducing a degree of ambiguity that could lead to discretionary interpretations beyond what is expressly provided for.

⁷⁴ Available at <https://www.boletinoficial.gob.ar/detalleAviso/primera/307616/20240517> (accessed December 2025).

⁷⁵ See Article 4 of Resolution 710/2024.

⁷⁶ Ministry of National Security, Response to FOI request. Note NO-2025-68968733-APN-SSLE#MSG, of 26 June 2025, PDF p. 2.

⁷⁷ Ministry of National Security, Response to FOI request. Note NO-2026-11569659-APN-DNTEI#MSG, of 2 February 2026. PDF p. 1.

⁷⁸ See, for example, this joint FOI request submitted by Amnesty Argentina, CELS, Fundación Vía Libre, ODIA, Access Now, Democracia en Red and ILSED: <https://www.vialibre.org.ar/pedimos-a-bullrich-que-informe-de-que-manera-hara-vigilancia-masiva-a-los-ciudadanos/>

⁷⁹ Resolution 428/2024. Available at: <https://www.boletinoficial.gob.ar/detalleAviso/primera/308291/20240528> (accessed December 2025). Although a similar protocol had previously been approved through Resolution 144/2020, it was repealed two years later by Resolution 720/2022 on the grounds that it had been issued in response to the specific circumstances of the Covid-19 pandemic.

⁸⁰ Resolution 428/2024, Articles 2 and 3.

⁸¹ In the past, other governments in Argentina, from different political parties, also issued protocols for the use of open source intelligence for justified crime prevention tasks. The first was issued in 2018, during the presidency of Mauricio Macri, through the Ministry of National Security (with Patricia Bullrich as minister). Two years later, in 2020, these guidelines were repealed and replaced by a new version, pursuant to the Ministry’s Resolution 144/20. This was under a new administration led by a different political party, opposed to the previous government: that of Alberto Fernández. Fernández repealed the resolution in 2022, leaving the Argentinian government without an open source surveillance protocol until the end of May 2024.

5.2.4 *EX-POST* FACIAL RECOGNITION: PROTOCOL FOR FACIAL RECOGNITION AND COMPARISON

In November 2024, the Ministry of Public Security published the Protocol for Facial Recognition and Comparison.⁸² This document, drafted by specialists from the federal security forces, establishes guidelines for the management of databases and the training of specialist technical staff, as well as operational procedures such as the submission of images for expert analysis or assessment against minimum quality standards. This protocol sets out the agreed working procedures related to the use of facial recognition.

Given the lack of clarity on this issue and the failed implementation of the Fugitive Facial Recognition System in Buenos Aires, which was suspended by the courts, Amnesty International submitted an FOI request with a number of questions. While the government declined to answer most of the questions raised, it did respond on the use of FRT by the security forces, stating that specialist officers from the Argentinian Federal Police, authorized by the courts, use a facial recognition system within the framework of active judicial investigations, adding that “it is not an online system that is permanently live on the streets, but works with evidence arising from ongoing judicial investigations”.⁸³ The response goes on to state that it is important to note that “the use of the system is carried out *ex post*... In this sense, the analysis carried out by the software is merely an indicator and/or element that the specialist will analyse when issuing a technical opinion”.

The government, therefore, acknowledges the use of FRT, but not as part of a continuous monitoring system. Rather, it is used on an “*ex-post*” basis at the request of the competent authority, pursuant to the Protocol for Facial Recognition and Comparison. According to the government response, automated technology serves to support the work of the experts and not as an element for determining the detention of individuals. However, Amnesty International has previously documented how retrospective 1:n facial recognition systems are subject to the same human rights risks and incompatibilities as live facial recognition, and must, as such, be treated with equal concern.⁸⁴ Furthermore, using proprietary company software can cause problems when attempting to audit the system and the operation of the algorithms, as happened in the case of the suspended Buenos Aires system.⁸⁵

⁸² Resolution 1234/2024, available at: <https://www.boletinoficial.gob.ar/detalleAviso/primera/317094/20241119> (accessed December 2025).

⁸³ Ministry of National Security, Response to FOI request. Note NO-2025-68968733-APN-SSLE#MSG, of 26 June 2025, PDF p. 4.

⁸⁴ Amnesty International, “EU proposals too weak to protect us from dangerous AI systems”, 21 April 2021, <https://www.amnesty.org/en/latest/news/2021/04/eu-legislation-to-ban-dangerous-ai-may-not-stop-law-enforcement-abuse-2/>

⁸⁵ For more information on the issue of auditing the SRFP system, see this statement from the Via Libre organization: <https://www.vialibre.org.ar/comunicado-de-prensa-el-reconocimiento-facial-sigue-suspendido-en-buenos-aires/>

6. ANALYSIS OF PROCUREMENTS AND COMMISSIONING OF SURVEILLANCE TECHNOLOGIES

In a further step towards the effective implementation of surveillance operations using digital technologies, the government issued purchase and services orders for an amount in excess of USD 1.2 million dollars, a significant sum in the context of wider austerity measures.

TABLE 2: PROCUREMENT AND COMMISSIONING OF TECHNOLOGY BY THE MINISTRY OF NATIONAL SECURITY⁸⁶

ID ⁸⁷	DATE PROCURED	DESCRIPTION	PROCUREMENT TYPE	AMOUNT IN USD
NAC-01	29/10/2025	Procurement of Clearview AI facial recognition software	Direct award	33,500
NAC-02	15/10/2025	Procurement of OSINT Maltego platform licence	Direct award	239,013
NAC-04a	28/08/2024	Procurement of compact drones for Public Security	Public tender	551,685
NAC-04b	19/09/2024			
NAC-05a	1/12/2025	Procurement of drone ground control stations	Public tender	391,325.00
NAC-05b	23/12/2025			

⁸⁶ Detailed information on each of the procurement procedures, together with links to the official procurement platforms, is available in Annex 1 of this report.

⁸⁷ The ID field was created as a methodological reference. Details of the procurement procedures, each with its corresponding ID, can be found in Annex 1.

ID ⁸⁷	DATE PROCURED	DESCRIPTION	PROCUREMENT TYPE	AMOUNT IN USD
NAC-06	13/11/2024	NOSIS credit history information service	Direct award	17,863.79

Source: Prepared by the authors based on information published on the ComprAR platform. See Annex 1 for detailed information on the procurement processes.

These procurements are part of an increased spending on security and a broader restructuring of the state's budgetary priorities. In a context of marked austerity and severe cuts across all areas of social protection, including health, social security, education, housing and food during 2025, the most significant increases in budget expenditure corresponded to the Ministry of Security (29%) and Intelligence (6%).⁸⁸

The scope of each of these procurements, including technical specifications, suppliers, type of procurement and the policy framework in which they are implemented, is analysed below, and structured around the type of technology.

6.1 TECHNOLOGIES PROCURED BY THE NATIONAL GOVERNMENT

6.1.1 SOCIAL MEDIA AND OPEN-SOURCE SURVEILLANCE

The Directorate of Cybercrime and Cyber Affairs (DCAC), which oversees the UIAAS, was involved in the commissioning of software for open-source investigations with a wide range of functionalities,⁸⁹ mainly centred around the Maltego application (Res. MSG 105/2025). According to the technical specifications (PET) for commissioning, this is a comprehensive OSINT platform aimed at strengthening the analysis and research capabilities of the security forces. The software being procured was required to enable the collection, integration, cross-referencing and visualization of large volumes of data from over a hundred open sources, including social media, the deep and dark web, personal and contact details, technical infrastructure, cryptocurrencies, security breaches and cyberthreats, as well as AI-assisted real-time monitoring, complex link analysis, profiling, case documentation and collaboration, usage auditing and evidence management (including messaging). In addition, it had to feature advanced connectivity through pre-configured connectors, integration with intelligence and security systems, and customized connectors as per contractor needs.

This combination of features poses a serious risk of mass surveillance without a court order or notification or consent from the individuals being monitored, which conflicts with Article 19 of the Argentinian National Constitution and the international standards on privacy and freedom of expression already mentioned in this report. Integrating such practices into police action without independent oversight or accountability mechanisms creates an opaque surveillance scenario that can have chilling effects on public discourse and public participation, particularly in contexts of protest or political dissent. Furthermore, these practices can lead to the mass collection of information that is not aligned with the principle of proportionality, as established in the international legal framework (see the three-part test described earlier), due to the type of information collected and the fact that individuals who are not suspected of having committed a crime can also be subject to surveillance.

Open-source surveillance operations may be supplemented by the procurement of additional services, either to perform further surveillance tasks or to address procedural matters relating to administration or communications issues in the relevant jurisdictions. An example is the procurement by the Ministry of the NOSIS service,⁹⁰ provided by an Argentinian company (NOSIS) that collects, processes and markets credit, commercial and asset information on individuals and companies. Its services are mainly used to assess credit risk and verify business background, as stated in the PET for the purchase process.

⁸⁸ Ministry of Economy, *Presupuesto Abierto. Sitio del ciudadano* [Open budget. Citizens' site], available at: <https://www.presupuestoabierto.gob.ar/sici/>

⁸⁹ Awarded by Resolution 105/2025 of the Ministry of Security. Available on the procurement process website: <https://comprar.gob.ar/PLIEGO/VistaPreviaPliegoCiudadano.aspx?qs=BQoBkoMoEhzoP5YumD%7C%7C4hV7IltKylInARzyvwBVeJ9/G8if3%7CnkZcQqA6MdIUlOeGIXtThiSv3Daj5fr3fg/eFloYhbKzCfni6kfa7RCrZ436YqOP5pi6vhE6tMK9DsB7H1eDnkwGW1WcLgVhKfA9%7Cpsfor6LCL>

⁹⁰ Procured under Provision number DI-2024-124849263-APN-SSGA#MSG.

