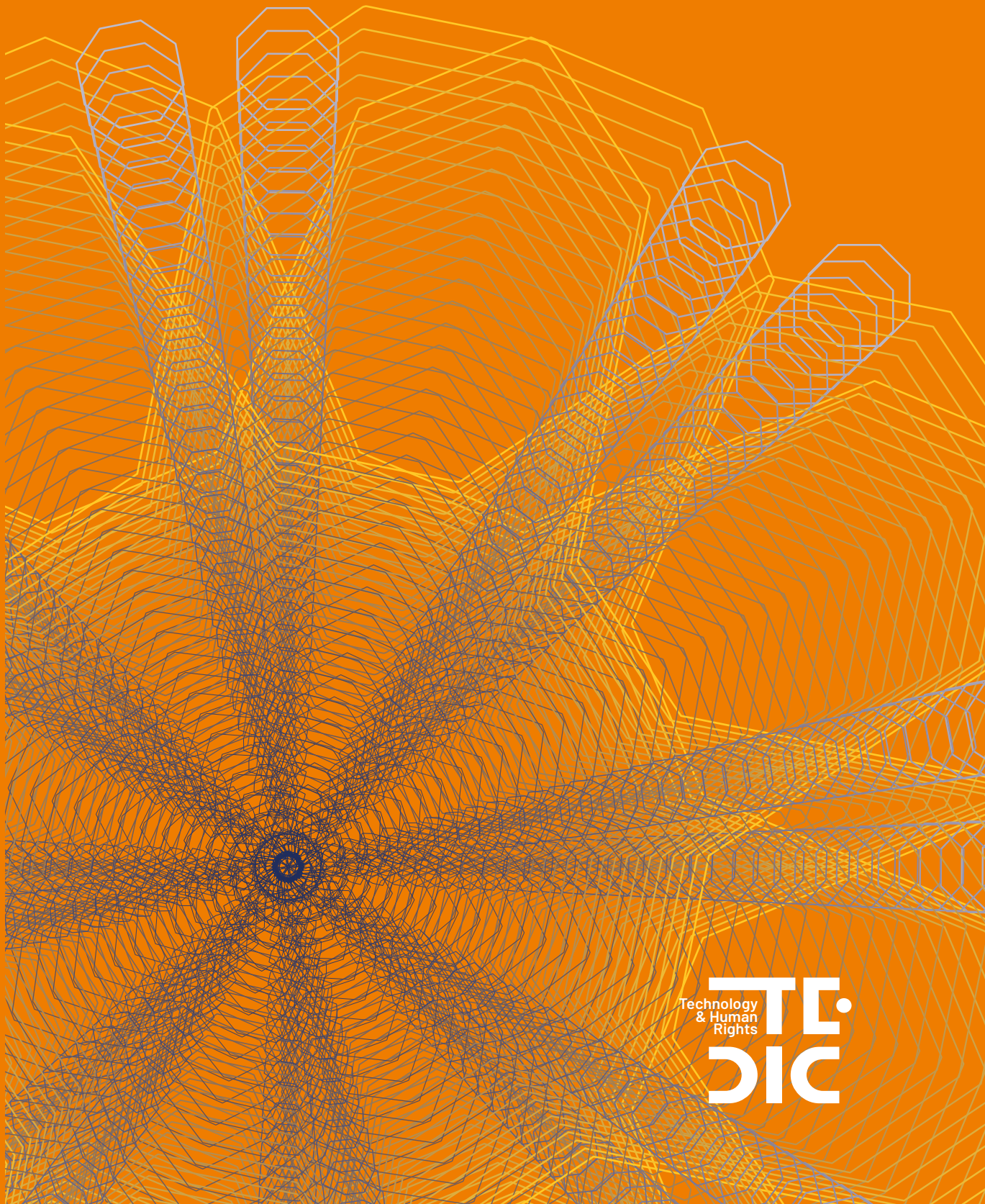
DRONES

Regulation and use of drones in Paraguay from a digital rights perspective



Technology & Human Rights

TEDIC

This publication has been funded by the European Union. Its content is the sole responsibility of TEDIC and does not necessarily reflect the views of the European Union.