6.1.2 IMAGE PROCESSING WITH FACIAL RECOGNITION TECHNOLOGY

The use of facial recognition technology by the security forces raises serious human rights concerns. These tools involve the processing of sensitive biometric data and can affect privacy, personal data protection and due process safeguards, especially when implemented without sufficient control and transparency mechanisms. The specific technologies procured are discussed in detail below.

On 20 October 2025, the Ministry of National Security opened a direct procurement process for a “facial recognition licence to support investigations within the framework of the ForCIC”, with the aim of “instantly identifying a person through a photograph”.⁹¹ The ForCIC is the Programme to Strengthen Cybersecurity and Cybercrime Investigation, operating under the DCAC, which was also involved in the procurement process. The technology acquired is the Clearview AI software, and it was acquired also, among others, by the Public Prosecutor's Office of the Autonomous City of Buenos Aires (MPFCABA)⁹² and the Government of the City of Buenos Aires, who acquired the service in November 2025.⁹³

As Clearview states on its website,⁹⁴ the company has developed a platform powered by facial recognition technology that “includes the largest known database of 70+ billion facial images sourced from public-only web sources, including news media, mugshot websites, public social media, and other open sources”. This platform, the description continues, is aimed at “empowering” agencies to “gain intelligence, disrupt crime, and enhance public safety by revealing leads, insights and relationships, aiding investigators in solving both simple and complex crimes”.

However, Clearview's practices have been challenged in multiple countries, where it has been fined and, in some cases, banned due to the mass exploitation of personal data, upon which its operations depend. In Europe, data protection authorities in countries such as France, Italy, the Netherlands, Austria and Greece imposed fines on the company for violating various articles of the European General Data Regulation (GDPR).⁹⁵ For example, in France, the data protection authority imposed a fine of EUR 20 million and ordered the cessation of its activities due to its unlawful processing of biometric data, in particular, the collection and use of facial images obtained from multiple websites without a valid legal basis, and also ordered the deletion of personal data already collected of people residing in the country. In the Netherlands, Clearview AI was fined EUR 30.5 million by the national data protection authority (*Autoriteit Persoonsgegevens*) for the unlawful collection and processing of personal and biometric data for facial recognition purposes, without a valid legal basis. The authority also ordered the cessation of ongoing violations through enforcement orders under warning of additional sanctions.

However, this product is not only controversial for its problematic processing of personal data. In October 2025, the Business and Human Rights Centre (CEDH) published an article about the use of Clearview to identify and detain students involved in pro-Palestinian protests.⁹⁶

Clearview's non-compliance with international data protection regulations, as well as the lack of transparency with which it operates, led various European organizations to step up their demands.⁹⁷ Added to this are the sustained demands of civil society organizations, which have documented direct impacts on human rights

⁹¹ According to information contained in the PET. Award confirmed by Provision 75/2025 of the Ministry of Security. Available on the procurement process website:

<https://comprar.gob.ar/PLIEGO/VistaPreviaPliegoCiudadano.aspx?qs=BQoBkoMoEhMnJfhTnfzqmq2csat2luK//I95vshX6TtCLuptwo9rlzhnoTMKNIpboD5me/KOrfo0IZVztlKn7APcYQCSPTguP6Cj88WhwziHnXaRQpew=> (accessed December 2025).

⁹² Direct award approved through Provision OAF 36/2025 of the MPF (Public Prosecutor's Office) in June 2025. Available at: <https://mpfcibad.gob.ar/storage/archivos/29fa8b177881168fc41dcf9979f63f08.pdf> (accessed December 2025).

⁹³ Purchase Order 347-0095-OC25. Process available at:

<https://www.buenosairescompras.gob.ar/PLIEGO/VistaPreviaPliegoCiudadano.aspx?qs=BQoBkoMoEhWLUetZJKeBjz2KRumWQOnwu7F2M9pcCyTbVr1XyIUksxomSCR3RSwouOleCfn1E8FaOnzyd2OZBALysYLCw6kuiYeCX7rRo4M%2fMbE6j6pYzPQwu9EquMSy96BILTrM2civDINs6ozRydT21DcoPNx4uUr6Bhw8IKItZY6QgoQQnZkG7pPAvAT> (accessed December 2025).

⁹⁴ Source: <https://www.clearview.ai/overview>. Accessed December 2025.

⁹⁵ The cases are available on the *European Data Protection Board* website:

-France: https://www.edpb.europa.eu/news/national-news/2023/facial-recognition-french-sa-imposes-penalty-payment-clearview-ai_en

-Italy: https://www.edpb.europa.eu/news/national-news/2022/facial-recognition-italian-sa-fines-clearview-ai-eur-20-million_en

-Austria: https://www.edpb.europa.eu/news/national-news/2023/decision-austrian-sa-against-clearview-ai-infringements-articles-5-6-9-27_en

-Netherlands: https://www.edpb.europa.eu/news/national-news/2024/dutch-supervisory-authority-imposes-fine-clearview-because-illegal-data_en

-Greece: https://www.edpb.europa.eu/news/national-news/2022/hellenic-dpa-fines-clearview-ai-20-million-euros_en

(accessed December 2025).

⁹⁶ Samantha Maldonado, “NYPD Bypassed Facial Recognition Ban to ID Pro-Palestinian Student Protester,” *The City*, July 18, 2025, reproduced by Business & Human Rights Resource Centre, “USA: Pro-Palestinian Protester Arrested Due to Facial Recognition Tool and No Clear Accountability for Misuse,” accessed July 30, 2026, <https://www.business-humanrights.org/en/latest-news/usa-pro-palestinian-protester-arrested-due-to-facial-recognition-tool-and-no-clear-accountability-for-misuse/> (accessed December 2025).

⁹⁷ The Vienna-based organization noyb filed a criminal complaint against Clearview AI and its executives in October 2025. See: <https://noyb.eu/en/criminal-complaint-against-facial-recognition-company-clearview-ai> (accessed December 2025)

and have initiated strategic litigation.⁹⁸ According to a report published in December 2025 by Privacy International (PI), these serious, systematic and cross-border violations are leading some jurisdictions to explore criminal liability mechanisms, considering that fines under the GDPR are insufficient to deter business practices based on the mass exploitation of biometric data.⁹⁹ The Privacy International report mentions the start of operations in Argentina as one of the worrying steps in the development of the company, which, far from addressing the concerns raised, seeks to continue to expand its operations.

This report does not have evidence to state how or under what framework the Clearview licences are used for facial recognition in national security activities in Argentina, given that the Ministry of National Security did not provide specific information on companies or suppliers when reporting the use of facial recognition technologies by the Federal Police.¹⁰⁰

CLEARVIEW AI'S HUMAN RIGHTS RESPONSIBILITIES

Companies have a responsibility to respect all human rights wherever in the world they operate and throughout their operations. This is a widely recognized standard of expected conduct as set out in international business and human rights standards, such as the UN Guiding Principles on Business and Human Rights (UN Guiding Principles).¹⁰¹ These standards make clear that the corporate responsibility to respect human rights is independent of a state's own human rights obligations and exists over and above compliance with national laws and regulations protecting human rights.¹⁰²

UN Guiding Principle 13 outlines that companies' responsibility to respect human rights entails a requirement to "avoid causing or contributing to adverse human rights impacts through their own activities, and address such impacts when they occur; and seek to prevent or mitigate adverse human rights impacts that are directly linked to their operations, products or services by their business relationships, even if they have not contributed to those impacts". To meet their corporate responsibility to respect human rights, all companies, including those in the tech sector, should have in place ongoing and proactive human rights due diligence processes to identify, prevent, mitigate and account for how they address their impacts on human rights.¹⁰³

In the context described in this report, what this means is that all of the companies supplying surveillance technology to the Argentinian authorities should be conducting human rights due diligence to assess whether there is any risk of their products or services contributing to or being linked to human rights abuses, and then if they identify a risk, to take action to prevent those abuses from happening.

There is little doubt that before entering into a contract with Argentina, Clearview AI employees knew or should have known about human rights risks arising from its business operations, including in Argentina. This is on the basis of information included in this report and previous Amnesty outputs on facial recognition outlining the incompatibilities of the technology with international human rights law, as well as the multiple enforcement and legal challenges brought against Clearview AI. However, to Amnesty International's knowledge, Clearview AI has not to date carried out a public, transparent and ongoing human rights impact assessment, nor demonstrated that the company has addressed any potential or actual adverse human rights impacts that their business products or activities may cause, contribute or be directly linked to in Argentina.

Amnesty International wrote to Clearview on 1 July 2026 outlining human rights concerns related to their products but have not received a response at the time of publication of this report.

⁹⁸ ReclaimYourFace, About Clearview AI's mockery of human rights, those fighting it, and the need for EU to intervene, 28 March 2022, <https://reclaimyourface.eu/about-clearviewai-mockery-human-rights-those-fighting-eu-intervene/> (accessed on 10 July 2026).

⁹⁹ Privacy International, Clearview and the long arm of the law, 17 December 2025, <http://www.privacyinternational.org/long-read/5715/clearview-and-long-arm-law> (accessed on 10 July 2026).

¹⁰⁰ Ministry of National Security, Response to FOI request. Note NO-2026-11569659-APN-DNTEI#MSG, of 2 February 2026. PDF p. 1.

¹⁰¹ This responsibility was expressly recognized by the UN Human Rights Council on 16 June 2011, when it endorsed the UN Guiding Principles on Business and Human Rights (UN Guiding Principles), and on 25 May 2011, when the 42 governments that had then adhered to the Declaration on International Investment and Multinational Enterprises of the OECD unanimously endorsed a revised version of the OECD Guidelines for Multinational Enterprises. See Human Rights Council, Resolution 17/4: Human Rights and Transnational Corporations and other Business Enterprises, 6 July 2011, UN Doc. A/HRC/RES/17/4; OECD Guidelines for Multinational Enterprises, 2011, www.oecd.org/corporate/mne

¹⁰² UN Guiding Principles, Principle 11 including Commentary.

¹⁰³ UNDP, *Heightened Human Rights Due Diligence for Business in Conflict-Affected Contexts: A Guide*, 16 June 2022, <https://www.undp.org/publications/heightened-human-rights-due-diligence-business-conflict-affected-contexts-guide>

6.1.3 DRONES, ROBOTS AND AERIAL SURVEILLANCE

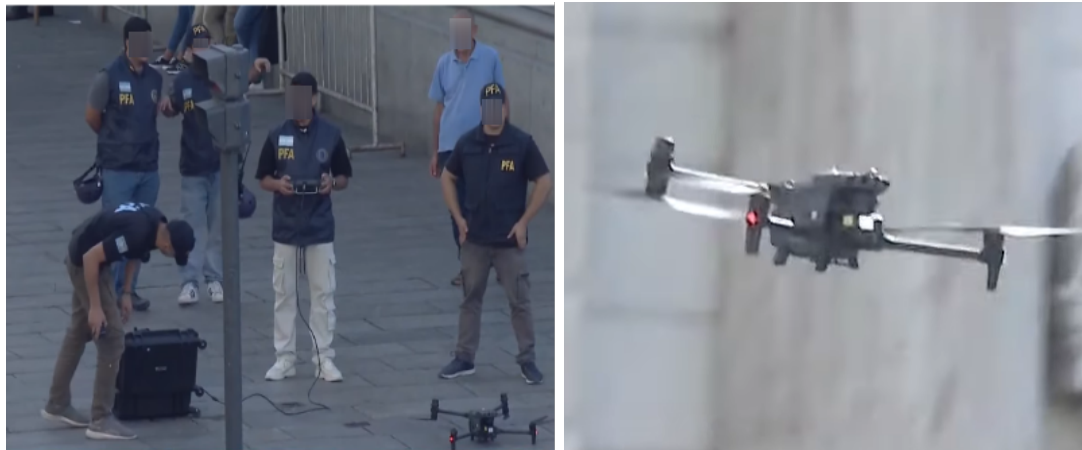
In August 2024, the national government acquired 69 drones, a procurement that was publicly announced by the then Minister of National Security, Patricia Bullrich, one year later, in 2025.¹⁰⁴ The drones are DJI models Matrice 30T and Mavic 3T.¹⁰⁵ Both drone models have artificial intelligence capabilities for the automated surveillance of people and vehicles as well as a thermal camera (as evidenced in the PET used in the procurement process, see Annex 1) that can track the movements of people without their knowledge or consent, making it possible to identify behavioural patterns and profiles, potentially affecting the right to privacy and freedom of movement and having a chilling effect on participation in public spaces.

In mid-December 2025, the Ministry supplemented the purchase of drones with the procurement of eleven tethered unmanned aerial vehicle (UAV) operating ground stations. These two procurements represented an expenditure of close to one million dollars by the Ministry of National Security on the acquisition of drones and associated resources for their use and training of staff (see Table 2 at the start of this chapter).

During the press conference held together with the security forces in September 2025, then Minister of National Security Bullrich, in response to a question from a journalist, said that the drones were not equipped with facial recognition, and that they were intended for use in criminal investigations, not in public demonstrations.¹⁰⁶ However, there is evidence of the use of drones for surveillance during protests on at least two occasions.

The first of these occasions, which was captured on video by a news channel, took place on 19 March 2025 as part of a federal law enforcement operation during a protest at the National Congress, prior to the press conference mentioned above. The images show federal police officers using one of the drones acquired in 2024.

IMAGE 1: DEPLOYMENT OF DRONES BY THE POLICE DURING PROTEST HELD IN FRONT OF THE NATIONAL CONGRESS ON 19 MARCH 2025



Left: Federal police officers operating relevant equipment. Right: The DJI Matrice 30T drone in flight, with the Congress in the background. Source: A24 news channel YouTube account.¹⁰⁷

¹⁰⁴ Press Office, Ministry of National Security (25 September 2025). *La ministra Patricia Bullrich entregó 69 drones de última generación a las Fuerzas Federales* [Minister Patricia Bullrich delivered 69 state-of-the-art drones to the Federal Forces]. Available at: <https://www.argentina.gob.ar/noticias/la-ministra-patricia-bullrich-entrego-69-drones-de-ultima-generacion-las-fuerzas-federales>

¹⁰⁵ Information provided through an FOI request, registered under File EX-2025-140781452-APN-DNPAIP #AAIP.

¹⁰⁶ Video of 25 September 2025. “Bullrich entrega drones de última tecnología a las fuerzas de seguridad [Bullrich delivers state-of-the-art drones to security forces]”, available at: <https://www.youtube.com/watch?v=vleqUppvw9o> (minute 10:15).

¹⁰⁷ Video of 19 March 2025. “Congreso blindado: inhibidores de señal y drones con la seguridad del G20 [Congress protected: signal inhibitors and drones with G20 security]”. Available at: <https://www.youtube.com/watch?v=nNR1AgSg2tE> (minute 6:33).

The second graphic evidence, showing that this is in fact a systematic practice, corresponds to an official video from the Argentinian Federal Police, published on 28 February 2026. In the video “The role of drones in police operations”, police officers show how these devices are used during police operations. What is notable about the video is that it was filmed during a demonstration. Several officers from the Aeronautical video and communications division speak on the video, stating that their role in such operations, including in demonstrations, is to provide images to institutional command, either via 4G transmission using transmission backpacks, or via satellite transmission using *Starlink* antennas.¹⁰⁸ They also claim to have state-of-the-art equipment that affords greater advantages when capturing video footage, thanks to its zoom capability, which facilitates subsequent image processing, facial recognition and identification of individuals.¹⁰⁹ At minutes 0:08 and 2:28, the video shows footage of passers-by with blurred faces, apparently to illustrate the capabilities of this equipment.

These testimonies raise three concerns in relation to the use of drones. First, the response from then Minister Bullrich does not reflect the evidence of the drones acquired being used during demonstrations, both before and after such procurement was officially announced. Second, the evidence does show that these drones do not have facial recognition capabilities; however, as stated by the officer in the video, and as derived from the mentioned FOI requests for information submitted, the images are sent by 4G or satellite transmission to the relevant authorities, who may have facial recognition capabilities for identifying individuals. Finally, there is little to no transparency around how the images that are transmitted in real time are processed and stored. Amnesty International submitted specific requests in this regard, but a response was denied on grounds of national security protection.¹¹⁰

6.1.4 PREDICTIVE ALGORITHMS: TOOLS FOR REINFORCING STEREOTYPES

The use of predictive algorithms and automated profiling systems in public safety operations raises serious concerns from a human rights perspective. These tools, far from being neutral, can amplify structural biases present in the data used, resulting in discriminatory practices, privacy violations, eroding the presumption of innocence and imparting indirect restrictions on freedoms. While there is no detailed information on the procurement of these technologies, the functions of the UIAAS include a specific point in this regard.¹¹¹

The hot spot policing programme implemented by the Ministry of National Security with support from the Inter-American Development Bank in 2017,¹¹² is a particularly noteworthy programme. Although it did not explicitly use artificial intelligence, the programme applied territorial targeting based on historical crime data to allocate police resources. Such strategies, which identify areas with high concentrations of crime and prioritize surveillance in those areas, can contribute to reinforcing existing spatial biases, while normalizing a constant police presence in historically stigmatized neighbourhoods.

These impacts must be seriously considered when designing similar tools that fall within the remit of the UIAAS, particularly if technical standards, exclusion criteria or public accountability mechanisms are not developed at the same time.

¹⁰⁸ Video of 28 February 2026. “*Prevenir: Rol de los drones en los operativos policiales* [Prevention: The role of drones in police operations]”. PFAOfficial (Argentinean Federal Police). Available at: <https://www.youtube.com/watch?v=pRm03XxqlcA> (minute 0:53).

¹⁰⁹ Video cited, minute 2:22.

¹¹⁰ Question: FOI request submitted on 8 May 2025. Question 2.G, page 4 of the PDF. Response: Ministry of National Security, Response to FOI request. Note NO-2025-68968733-APN-SSLE#MSG, of 26 June 2025, page 2 of the PDF.

¹¹¹ Article 4c of Resolution 710/2024: “Use of machine learning algorithms to analyse historical crime data and thereby predict and help prevent future crimes.”

¹¹² Funding for this policy still seems to be in place, under the Federal Security Program, financed by the IDB in the amount of USD 25 million, with the effectiveness of criminal policy data systems playing a crucial role. See: <https://www.iadb.org/en/project/AR-L1255>

6.2 SURVEILLANCE TECHNOLOGIES PROCURED BY THE CITY OF BUENOS AIRES: INCREASED VIDEO SURVEILLANCE CAPABILITIES AND NEW FACIAL RECOGNITION TECHNOLOGY

Expanding surveillance infrastructure in the city of Buenos Aires, in particular in the vicinity of the National Congress, has been a particularly concerning development, as one of the epicentres of social mobilization in Argentina. In this regard, it is worth noting how the infrastructures of these two jurisdictions complement and reinforce one another: the national government procured technology aimed at addressing federal crimes on a national scale, while the GCABA procured tools that enable greater spatial coverage for surveillance within the city. Together, these two layers of technology create a denser and more extensive surveillance network in the Autonomous City of Buenos Aires.

TABLE 3: PROCUREMENT OF SURVEILLANCE INFRASTRUCTURE BY THE GOVERNMENT OF THE CITY OF BUENOS AIRES (GCABA)

ID	YEAR OF ACQUISITION	DESCRIPTION	PROCUREMENT TYPE	AMOUNT IN USD
CABA-01	23/12/2025	Commissioning of video image analysis and alert services	Public tender	4,997,281
CABA-02	06/11/2025	Acquisition of facial recognition (Clearview) and other software	Public tender	828,916
CABA-03	17/10/2025	Electrical maintenance and power supply services for video capture points	Public tender	810,956
CABA-04	02/10/2025	NOSIS credit history information service	Public tender	93,805
CABA-05	23/06/2025	Connectivity service for devices within the video security platform	Public tender	14,184,463
CABA-06	8/5/2025	Acquisition of capture points and hardware and software for processing and storage	Public tender	27,077,219

Source: Based on procurement and commissioning processes published on the Buenos Aires procurement platform (BAC).