Funded by the European Union

WITH THE SUPPORT OF
La gente cambia el mundo Diakonia

Technology & Human Rights TEDIC

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

DRONES

Regulation and use of drones in Paraguay from a digital rights perspective

SEPTEMBER 2025

COORDINATION
Maricarmen Sequera

RESEARCHERS
Antonia Bogado
Hugo Mendieta

ASSISTANCE
Maricel Achucarro

COMMUNICATION
Romina Aquino González

LAYOUT
Horacio Oteiza

ABOUT THE RESEARCHERS

Antonia Bogado Rodas: Lawyer, LL.M. from the London School of Economics and Political Science, and Master's in Ethical Governance of Artificial Intelligence from the Pontifical University of Salamanca. Her research interests include digital rights and the intersection between law and technology.

Hugo Mendieta Cuevas: Law graduate from the National University of Asunción (UNA), member of the editorial board of *Liberoamérica*, and member of the Asunción Flores Collective. He writes regularly for *Adelante! Noticias*.

TABLE OF CONTENTS

INTRODUCTION AND RESEARCH METHODOLOGY 5

THEORETICAL FRAMEWORK 8

Drone technologies: definition, uses and capabilities 8

Technical types, surveillance capabilities and classifications 8

Drones as dual technologies: civil, commercial and military uses 10

A brief genealogy of the state's use of drones 12

DRONES AND HUMAN RIGHTS IN THE DIGITAL AGE 15

Conceptual framework 15

Privacy in the digitized public space 19

Freedom of expression and the right to protest amid the threat of aerial surveillance 21

Legality and proportionality in technological surveillance measures 23

State surveillance, social control and power structures 25

The digital panopticon and aerial surveillance 26

Drones and the militarization of civilian space 28

INTERSECTIONAL PERSPECTIVE AND SELECTIVE SURVEILLANCE 31

Gender, racialization and control technologies: 31

Asymmetries in access to and use of technologies 34

GLOBAL GOVERNANCE, GEOPOLITICS AND REGULATION 36

The Paraguayan case: regulatory fragmentation and technological sovereignty 38

LIMITATIONS OF THE STUDY 41

RECOMMENDATIONS 42

CONCLUSIONS 43

EPILOGUE 44

BIBLIOGRAPHY 45

DRONES
REGULATION AND USE IN PARAGUAY FROM A DIGITAL RIGHTS PERSPECTIVE

KEYWORDS: *Drones, digital rights, privacy, surveillance, Paraguay, human rights, emerging technologies, civil liberties, gender, public policy.*

INTRODUCTION AND RESEARCH METHODOLOGY

The growing use of drones[1] by state and private institutions in Paraguay poses urgent challenges to privacy, surveillance and human rights. While their use can be justified for legitimate tasks such as environmental monitoring, precision agriculture or emergency response, problematic uses have also been documented in areas such as territorial control, surveillance of social protests and harassment of communities in militarized zones.

This duality—between social utility and repressive potential—is exacerbated by the absence of regulatory safeguards and effective mechanisms for transparency and accountability in Paraguay. The regulatory vacuum exposes citizens to increasingly sophisticated and complex forms of surveillance, where technology amplifies the state's control capabilities without corresponding safeguards for human rights protection.

The relevance of this research lies in the need to anticipate and document the negative effects of the deployment of emerging surveillance technologies in contexts of weak institutionality. In a country where social tensions often manifest through protests and citizen mobilizations, and where territorial conflicts with peasant and indigenous communities persist, the unsupervised use of drones poses a significant risk to the exercise of fundamental rights such as privacy, freedom of expression, the right to protest and freedom of movement.

This research adopts a critical, human rights–based approach, drawing on regulatory frameworks and comparative international experiences. Our analysis focuses specifically on uses that may be intrusive, disproportionate or lacking in control, aiming to highlight the risks associated with surveillance, persecution or social control through these technologies.

The study is guided by the following central questions:

- What is the degree of public transparency regarding the acquisition and use of drone technologies by the Paraguayan state?
- Which institutions control these technologies and under what regulatory frameworks do they operate?
- Are there independent oversight mechanisms or parliamentary control over their use?
- How does the deployment of drones affect the right to privacy in both public and private spaces?
- What impact does their use have on the exercise of freedom of expression and the right to peaceful protest?
- How are the differentiated effects manifested according to gender, ethnicity and social class?
- What official justifications support the use of drones in different operational contexts?