Table 3¹¹³ shows the procurement of technologies that do not necessarily represent surveillance as defined in the methodology section of this report, but rather the enabling infrastructure for obtaining and processing images, as well as their maintenance. The amounts are significantly higher than those at the national level, although they relate to different technologies. The city spent nearly USD 48 million on the selected procurements alone.

Expansion of the video surveillance system accounts for more than half of this amount, as can be seen in the table under “Acquisition of capture points and hardware and software for processing and storage”.

According to the local government, the video surveillance system achieved “82% coverage” of the city by July 2025.¹¹⁴ In that year, the government acquired 850 capture points, with a total of 3,400 cameras.¹¹⁵

¹¹³This report analyses the regulatory reforms and technology procurements made by the Argentinean national government and the city of Buenos Aires. It does not seek to provide a comprehensive analysis of how the corporate actors involved comply with human rights. In this regard, allegations are made against Clearview AI only.

¹¹⁴ GCBA (2025). “Jorge Macri supervisó la instalación de 1.200 cámaras para ampliar la vigilancia urbana [Jorge Macri supervised the installation of 1,200 cameras to expand urban surveillance]”. Available at: https://buenosaires.gob.ar/gcaba_historico/noticias/jorge-macri-superviso-la-instalacion-de-1200-camaras-para-ampliar-la (accessed March 2026).

¹¹⁵ The process of acquiring video capture points for the comprehensive video surveillance plan began with the original Purchase Order approved through Resolution 984/MSEGC/24 of 11 October 2024, which contemplated the purchase and installation of 150 units for an amount of USD 2,341,800. Subsequently, Resolution 1186/MSEGC/24 of 11 December 2024 approved a first increase that

Although the information is patchy, there is reason to believe that Danaide provides not only the facial recognition software,¹¹⁶ but also the remaining capture points that were installed in the city of Buenos Aires between 2018 and today.¹¹⁷

The GCBA did not publish official information on the specifications of the cameras installed between 2019 and 2023,¹¹⁸ which would be required to understand the capabilities of these devices for recording individuals in the context of protests in public spaces, for instance. However, as of 2024, the technical specifications (PET) of the 3202-0540-LPU24 Procurement Process provides details on the technical characteristics of bullet (fixed) cameras and PTZ (dome) cameras.

TABLE 4: GCABA REQUIREMENTS FOR VIDEO SURVEILLANCE CAMERAS 2024-2025, AS PER TECHNICAL SPECIFICATIONS IN PROCUREMENT PROCESS 3202-0540-LPU24

FEATURES	FIXED CAMERA	PTZ DOME CAMERA
Main function	Continuous capture over a fixed point	Dynamic surveillance with monitoring and tracking of surroundings
Resolution and sensor	CCD/CMOS sensor, 4K (3840x2160)	12 MP CCD/CMOS sensor, 4K (3840x2160)
Lens / Zoom	Motorized zoom 4–12 mm	Optical zoom ≥ 20x + digital zoom ≥ 12x
Movement	No mechanical movement	360° continuous panning and 0°–90° tilt, high speed
Day / night capacity	Automatic switching to monochrome + IR ≥ 50m	Day/night capture in colour + monochrome
Remote control operation	IP management, multiple flows, ONVIF, remote settings	IP management, multiple flows, ONVIF, presets and tours

Source: Prepared by the authors based on the PET from Procurement Process 3202-0540-LPU24.

Although dome cameras and capture points provide the broadest surveillance coverage across the city, both the national and city governments have also incorporated portable and mobile technologies into their surveillance capabilities. Both jurisdictions acquired drones to strengthen their surveillance capacity. In 2022, the Government of the City of Buenos Aires (GCABA) purchased a total of four drones: two “for complex operations and long-range observation with thermal imaging cameras,” and two for pilot training. These are the resources are used by the city police Drone Squad.¹¹⁹ According to the head of the Police Aviation Department, the squad’s most modern drone is the DJI Matrice 200, which has an auto track system that allows marking and tracking of the vehicle or individual being pursued, recording data on the route taken.¹²⁰

significantly expanded the procurement with 400 additional units for USD 6,244,800. Finally, Resolution 511/MSEGC/25 of 8 May 2025 incorporated a third increase of 300 units for USD 4,683,600. The full process, therefore, consolidated the acquisition of a total of 850 capture points, considering the original purchase with its successive extensions.

¹¹⁶ Commissioning process 2900-0472-CDI19, which was initiated in 2019 and extended in 2020 and 2021, refers in its technical specifications to the “Commissioning of a comprehensive video analysis service”, but the description in the BACompras platform refers to “Video camera installation services for a road surveillance system. The service includes hardware for assembly, minor supplies and labour costs for its proper operation”. The period 2019-2025 saw the greatest expansion in the city’s video surveillance system.

¹¹⁷ In October 2018, following a dispute over the installation of video surveillance cameras outside the home of former president Cristina Kirchner, the provider issued a statement in which it claimed to have installed “some 8,000” cameras on public roads, stating that it was not the company but the clients who decided where the cameras should be installed. The statement was published by a media outlet. Available at: <https://www.infobae.com/politica/2018/11/16/la-empresa-que-acuso-cristina-kirchner-aclaro-por-que-instalaba-camaras-frente-al-edificio-de-recoleta/>

¹¹⁸ The government has so far not provided specific information on the make and model of the devices installed.

¹¹⁹ From Procedure 2900-1001-LPU22, acquired through Resolution RESOL-2022-319-GCABA-SSGA of 14 October 2022.

¹²⁰ GCABA Press Office, 30 January 2023 “*Así funciona el escuadrón de drones de la Ciudad que ayuda a apagar incendios, perseguir a ladrones y encontrar personas perdidas* [This is how the city’s drone squad works to help put out fires, chase down thieves and find missing persons]”. Available at: https://buenosaires.gob.ar/gcaba_historico/noticias/asi-funciona-el-escuadrón-de-drones-de-la-ciudad-que-ayuda-apagar-incendios-perseguir

6.2.1 WHAT DOES THIS LOOK LIKE IN A REAL PROTEST SCENARIO IN BUENOS AIRES?

To analyse the human rights implications of the use of video surveillance cameras with the characteristics described, a specific case can be used as an example, namely the cameras installed in areas around the National Congress and the Avenida 9 de Julio, in the city of Buenos Aires. These two areas have been the scene of many of the most massive protests that have taken place in the period being analysed.

IMAGE 2



Protest in Congress Square (top) and Avenida 9 de Julio (bottom).

Source: TOMAS CUESTA/AFP via Getty Images (top) and ELENA BOFFETTA / AFP via Getty Images (bottom)

Amnesty International, together with local human rights organizations, held a hackathon in October 2025. The event aimed to collaboratively map the coverage of surveillance cameras located in the vicinity of the National Congress and the Avenida 9 de Julio and thus ascertain their coverage as a reference for potential use in facial recognition technologies.¹²¹

¹²¹ In a freedom of information request submitted to the Government of the City of Buenos Aires on 4 February 2026, Amnesty International sought information on the context surrounding the implementation of Clearview AI, whose procurement was documented under Purchase Order No. 3202-0419-OCA25, dated 11 November 2025. In its response, dated 17 March 2026, the Government of the City of Buenos Aires stated that: “Clearview, a technological tool associated with facial recognition, is not currently in use by either

The location was identified as one frequented by civil society during protests in particular and was the reference for establishing the scope and exposure to possible mass surveillance. As Amnesty International has previously documented, through mapping the locations of CCTV cameras,¹²² the potential reach of facial recognition exposure can be established,¹²³ as the technology is frequently paired as software used with cameras.¹²⁴ This method does not make a distinction between facial recognition exposure by whether it is real time or through subsequent processing by the GCABA or the national government in that area. Rather, participants browse the streets in a radius of eight blocks within the National Congress looking for cameras mounted to building and other public infrastructure (e.g. lamp posts, traffic signals, etc.), generating a list of coordinates of discovered cameras. The list is subsequently peer reviewed by participants, and a map generated from the coordinates.

The results of this event made it possible to generate a coverage reference map, as well as a space for discussion and exchange between the participating organizations.

IMAGE 3: MAP OF CAMERAS LOCATED IN THE VICINITY OF THE NATIONAL CONGRESS



  Source: Prepared by Amnesty International and partner organizations based on collaborative work

The map shows an indication of the coverage provided by dome cameras, which are usually mounted on capture points together with fixed cameras. The circles do not represent the specific location of each camera. Places of interest were marked for reference, in black. A range of 35 metres was established for the dome cameras by way of illustration only, given that the specifications listed before would allow greater ranges. For the analysis, a perimeter was drawn to span four blocks to the north, four blocks to the south and four blocks to the west of the Congress building. The limit to the east was increased to reach the Avenida 9 de Julio, one of the potential exit routes for protesters.

Protests usually take place around Congress Square ('Plaza del Congreso' in Image 3), which can be seen in the image to be completely and disproportionately more covered by cameras. There is also full camera

the Government of the Autonomous City of Buenos Aires or the City Police, pursuant to the judicial orders currently in force requiring the suspension of the use of facial recognition systems."