1 This paper focuses on aerial drones, although the technology extends beyond this configuration. As Chamayou (2016) notes, any unmanned vehicle—whether aerial, terrestrial or submarine—can be "dronized," thereby broadening the scope of the concept beyond the field of aeronautics.

- Is there proportionality between the stated purposes and the technological means employed?
- What safeguards exist to prevent abuse or misuse of the information collected?

To meet the objectives of the project, we propose a mixed qualitative methodology that combines systematic desk research with fieldwork focused on collecting use cases. This approach will enable both the mapping of the regulatory and institutional landscape and the documentation of concrete practices—both nationally and internationally—and their impacts in different social contexts. The research is structured into three complementary phases, which will be developed partially simultaneously to maximize source triangulation and cross-validation of findings.

The first phase will focus on regulatory and institutional mapping, aiming to characterize the current legal framework and identify the institutional actors involved in the acquisition and use of drones. This stage will include a documentary analysis of current regulations, particularly the regulations of the National Directorate of Civil Aeronautics (DINAC), executive decrees, ministerial resolutions and any other applicable provisions. At the same time, the study will review archived and pending legislative initiatives related to the regulation of drones and surveillance technologies. It will also carry out a systematic mapping of public procurements available on the website of the National Directorate of Public Procurement (DNCP), identifying purchases of equipment, maintenance services and training related to drones. This phase will be complemented by formal requests for access to public information addressed to key institutions such as the Ministry of the Interior, the National Police, the Ministry of Defense, the National Intelligence Secretariat (SNI), the Ministry of Agriculture and Livestock (MAG) and the Joint Task Force (FTC). The expected outcomes of this phase include a comparative matrix between the national regulatory framework and international human rights standards, a database of public procurement related to aerial surveillance technologies and a detailed mapping of institutional actors and their specific competencies.

The second phase will focus on documenting specific practices and cases, aiming to identify and analyze specific uses of drones in different operational contexts, with special attention to those that may affect fundamental rights. This stage includes the analysis of documented cases where the use of drones has been reported in contexts such as social protest, security operations, or territorial control in rural areas, complemented by a systematic review of media coverage on the use of drones by security forces and other state institutions. Social media monitoring will also be incorporated to track testimonies, images and videos that document the deployment of these technologies from the citizen's perspective, as well as interviews with those affected, including social leaders, activists, community leaders and organizations that have experienced surveillance by drones. The case selection criteria will prioritize the use of drones in demonstrations or social protests, security operations in territories with socio-environmental conflicts, surveillance in border and rural areas and cases that have led to complaints of human rights violations.

The third phase will focus on comparative analysis and the development of recommendations, contextualizing national findings within the framework of regional and international experiences to identify common patterns and best practices. This stage will include comparative case studies from countries in the region that have faced similar challenges, such as Colombia, Brazil, Mexico and Chile, along with interviews with specialists in digital rights, surveillance technologies and security policies at both national and regional levels. It will be complemented by a thorough review of specialized literature, including academic research, reports from international organizations and

public policy documents on drone regulation and human rights protection. Interviews will be conducted with experts from various fields, including specialists in digital rights and surveillance technologies, academics with experience in security and militarization policies, public officials from regulatory institutions such as DINAC and the National Police, human rights activists and organizations with experience in state surveillance, and international experts in drone regulation and privacy protection.

Given that the research addresses sensitive issues related to security and state surveillance, specific ethical and methodological considerations will be implemented to ensure the rigor and accountability of the process. Methodological triangulation will be prioritized by cross-referencing information from different documentary sources to validate findings and minimize bias, explicitly documenting limitations in access to information, potential biases in sources and time constraints that may affect the comprehensiveness of the study.

At the conclusion of the research, it is expected to have a comprehensive diagnosis that highlights problematic practices, identifies specific risks to human rights and proposes concrete recommendations for the responsible use of drones from a perspective of human rights protection and public governance based on principles of legality, proportionality and transparency. Specific outputs will include a comprehensive mapping of the institutional and regulatory ecosystem, documentation of paradigmatic cases and their differentiated impacts, a comparative analysis with international experiences and recommendations addressed to various stakeholders.

This research aligns with TEDIC's institutional mission to promote digital rights and strengthen democratic control over the use of technologies, contributing to an agenda that ensures transparency, equity and respect for human rights in the digital and physical environment, while positioning Paraguay in the regional debate on the responsible regulation of emerging surveillance technologies.

THEORETICAL FRAMEWORK

DRONE TECHNOLOGIES: DEFINITION, USES AND CAPABILITIES

A drone or unmanned aerial vehicle (UAV) is a technological device with various configurations and uses. The International Civil Aviation Organization (ICAO) uses several terms to refer to these devices or their systems, including: RPA (Remotely Piloted Aircraft), RPAS (Remotely Piloted Aircraft System), UA (Unmanned Aircraft), and UAS (Unmanned Aircraft System(s)). However, the term "drone" is the most commonly used to refer to unmanned aircraft.

According to ICAO's Global Air Traffic Management Operational Concept (Doc 9854), an unmanned aerial vehicle (UAV) is an aircraft without a pilot on board, flying without a pilot in command, and remotely and fully controlled from another location (whether ground, another aircraft, space) or programmed to be fully autonomous. This definition was endorsed by the 35th ICAO Assembly in 2011 (ICAO, 2011). The georeferenced flight coordinates are either programmed by software or controlled remotely.

Drones come in different sizes, capabilities and a variety of models, ranging from recreational to more complex uses. They are classified in various ways according to their structure, size, technical capabilities and applications. By wing type, drones include multirotors, which are easy to maneuver but have limited autonomy; fixed wings, ideal for long and stable flights; single-rotor drones, capable of carrying heavy payloads; and hybrid fixed-wing VTOLs, which combine vertical takeoff with extended autonomy.

TECHNICAL TYPES, SURVEILLANCE CAPABILITIES AND CLASSIFICATIONS

Structural classification of drones

- Fixed-wing drone: This design is similar to that of airplanes, with a composition designed to save energy and generate adequate aerodynamic lift. They have better stability for long-range operations, and the vast majority of military drones have a fixed-wing design, including HALE[2] drones, which are primarily used for surveillance and territorial reconnaissance in military operations.

- Single-rotor drone: This design is similar to that of a helicopter, with a rotor that propels the drone. It typically has the capacity to incorporate larger propellers to increase efficiency. These drones are commonly used for topography and the transportation of heavy payloads.

- Multirotor or rotary-wing drone: This type consists of multiple propellers supported by a centralized chassis to achieve stability and lift. It is a versatile and simple model, though it has limited autonomy. These drones are the most common in the civil and government market, typically used for surveillance or aerial photography, etc.

  - Tritor: It has three rotors located on three arms, providing control and movement. This configuration is the most economical and the least autonomous.

2 High-altitude long endurance

- Quadcopter: Commonly used model for civil applications. It consists of four rotors supported by a frame, with two of the propellers rotating in the opposite direction to the other pair. It offers greater stability than trirotor drones.
- Hexacopter: Six rotors supported by a proportionally sized chassis. The rotors are positioned so that each arm provides balance and power, with three of the propellers rotating in the opposite direction to the others. Its energy consumption is high.
- Octocopter: This model enhances the stability of the hexacopter by incorporating eight rotors, with the propellers working in pairs of four, rotating in opposite directions for exceptional stability and control. It is typically used for professional purposes.
- Coaxial multirotor: It consists of paired arms that support two or more rotors on each arm, with each rotor rotating in opposite directions. The coaxial multirotor offers greater altitude capabilities and versatility than other designs.

- Hybrid fixed-wing drone (VTOL): This design combines fixed wings with rotors integrated into the structure, offering advantages in both stability and maneuverability. It is primarily used for transport and package delivery.