¹²² Sophie Dyer and Matt Mahmoudi, Amnesty International's Citizen Evidence Lab Blog, How We Enrolled Seven Thousand Volunteers to Generate Data the NYPD Wouldn't Publish, 9 September 2021, <https://citizenevidence.org/2021/09/09/decode-surveillance-nyc/> (accessed on 22 July 2026)

¹²³ Julien Cornebise, Swetha Pillai, Martyna Marciniak, and Sophie Dyer, Amnesty International's Citizen Evidence Lab Blog, Decode Surveillance NYC early analysis, 17 November 2021, <https://citizenevidence.org/2021/11/17/decode-surveillance-early-analysis/> (accessed on 22 July 2026)

¹²⁴ Amnesty International, Inside the NYPD's Surveillance Machine, <https://banthescan.amnesty.org/decode>

coverage at different points on the adjacent streets, which are also potential exit routes for protestors, as well as along the previously mentioned Avenida 9 de Julio. This avenue is also one of the main protest locations for social organizations, for example, in connection with the popular economy.

In short, the policies and procurement of technologies by the two jurisdictions are complementary. While the national level creates the ecosystem for state surveillance through the work of federal law enforcement agencies and the intelligence systems, the GCBA has built a level of video surveillance coverage that extends to a large portion of the territory of the city of Buenos Aires.

As mentioned in the previous section, organizations of the universal and regional human rights system have warned of the chilling effect that these technologies and government actions may have on the population.

7. THE CHILLING EFFECT: WHEN THE PERCEPTION OF SURVEILLANCE TECHNOLOGIES AFFECTS PEOPLE'S RIGHTS

This section analyses state surveillance, deterrence, and the chilling effect, looking in particular at the impact of surveillance on the rights to political participation, freedom of expression and freedom of assembly in urban contexts, based on interviews with witnesses.¹²⁵ This chapter examines the different forms of self-censorship and other behavioural changes linked to surveillance and how surveillance, whether real or perceived, affects trust within groups and between organizations, and how this in turn influences their willingness to engage with people or movements deemed to be under surveillance. It also examines how surveillance reduces the capacity of groups to organize, mobilize and take collective action.¹²⁶

The analysis presented below is based on consultations with 21 people, through individual and group interviews, to identify perceptions on and differentiated impacts of the use of surveillance technologies. The interviewees were selected from a range of backgrounds and exposure levels, including students and young persons, pensioners, human rights defenders and a government official, as well as journalists and media workers, one of the sectors most affected by security policies of this type. Given Amnesty International's informed consent policy, some of the testimonies received were anonymized.

¹²⁵ Amnesty International has examined the chilling effects of surveillance technologies on multiple occasions, emphasizing that their existence reflects a failure by states and private actors to comply with their human rights obligations. Where safeguards such as transparency, oversight of abuses, and access to effective remedies are lacking, the perception of being under surveillance fosters widespread mistrust and may directly restrict freedom of expression and the right to privacy. This argument, for example, was presented by Amnesty International to the United Nations Human Rights Council's Special Rapporteur on the rights to freedom of peaceful assembly and of association in a 2025 submission on digital surveillance and chilling effects. Available at: <https://www.amnesty.org/en/documents/ior40/0484/2025/en/>

¹²⁶ The methodology section at the beginning of this report provides a detailed description of the interviews conducted, the selection criteria applied and other information on methods used.

7.1 CHILLING EFFECTS AND BEHAVIOURAL ADJUSTMENTS RESULTING FROM SURVEILLANCE

There is one thing in common amongst all the persons interviewed for this section: all of them expressed that, in some form or other, they have been or are being surveilled or that, at the very least, the authorities know who they are.

“We’ve all been fully identified for a long time now... Sometimes as you’re walking you get to [where you were going] and suddenly you see the drone hovering just above your head. Sometimes within six feet. Why so close? Why is it so invasive?” says Ana Tapia, a member of the Insurgent Pensioners (*Jubilados Insurgentes*) collective. Pensioners march every Wednesday to the National Congress to protest against the pension cuts made by the national government.

Matías Darabós, a member of the Association Against Institutional Violence (ACVI), which, among its other objectives, seeks to record police abuses during protests, states: “There is a very strong feeling that you are being controlled and watched. In fact, when we go to marches to record what goes on, they are constantly pointing at us or filming us.”

Bianca Abella, a freelance photographer, said that police surveillance affects her work:

“The police are always just inches away, with the cameras constantly watching us. And the drones. And it instils fear and mistrust. It makes you doubt your own work many times and disrupts the way you work while out on the streets. It’s quite complicated, at least for us. Quite difficult.”

As described earlier in this report, federal law enforcement agencies currently have a varied range of equipment for video and audio recordings. In response to an FOI request submitted by Amnesty International, government sources confirmed the use of professional video cameras, different types of body cameras and drones.¹²⁷

The interviews showed that there was a perception of increased surveillance against journalists in particular, as one of the groups most affected by the repression.¹²⁸ In the interviews, this situation was analysed particularly by various trade union representatives of media workers. Paula Cejas, director of the Latin America Office of the International Federation of Journalists (IFJ), said:

“We are feeling an increase in surveillance mechanisms focused on journalists. We cannot categorically state that this is the case, but there does seem to be the intent to attack independent and opposition media. There are also mechanisms, such as the Cyber Patrolling Unit, that keep you on constant heightened alert.”

In addition to being the regional director of the IFJ, Cejas is a resident of Buenos Aires, so her perspective is particularly relevant given her knowledge of both the regional circumstances and the more local scenario.

Agustín Lecchi, director of the Buenos Aires Press Union (SiPreBA - Sindicato de Prensa de Buenos Aires), said:

“There was a period of heightened surveillance during the Macri government.¹²⁹ They drew up a basic profile of every person accredited to the G20 by monitoring their social media to assess their political and ideological leanings.¹³⁰ Now we are in a similar situation: [journalists] are monitored on social media and, based on that, subjected to different levels of union or labour persecution. Then, during demonstrations and street protests, there is a particular degree of viciousness and repression against the media.”

Similarly, a journalist specializing in women’s rights and diversity, who will here be called Participant 6, stated:

¹²⁷ Registered under File EX-2025-140781452-APN-DNPAIP#AAIP.

¹²⁸ For more information on the consequences of the repression of social protest and attacks on the press, see this report by Amnesty Argentina, published two years after Javier Milei’s government took office: <https://amnistia.org.ar/noticias/dos-anos-del-protocolo-antipiquetes-mas-de-2-500-personas-heridas-y-una-escalada-de-represion-a-la-protesta> (in Spanish).

¹²⁹ Macri was in office from 10 December 2015 to 9 December 2019.

¹³⁰ Cecchi is referring to the G20 Summit and the WTO conference, international events that took place in Buenos Aires in 2018 and 2017 respectively, during the tenure of Mauricio Macri. In 2020, with the change in the administration, the intelligence agency was investigated and it was revealed that detailed profiles on journalists, human rights defenders and civil society organizations, among others, had been compiled as part of the process for authorizing access to the summit and granting entry into the country. According to a written statement issued by Via Libre Foundation to publicly call out such actions, “the two events enabled the Federal Intelligence Agency (AFI) to carry out mass surveillance of journalists, academics and businesspeople registered as participants, and also to infiltrate left-wing parties organizing protests against the summit.” (Via Libre Foundation, 2020).

“I consider myself surveilled, I don't know how to explain it, it's like I feel I've already been profiled, at least publicly, because I had or have exposure, or a certain level of exposure or whatever. I just assume that someone is watching me, whether that's groups that are opposed to the issues I work on, or the government, or the security forces, or the government's communications apparatus, anyone.”

This was a feeling held not only by those working on human rights issues, but also by some who covered the current government's election campaign and rallies. “Personally, I feel that I've been *fichado*¹³¹ from the word go, because I've been there since Javier Milei's first act as a politician in 2020.” Emilio Laszlo, general coordinator of the streaming platform Gelatina, is referring to his coverage of the current president's election campaign. And he goes on to say:

“I was there when there were 50, 100 people... up until he took over at the Casa Rosada. So I'm in no doubt about it. I have a good relationship with some of them, with others I have none. But I'm sure there's a file on me and on all those of us who go to those places, with our names, our faces and details of where we work.”

Those interviewed offered some speculation on the issue of what the government might do with this information. One of them, an international correspondent who will here be called Participant 4, expressed concern about automated data processing, noting that while not considering themselves an individual surveillance target, the risk increases significantly with the automation of these technologies. They warned that databases of journalists could very easily be built and their activity monitored in real time, making their situation more delicate by reducing the chances of anonymity. In that context, they also expressed concern regarding the political climate, noting that hostile rhetoric against journalists could pave the way for the use of these tools against journalism as a whole.

Similarly, Participant 6 pointed out that, while not having direct evidence of current surveillance, she believes that certain profiles and content are monitored today, aided by technological and AI tools. She also mentioned that she had reduced her public exposure, which influences her perception of current surveillance, though she went on to say that “I do believe there are... companies involved in this and alerts go out” aimed at tracking what certain individuals, such as journalists, publish or share. However, she insisted that she had not had any recent concrete experiences.

Finally, the group of young people expressed concern about the monitoring of social media by government officials. In this regard, one participant mentioned the Ian Moche case, an incident in which government representatives made disparaging remarks about a child with a disability, following his public engagement and activism. “The government is monitoring social media to see what people think,” the participant said.

Thus, there was consensus among those interviewed regarding the perception that the government may have systematic information on individuals or that they may have closely monitored their work. Based on these perceptions, interviewees were asked about any behavioural changes regarding their work and activism. Their responses enable an analysis of whether their rights to freedom of assembly and expression are being affected.

7.2 SHRINKING OF CIVIC SPACE

Responses from those interviewed indicate that the perception of surveillance does have an impact on the rights to freedom of association, assembly and expression, although not across the board.

Ana Tapia, for example, stated that security forces pay special attention to what they do as an organization, but that this does not intimidate them: “We don't stop working, but we do change our strategies.”

Matías Darabós of ACVI was, like Tapia, a victim of police violence, and this has had an impact on his readiness to participate in and monitor demonstrations. “After being kicked [by the police], I stopped going to some of the marches. Before, we used to break up into one or two groups to cover more territory; now we try to stay together. That limits operational capacity.”

This issue also affects those working in the media. “There are colleagues who are now hesitant to take to the streets under the organization's banner. We know that they have all our data, we know that there are colleagues being attacked by the security forces, colleagues who receive threats... and we know that [the authorities] are aware of all of our movements,” says Paula Cejas, IFJ representative for Latin America. She also spoke about how the police presence and repression have brought about a change in the way organizations communicate. “Practices have been modified: some have stopped using WhatsApp and

¹³¹ A term in *Lunfardo*, the urban slang of Buenos Aires, meaning “watched” or “blacklisted/identified”.

switched to Signal or Telegram. Protective gear such as helmets and vests has been handed out, something that had never been done before.” The journalist specializing in gender issues, Participant 6, agreed. She said she was not deterred from going to marches, but she did adopt certain strategies. “I post about it on social media, I tell my family, I talk to colleagues about what to do if everything goes wrong.”

There is a certain conflict between the exposure required as a journalist and the perception of being under surveillance by the security forces. In this regard, Alejo Fraile, a member of the Policing Map, states: “I don’t go to as many marches anymore, only to the mass protests where I know there will be no repression.” The Policing Map is a project carried out by a multidisciplinary collective of activists, in collaboration with human rights organizations and the media. Their work has made it possible to identify police officers responsible for causing injuries to protesters, as in the case of photojournalist Pablo Grillo, who was seriously injured by a tear gas canister fired directly at him, in breach of the relevant protocols. This was verified thanks to a forensic analysis carried out by the collective.¹³²

When asked about the possibility of not going to a protest due to the perception of being under surveillance, a media worker who will here be called Participant 7 pointed out that their decision would not be so much linked to the surveillance issue, but to the actual risk of physical repression. They explained that surveillance feels more abstract, whereas the possibility of direct violence, such as tear gas being used or physical assault, is a more immediate and concrete risk. Personal circumstances, such as being the main breadwinner in the family, influence decisions. Avoiding physical harm is a priority, as it may stop you from working. For this reason, Participant 7 stated having reduced participation in demonstrations, currently attending only for work reasons and prioritizing self-care over other motivations.

The combination of repression and surveillance policies has had a particular impact on migrants. As has been previously mentioned, the so-called “Anti-picket Protocol”¹³³ stipulated that any migrants obstructing traffic during a protest would be reported to the immigration authorities. In this regard, two migrants who participated in the group interview with young people said that they stopped participating for fear of reprisals, such as losing their immigration status.

YOUNG PEOPLE UNDER STATE SURVEILLANCE: STRATEGIES FOR SELF-CARE AND VISIBILITY MANAGEMENT

Although the interviews conducted do not show any clearly differentiated impact of the perception of surveillance based on age, some relevant nuances in the experiences and practices of the young people interviewed can be identified. In general, their perception of surveillance, as well as the strategies they use to address it, are similar to those observed in other interviewees, particularly those active on social, political or gender issues. In this sense, the fact of belonging to activist or rights-based groups appears to have a more differentiated impact than simply age.

Some of the situations of greatest vulnerability identified among the young people interviewed are linked to personal characteristics such as, for example, migrant status, rather than to youth as a specific category. In some cases, these situations had a direct impact on changes in everyday practices, particularly in relation to mobility, public participation and expression in the digital space. In the case of migrants, it was clear that migrant status combined with surveillance policies was a decisive factor in the changes in behaviours of those interviewed.

However, one particularly significant feature can be observed in relation to social media and digital spaces. Several young people interviewed claimed to have reduced what they posted, closed their accounts or toned down their contributions on digital platforms, mainly as a result of harassment, hate messages or threats received online. While these situations were not attributed exclusively to state surveillance, they do appear to be linked to a wider context of exposure and perceived conflict. In this context, the changes observed point not only to self-censorship practices but also to strategies of self-care and selective visibility management, aimed at reducing perceived risks in potentially hostile environments.

Given that social media networks play a central role in contemporary forms of social interaction, expression and political engagement, these changes take on a particular significance for the young people interviewed. In this regard, rather than a differentiated impact associated directly with

¹³² Available at: <https://mapadelapolicia.com/#/investigacion/metodo-pablo-grillo> (accessed December 2025).

¹³³ Approved through Resolution 943/2023 of the Ministry of Security.

surveillance, the testimonies suggest processes of self-care and management of digital visibility in the face of scenarios perceived as potentially hostile.

7.3 SELF-CENSORSHIP AND LACK OF GUARANTEES FOR FREEDOM OF EXPRESSION

The interviews reveal a range of views on this point. For example, photographer Bianca Abella will not stop going to the protests in the face of repression and police surveillance, but she does say:

“The thing is, I need to go and cover these events to show what’s happening; I need to show it, though many times you also take too much care of yourself and that also limits what you want to show. Another limiting factor is that fewer and fewer people are going, or they don’t want me to take pictures of them because they are afraid they will be published somewhere.”

Similarly, Ana Tapia, from the pensioners collective, stated: “I say what I have to say, wherever I am... we mustn’t keep quiet. The last thing we should do is stay silent.”

Agustín Cecchi, from SiPreBa, also pointed out that, in the face of what they perceived as a more repressive context, the union had adopted a more cautious and coordinated approach when participating in protests, but stressed that this did not mean that they would stop demonstrating or substantially modify their public stance or forms of expression.

Two people expressed concern regarding an issue of critical significance to journalists, namely the protection of sources. Paula Cejas, of the IFJ, highlighted the scale of the video surveillance system in the city of Buenos Aires and its potential to monitor and identify people in public spaces. She pointed out that this situation is a perception and a demand from the sector as it affects the exercise of journalism, particularly in terms of potential impact on the confidentiality of sources, saying that “it is very difficult to contact sources freely” in an environment filled with cameras, with potential interception of communications and access to biometric data. She also called out the lack of information from the authorities regarding the scope and operation of these surveillance systems.

Similarly, Participant 4 noted that while journalists are not usually the main targets of surveillance, their main concern lies in protecting their sources. Monitoring systems enable movements to be tracked, making it possible, for example, to identify where they meet with informants or who they meet, which puts confidentiality at risk. They also mentioned that this type of surveillance has already been observed in other contexts, such as a case in Brazil, and stressed that, although there is no direct evidence of this happening in Buenos Aires, it is technically possible and would be relatively easy to implement.

Participant 7, meanwhile, recounted a personal experience involving surveillance on two separate occasions. The first was during the previously mentioned G20 summit under the government of Mauricio Macri, when a political profile was drawn up about them based on their social media posts, with published content being interpreted as an indication of their political beliefs. The second was in the context of a journalistic investigation they were working on, when they discovered that they, together with a colleague, had been included in a mass request for information and that, in their case specifically, there was evidence of surveillance through biometric data on several occasions. They stated that at the time, they had tried to find out how the information had been obtained and what information had actually been collected. However, they had decided against taking legal action for fear of reprisals, including risks to family members, particularly children, given the extent of the state’s access to personal information. Consequently, in an exercise of self-censorship, they chose not to proceed.

ATTACKS AND BEHAVIOURAL CHANGES ON MEDIA PLATFORMS: DIGITAL MANIFESTATIONS OF SELF-CENSORSHIP

Several interviewees reported changing their behaviour on social media, including those with public profiles or who engage in activities that require visibility. These changes are not always directly linked to acts of state surveillance, but respond to a climate of digital harassment, violent rhetoric, threats via

direct messaging and coordinated attacks that are either currently happening or believed to be happening by those interviewed. Many of the testimonies collected from those interviewed point to a perceived link between the increase in state repression, the public stigmatization of critical voices, and the actions of organized or semi-organized groups on social media.

In this regard, Alejo Fraile, from the Policing Map, pointed out that, based on the monitoring work carried out by research groups linked to media outlets such as *Revista Crisis*, they have been able to identify systematic patterns of harassment practices on social media, particularly in cases of doxxing and coordinated attacks. He also stated that, by using tracking and monitoring tools, they had detected that many of the accounts involved in these attacks have similar characteristics, such as profiles with little organic activity, few or no followers, and repetitive behaviours. These attacks target posts about investigations that are critical of police action.

Likewise, Emilio Lazlo, of streaming channel Gelatina, a platform that is largely critical of the current government, described specific instances in which waves of aggressive comments targeting specific individuals, often with references to their personal or family life, followed certain publications or public appearances. According to their analysis, these behaviours are not spontaneous but show a certain degree of organization and coordination.

Matías Darabós, representative of ACVI, referred to the comments received on their social media posts, which are one of their main channels for publicizing the organization's work analysing police abuses. "There are always people making insulting or threatening comments on your posts, which makes you cautious and gets you to think about how much exposure you want. Some colleagues prefer not to draw attention to themselves, and not appear [on any posts]."

Paula Cejas, from the IFJ, expressed that social media networks are not a safe space. "Social media and the streets are no longer a safe space for journalists. Even I myself think about what I'm going to post to the IFJ account, what language to use so that I'm not put on a list and get us all harassed."

Similarly, Participant 6 stated that she had totally changed the way she interacted on social media. "Before, I used to comment and give my opinion on everything, now I just use it recreationally. I think a lot about the words I use, I moderated my rhetoric and reduced my interaction 100%, especially on Twitter. I embody everything that rubs people up the wrong way: I'm a woman, a journalist, a feminist and a human rights defender."

In the group interview with young people, this point was particularly relevant. Many participants said they had made their social media accounts private in order to have more control over their followers. For example, they said that they would no longer accept follow requests from people with whom they have no followers in common because "you can't let just anyone in". The interviewees stated that hateful comments were one of the main reasons for restricting access of people they do not know to their social media accounts, given the huge increase in such behaviour by people dedicated specifically to disparaging others.