  Depending on their size, drones are classified as very small (nano), small, medium and large, with uses ranging from covert surveillance to filming or deliveries. In terms of payload capacity, they are classified as ultralight, light, medium and heavy-lift drones, suitable for missions ranging from recreation to military applications. According to their range, drones vary from very short-range (up to 5 km) to long-range (over 644 km), with flight times that can exceed 24 hours. They are also categorized by their power source, such as batteries (the most common), gasoline, hydrogen or solar. In terms of engine type, drones can have brushed motors (economical but less durable) or brushless motors (more powerful and efficient). Finally, depending on their functionality, drones are categorized as toy drones, photographic drones, racing drones, GPS drones, professional drones, military drones and delivery drones, which reflects the growing specialization and diversification of this technology. (JOUAV, 2025).

  These are the basic internationally recognized classifications, although many other classifications exist in regional and national regulations, such as the classification of the European Union Aviation Safety Agency[3] (EASA), which distinguishes drones into six classes according to their weight or mass.

  The classification reference in Paraguay distinguishes between two general types of drones: 1) autonomous aircraft; and 2) remotely piloted aircraft (Regulation on Remotely Piloted Aircraft (RPA) and Remotely Piloted Aircraft System, 2017). This distinction is based on the autonomous capabilities of the equipment. Additionally, there are technical classifications based on weight/mass at takeoff, intended use and regulatory categories that define whether the drone is operated with an open, certified or specific license.

  All these types of drones are capable of surveillance (e.g., data processing) and military use, but they also have significant potential for technical applications in many sectors of goods and services, including activities of scientific interest.

3 See more on the EASA website: https://www.easa.europa.eu/en/document-library/general-publications/drone-class-identification-labels-and-information-notices

DRONES AS DUAL TECHNOLOGIES: CIVIL, COMMERCIAL AND MILITARY USES

Drones, or UAVs, embody the dual nature that characterizes many contemporary technologies. On one hand, they can enhance the capabilities of states, corporations and citizens for legitimate, public-interest purposes; on the other hand, their use without clear boundaries can lead to practices of social control, exclusion or disproportionate surveillance. This technical ambivalence calls for a critical approach that avoids both their enthusiastic and uncritical adoption for their potential benefits, as well as their automatic disqualification due to the risks they entail.

Various international organizations have highlighted the benefits of drones in key sectors. The World Bank (2024) has identified five priority areas in which their implementation has had positive impacts: "the delivery of medical supplies to remote areas, precision agriculture, disaster risk management, critical infrastructure monitoring and ecosystem restoration." These functions not only reduce operating costs and overcome geographical barriers, but in certain contexts, they become indispensable tools for guaranteeing social rights such as health, a healthy environment and access to basic services.

In Latin America, experiences in Brazil, Mexico, Peru and Argentina show emerging applications for monitoring forest fires, urban planning, controlling vector-borne diseases and monitoring endangered species (World Bank, 2024; Jokura, 2021). In the field of sexual and reproductive health, the use of drones has been key in circumventing regulatory restrictions, as seen in the case of the delivery of abortion pills from Germany to Poland, organized by the organization Women on Waves (Browne, 2015). Similarly, initiatives in countries such as Ghana, Nepal and Botswana have demonstrated the viability of using drones to distribute medicines, collect medical samples, and even send blood for transfusions to rural and isolated areas (United Nations, 2021).

These uses are not unfamiliar to Paraguay, although their development remains in its early stages. The private sector has begun to incorporate agricultural drones into various productive activities, mainly for spraying crops such as cereals, yerba mate and forest species, appreciating their low operating cost and versatility (ABC Color, 2025). Multispectral drones are also used for mapping and analyzing field conditions, as well as for monitoring animals, planting and fertilization tasks. While the Ministry of Agriculture and Livestock (MAG) has only acknowledged the use of drones for institutional press purposes since 2024[4], without establishing specific regulations for the private sector, other institutions, such as the Ministry of Information and Communication Technologies (MITIC), use them for advertising, in compliance with DINAC provisions[5].

Outside the state sphere, international experiences such as those of Amazon and DHL show a growing interest in automated package delivery. In catastrophic events such as floods or forest fires—like those in Texas and Los Angeles—drones have also been deployed for search operations and damage assessment (Castleman & Toohey, 2025).

4 This information is based on the official response provided by the MAG to the request for access to public information (No. 93399), available on the Unified Public Information Portal (Ministry of Agriculture and Livestock, 2025).