In summary, while many of those interviewed have persisted in their activism and in defending their right to protest despite surveillance practices, many of them also acknowledge having changed their behaviour with regard to both their exercise of freedom of association and protest, and their right to freedom of expression. These changes have been prompted by the implementation of repressive policies and government surveillance, as surveillance policies further restrict the exercise of rights when accompanied by force on the streets.

8. CONCLUSIONS AND RECOMMENDATIONS

This report presents an analysis of reforms to the security and intelligence systems, as well as of the surveillance technology acquired by the national government and the city of Buenos Aires. As has been described here, the national government has implemented structural reforms by modifying the powers and functions of the National Intelligence System and the security forces, such as the Federal Police, and has acquired a wide range of surveillance technologies. This poses serious risks to Argentina's human rights framework, which is aligned with international standards as recognized in the National Constitution, and supported by local regulations on matters such as the protection of personal data and access to information.

The analysis confirms that surveillance and control practices supported by digital technologies have become one of the fastest-growing areas of state security policy. The creation of new units and protocols, the procurement of technological tools and the expansion of the security forces' operational powers are evidence of an increasing prioritization of surveillance technologies, including those based on artificial intelligence, data analysis and digital monitoring. However, this expansion process has come about without a clear and specific regulatory framework, with no adequate external controls, and with insufficient levels of transparency, creating a serious conflict with Argentina's international obligations.

In particular, the practices analysed show a trend towards the concentration of broad surveillance capabilities, ranging from the monitoring of social media and open digital sources, to the use of biometric systems, drones and automated analysis tools, without clear guarantees regarding their necessity, proportionality or legality. The breadth and overlap of these functions, combined with the absence of a precise determination of institutional competencies and responsibilities, undermine oversight mechanisms and hinder accountability. This scenario is particularly concerning in light of the Argentinian state's obligations regarding the protection of rights to privacy, freedom of expression, freedom of peaceful assembly and freedom of association.

Uncertainties persist regarding the use of retrospective facial recognition technology for identification carried out by the Federal Police. If, for example, the procurement of the Clearview software is linked to this process, it would imply the analysis of large volumes of data on individuals who do not necessarily have active legal proceedings or arrest warrants against them. Furthermore, this type of software presents challenges when it comes to being audited. Amnesty International has concluded that Clearview AI should have been aware of the human rights risks arising from its business operations more broadly, including in Argentina. Under the UN Guiding Principles on Business and Human Rights (UN Guiding Principles), companies must promptly address adverse human rights impacts with which they are involved, no matter where they operate. This corporate responsibility to respect human rights exists independently of a state's ability or willingness to fulfil its own human rights obligations and over and above compliance with national laws and regulations protecting human rights. To meet this corporate responsibility, a company must take early, proactive and ongoing steps to identify and respond to its potential or actual human rights impacts by conducting due diligence to identify, prevent, mitigate and account for any negative human rights impacts resulting from their operations or as a result of their business relationships with other actors.

Amnesty International has found that Clearview AI has not to date carried out a public, transparent and ongoing human rights impact assessment, nor demonstrated that the company has addressed any potential or actual adverse human rights impacts that their business products or activities may cause, contribute or be directly linked to in Argentina. As such, Clearview AI must cease the development, sale, deployment and

export of FRT in Argentina, or risk that the company contributes to or becomes directly linked to the increasingly hostile environment faced for human rights in the country.

A study of the chilling effects of these technologies furthermore provided evidence of changes in people's behaviour, driven by repression during protests and by the perception of being subjected to surveillance by the government.

While surveillance technologies and surveillance policies have been introduced as tools to ostensibly address specific forms of criminal activity, Amnesty International's research shows that broadly drafted legal provisions and the documented history of abuses and misuse of such technologies in Argentina, violate the rights to privacy, equality and non-discrimination, freedom of expression and peaceful assembly, while also stifling transparency and freedom of information.

In this context, and considering recent precedents such as the Fugitive Facial Recognition System (SRFP), it is crucial to review and restrict the deployment of surveillance technology until safeguards that align with international human rights law are put in place. This should include adopting specific legal frameworks, conducting human rights impact assessments, establishing independent and effective oversight mechanisms, and guaranteeing accessible remedy proceedings. Without these safeguards, the expansion of surveillance policies represents a real risk of arbitrary interference, with potential chilling effects on the exercise of dissent, political participation and democratic life.

The findings of this report show that the deployment of surveillance technologies without adequate safeguards not only violates rights but also undermines the legitimacy of public policies, increases the risk of authoritarian practices emerging and erodes democratic trust in state institutions. Where the government is engaged in the deployment of technologies of mass surveillance, such as facial recognition for identification (or 1:n), this technology must be prohibited.

Given the above, the following recommendations are made:

8.1 TO THE NATIONAL GOVERNMENT AND THE CITY OF BUENOS AIRES:

- Ban the development, production, sale, and use of biometric technologies that enable mass surveillance and discriminatory targeted surveillance, by all public and private actors;
- Ban the development, production, sale, and use of AI systems that create or expand facial recognition databases through the untargeted scraping of facial images from the internet or CCTV footage;
- Ban automated risk assessment and profiling systems in the context of migration, when used to determine whether people on the move present a 'risk' of unlawful activity or security threats;
- Immediately suspend the use of all surveillance technologies acquired or deployed without specific legal grounds, human rights and data protection impact assessments (DPIA), or external oversight mechanisms. This includes, in particular, open-source monitoring and aerial surveillance tools.
- Establish, in all procedures for the procurement of surveillance technologies, the specific public policy under which they will be used, in order to ensure the traceability of all measures taken.
- Prohibit the use of predictive policing technologies, as these systems reproduce and reinforce historical biases and lack sufficient empirical grounds to justify their impact on basic rights.
- Develop and enact binding human rights-based AI regulation with strong enforcement and independent oversight mechanisms, and ensure that both development and implementation of this legislation follows a transparent, accountable, easy to access, and rules-based policymaking process with meaningful engagement of impacted communities and civil society.
- Make it a mandatory requirement to perform a data protection impact assessment (DPIA), conducted by an independent body and with public consultation, for the implementation of any tool involving the mass or automated processing of personal data.
- Effectively appoint the Bicameral Commission for the Oversight of Intelligence Bodies and Activities (Article 31 of Law 25.520) within the National Congress and ensure its proper functioning pursuant to the powers set forth in the legislation.

- Reject blanket or disproportionate exemptions based on policing, national security or military grounds;
 - Reject granting discretion to companies developing AI systems the possibility of opting out of established rules;
 - Create and maintain publicly available and accessible databases for reporting development and deployment of AI technologies that can have an impact on human rights;
 - Oblige providers of AI systems with human rights impact to register themselves and the given AI system in relevant public databases, including during testing of AI systems in real world conditions;
 - Oblige all public and private deployers to register the use of AI systems that can have an impact on human rights in relevant public databases;
 - Oblige deployers to ensure meaningful transparency of AI systems and algorithmic decision-making with human right impact to effected persons, including during testing of AI systems;
 - Oblige providers and deployers of AI systems to proactively disclose information needed to assess the human rights impact of their systems and to respond when requested by public interest organisations, including through freedom of information requests.
-
- Establish effective, independent, and accessible control mechanisms over the use of surveillance technologies, including at least:
 - prior judicial authorization for any surveillance measure that could affect individual rights, subject to criteria of legality, necessity, proportionality and non-discrimination;
 - administrative oversight by the bodies with competence in this area, such as the Agency for Access to Public Information (AAIP – A, the Ombudsperson’s Office and audit and control bodies, and any others that may need to be created or assigned, vested with effective powers of inspection, audit and sanction, as well as adequate resourcing;
 - regular legislative review of procurements, use, and outcomes of surveillance policies;
 - guaranteeing the right of the affected persons to know, in the terms permitted by law, if they were subject to surveillance, and to challenge the legality of such surveillance before an independent body.
 - Guarantee the principle of transparency in all actions relating to the use of surveillance technologies by regularly and publicly publishing information on the technologies procured, the contracts and suppliers involved, the use protocols in force and the results of audits carried out, as well as by responding substantively to freedom of information requests on this issue, without broadly or unjustifiably claiming exceptions.

8.2 TO THE NATIONAL GOVERNMENT AND THE MINISTRY OF SECURITY IN PARTICULAR:

- Immediately publish substantive information on the structure, budget, suppliers and technical criteria of all the functions assigned to the UIAAS, as a minimum requirement for transparency and accountability.
- Set up an intersectoral working group comprising oversight bodies, civil society, and experts in technology and human rights, with a defined mandate, deadlines and expected results, for the purpose of reviewing the scope of the UIAAS and establishing agreed criteria for its regulation.
- Carry out a technical and institutional review of cooperation agreements between the state and local jurisdictions, in particular in connection with the use of video surveillance infrastructure, biometric data and proprietary software, in order to guarantee minimum standards of interoperability, transparency and oversight.

8.3 TO THE NATIONAL CONGRESS:

- Set up and ensure the effective functioning of the Bicameral Commission for the Oversight of Intelligence Bodies and Activities, pursuant to Article 31 of Law 25.520, providing the resources and powers required to carry out specific oversight of surveillance technologies.
- Support a parliamentary debate on the regulation of the use of surveillance technologies, establishing clear definitions, specific authorizations, limits on use and prohibitions, safeguards, independent oversight mechanisms and sanctions for non-compliance, in line with international human rights standards.

8.4 TO REGIONAL AND INTERNATIONAL HUMAN RIGHTS BODIES:

- Enact legislation to ban the use, development, production, sale and export of remote biometric recognition technology for mass surveillance as well as remote biometric or facial recognition technology used for identification purposes used within their own jurisdictions by both state agencies and private sector actors, as technologies that are fundamentally incompatible with international human rights law
- Pending the ban on such technology, as recommended by the UN Special Rapporteur on contemporary forms of racism, racial discrimination, xenophobia and related intolerance, take “swift and effective action to prevent and mitigate the risk of the racially discriminatory use and design of emerging digital technologies, including by making racial equality and non- discrimination human rights impact assessments a prerequisite for the adoption of systems based on such technologies by public authorities. These impact assessments must incorporate meaningful opportunities for co-design and co-implementation with representatives of racially or ethnically marginalized groups. A purely or even mainly voluntary approach to equality impact assessments will not suffice; a mandatory approach is essential”¹³⁴

¹³⁴ United Nations Human Rights Council, Racial discrimination and emerging digital technologies: a human rights analysis: report of the Special Rapporteur on Contemporary Forms of Racism, Racial Discrimination, Xenophobia and Related Intolerance, UN Doc A/HRC/44/57, 18 June 2020, <https://digitallibrary.un.org/record/3879751> accessed 2 February 20

ANNEX 1 – DETAILS OF PROCUREMENTS AND CONTRACTS

PROCUREMENTS AND COMMISSIONING BY THE NATIONAL GOVERNMENT

ID	TENDER PROCESS NO.	PURCHASE ORDER NO.	EFFECTIVE DATE	JURISDICTION	DESCRIPTION	PROCUREMENT TYPE	CONTRACT DURATION	TYPE	AMOUNT IN ARS	AMOUNT IN USD	AVAILABLE AT
NAC-01	347-0026-CDI25	347-0095-OC25	29/10/2025	National	Acquisition of a software licence to support investigations under the ForCIC	Direct award	12 months	No modality		33,500	Link
NAC-02	347-0024-CDI25	347-0091-OC25	15/10/2025	National	Renewal, upgrade, maintenance and support of the licence for open source investigation platform	Direct award	12 months	No modality		239,013	Link
NAC-04a	347-0009-LPU24	347-0059-OC24	28/08/2024	National	Acquisition of compact unmanned aerial vehicles (UAVs) for Public Security	Public Tender	90 calendar days	No modality		417,530	Link
NAC-04b	347-0009-LPU24	347-0064-OC24	19/09/2024	National	Acquisition of compact unmanned aerial vehicles (UAVs) for Public Security	Public Tender	90 calendar days	No modality		134,155	Link
NAC-05a	347-0020-LPU25	347-099-OC05	01/12/2025	National	Centralized acquisition of unmanned aerial vehicle (UAV) operating ground stations, tethered mode.	Public Tender	90 calendar days	No modality		355,750.00	Link

ID	TENDER PROCESS NO.	PURCHASE ORDER NO.	EFFECTIVE DATE	JURISDICTION	DESCRIPTION	PROCUREMENT TYPE	CONTRACT DURATION	TYPE	AMOUNT IN ARS	AMOUNT IN USD	AVAILABLE AT
NAC-05b	347-0020-LPU25	347-0106-OC25	23/12/2025	National	Centralized acquisition of unmanned aerial vehicle (UAV) operating ground stations, tethered mode.	Public Tender	90 calendar days	No modality		35,575.00	Link
NAC-06	347-0029-CDI24	347-0089-OC24	13/11/2024	National	NOSIS Credit history information service	Direct award	12 months	No modality	18,381,663.36	17,863.79	Link

PROCUREMENTS AND COMMISSIONING BY THE GOVERNMENT OF THE CITY OF BUENOS AIRES

ID	TENDER PROCESS NO.	PURCHASE ORDER NO.	EFFECTIVE DATE	JURISDI CTION	DESCRIPTION	PROCUREMENT TYPE	CONTRACT DURATION	TYPE	AMOUNT IN ARS	AMOUNT IN USD	AVAILABL E AT	COMMENTS
CABA-01	2900-1208-LPU20	2900-0036-OCA21	23/12/2025	City	Commissioning of video image analysis and alert services	Public tender	24 months	Open purchase order	701,656,557	4,997,281	Link	Amount in pesos is sum of each extension with respective increases. Amount in dollars is sum of each amount according to dollar reference rate on date of resolution or call for tenders.
CABA-02	3202-1155-LPU25	3202-0419-OCA25	06/11/2025	City	Licence provision and migration for strengthening digital forensics capacity	Public tender	12 months	Open purchase order	1,222,237,276.04	828,916	Link	Rate used: 1 USD = ARS 1474.5. Depending on rate at award resolution.
CABA-03	3202-0928-LPU25	3202-0381-OCA25	17/10/2025	City	Electrical maintenance and power supply services	Public tender	24 months	Open purchase order	1,123,628,600	810,956	Link	Rate used: 1 USD = ARS 1,385.56. According to BCRA reference retail exchange rate (buyer)

ID	TENDER PROCESS NO.	PURCHASE ORDER NO.	EFFECTIVE DATE	JURISDI CTION	DESCRIPTION	PROCUREMENT TYPE	CONTRACT DURATION	TYPE	AMOUNT IN ARS	AMOUNT IN USD	AVAILABL E AT	COMMENTS
					for video capture points							for 31 July 2025, opening date of tender.
CABA-04	3202- 0970- LPU25	3202- 15648- OC25	02/10/2025	City	Data analysis service	Public tender	24 months	No modality	120,720,000	93,804.64	Link	Rate used: 1 USD = ARS 1,286.93. According to BCRA reference retail exchange rate (buyer) for 13 August 2025, opening date of tender.
CABA-05	3202- 0066- LPU25	3202-0184- OCA25	23/06/2025	City	Connectivity service for devices within the video security platform	Public tender	12 months	Open purchase order	14,823,189,156	14,184,463	Link	Rate used: 1 USD = ARS 1045.03. According to the BCRA reference retail exchange rate (buyer) for 3 April 2025, opening date of tender.
CABA-06	3202- 0540- LPU24	3202-0132- ICA24	08/05/2025	City	Acquisition of capture points and hardware and software for processing and storage	Public tender	24 months	Open purchase order	25,102,477,483	27,077,219.07	Link	Rate used: 1 USD = ARS 927.07. Depending on rate at award resolution. Total amount includes all the lines awarded (in pesos and in dollars), according to award resolution. Includes all detected increases.

CAPTURE POINT ACQUISITION AMOUNTS UNDER CABA EXTENSION RESOLUTIONS

LINE	DESCRIPTION (AS PER TECHNICAL SPECIFICATIONS)	ORIGINAL PO RES. 984/MSEGC/24 11 OCTOBER 2024	EXTENSION 1 RES. 1186/MSEGC/24 11 DECEMBER 2024	EXTENSION 2 RES 26/SSGA/25 5 FEBRUARY 2025	EXTENSION 3 RES. 511/MSEGC/25 8 MAY 2025	TOTAL AMOUNT
1	Acquisition and installation of video capture points for the comprehensive video surveillance plan	One hundred and fifty (150) units USD 2,341,800.00	Four hundred (400) units USD 6,244,800.00	<i>No increase</i> <i>No increase</i>	Three hundred (300) units USD 4,683,600.00	USD 13,270,200.00
2	Acquisition and implementation of hardware and software for the processing and management of video capture devices for the MSEG video surveillance system	Three (3) units USD 429,345.00	Six (6) units USD 858,690.00	<i>No increase</i> <i>No increase</i>	Six (6) units USD 858,690.00	USD 2,146,752.00
3	Acquisition and implementation of hardware and software for image storage for the MSEG video surveillance system	Three (3) units USD 1,302,854.58	Six (6) units USD 2,605,709.16	<i>No increase</i> <i>No increase</i>	Six (6) units USD 2,605,709.16	USD 6,514,272.9
4	Technical support service, help desk and hardware maintenance for monitoring centers and data centre of the MSEG video surveillance system	Twenty-four (24) months USD 4,234,964.16	<i>No increase</i> <i>No increase</i>	<i>No increase</i> <i>No increase</i>	<i>No increase</i> <i>No increase</i>	USD 4,234,964.16
5	Acquisition of components of the monitoring centres of the MSEG public video surveillance system as per items in Table II	One (1) unit USD 438,667.60	<i>No increase</i> <i>No increase</i>	Increase by 30 units for items 1 and 2 USD 457,493.40.	<i>No increase</i> <i>No increase</i>	USD 896,161

LINE	DESCRIPTION (AS PER TECHNICAL SPECIFICATIONS)	ORIGINAL PO RES. 984/MSEGC/24 11 OCTOBER 2024		EXTENSION 1 RES. 1186/MSEGC/24 11 DECEMBER 2024		EXTENSION 2 RES 26/SSGA/25 5 FEBRUARY 2025		EXTENSION 3 RES. 511/MSEGC/25 8 MAY 2025		TOTAL AMOUNT
6	On-site technical assistance service for support at the Monitoring Centre	Seventy-two (72) modules	ARS 13,759,200	<i>No increase</i>	<i>No increase</i>	<i>No increase</i>	<i>No increase</i>	<i>No increase</i>	<i>No increase</i>	ARS 13,759,200

Total USD amount

**AMNESTY INTERNATIONAL
IS A GLOBAL MOVEMENT
FOR HUMAN RIGHTS.
WHEN INJUSTICE HAPPENS
TO ONE PERSON, IT
MATTERS TO US ALL.**

CONTACT US



contactus@amnesty.org



+44 (0)20 7413 5500

JOIN THE CONVERSATION



www.facebook.com/amnesty



@Amnesty

SENSING THE SURVEILLANCE STATE

ARGENTINA'S EXPANDING POLICIES AND TECHNOLOGIES OF MASS SURVEILLANCE

Between December 2023 and December 2025, the Argentinian government implemented a slew of security and intelligence reforms and expanded their use of surveillance technologies. In just two years, the national government drove a set of institutional reforms designed to expand its surveillance and intelligence capabilities, implemented mainly through executive decrees and resolutions, with no parliamentary debate.

This report shows that the deployment of surveillance policies and technologies in Argentina, nationally as well as at the city level, has direct impacts on human rights, while also having significant indirect effects on the exercise of human rights, through perpetuating discrimination, chilling free expression and peaceful assembly.