5 According to the official response from MITIC to Request No. 93400, the entity acknowledged owning a DJI MINI 4 PRO drone with a camera (serial number 1581f6z9c239k0038je2), which is used exclusively for advertising and institutional production purposes (MITIC, 2025).

Thus, the dual nature of this technology also raises tensions and questions about the purposes, contexts and frameworks guiding its implementation. The same device that allows vaccines to be delivered to remote areas can, in the absence of adequate controls, be used to monitor protests, track movements or carry out targeted persecution. In fact, interference between private drones and rescue operations has been documented, creating serious risks in emergency contexts (Castleman and Toohey, 2025).

In the military sphere, armed or intelligence-specialized UAVs have been increasingly deployed in international conflicts[6], significantly transforming modern warfare, introducing new methods of combat and posing complex challenges in the field of defense. As Seth J. Frantzman (2021) has warned, in recent years, drones have played a strategic role in wars worldwide in recent years, establishing themselves as tools for both attack and surveillance.

In the war between Russia and Ukraine[7], for example, the intensive use of drones by both state forces and irregular groups has been documented, contributing to a redefinition of the logic of the battlefield based on low-cost, high-precision technologies. Some reports have even argued that "drones and unmanned vehicles are already beginning to replace soldiers" (Kardoudi, 2025).

Similarly, in the context of the conflict between Israel and Palestine[8], drones equipped with thermal cameras and weapons have been used for reconnaissance and attacks, leading to serious allegations of collateral damage, mass surveillance and psychological impacts, especially on the civilian population. There have also been recent reports of drones being deployed between Iran and Israel[9], which has intensified regional tensions and highlighted the increasing automation of armed conflict.

According to Frantzman (2021), the future of drone warfare is moving towards greater autonomy and the integration of artificial intelligence (AI), with humans playing a "human-on-the-loop" (supervisory) role rather than a "human-in-the-loop" (direct control) role. In this context, various national and international organizations—including TEDIC—have raised ethical concerns about the use of armed drones, particularly regarding the possibility of these systems making lethal decisions without direct human oversight[10].

---

6 Although this paper primarily focuses on aerial drones, it is important to highlight the complementary role of such technologies in other environments, as demonstrated by Germany's use of the "Blue Whale" submarine drone for defensive patrols in the Baltic Sea (DCD, 2025).

7 The conflict between Russia and Ukraine has been one of the first conventional confrontations in which drones—both commercial and military—have been extensively deployed by both sides, redefining tactics in warfare, reconnaissance and targeted attacks (Edmonds & Bendett, 2022; United Nations, 2025).

8 The systematic use of armed drones by Israel in the Gaza Strip has been documented, deployed for both surveillance and targeted attacks, leading to a high number of civilian casualties and prolonged psychological distress among the population. (See: Abualouf, R. (2025, June 26). Israeli strike at Gaza market kills 18 Palestinians,' doctor and witnesses say. BBC). https://www.bbc.com/news/articles/cly8dlzx918o.

9 In recent years, Iran and Israel have engaged in a technological escalation through the use of armed drones in targeted attacks and retaliatory operations. See: Reuters. (2025). Mapping the conflict between Israel and Iran. https://www.reuters.com/graphics/IRAN-NUCLEAR/ISRAEL/dwvklgrgjpm/

10 To learn more about the arguments surrounding this issue, see the "Stop Killer Robots" campaign: https://www.stopkillerrobots.org/

Frantzman (2021) also argues that the transformation of warfare by drones is an ongoing process, where rapid technological advances and proliferation challenge existing defense strategies and require constant adaptation. To this, we add that the widely documented functional versatility imposes a clear demand: to evaluate each implementation based on its purposes, its proportionality, its impact and the governance frameworks that accompany it. It is not just a question of who operates the drone, but for what purpose, with what safeguards and under what system of accountability. In a technological ecosystem where the boundaries between civil, commercial and security uses are rapidly blurring, thinking of drones as dual-use technologies is the first step in ensuring that their benefits do not end up concealing new forms of exclusion, surveillance or structural violence.

A BRIEF GENEALOGY OF THE STATE'S USE OF DRONES

To delve deeper into the technology and its current status, it is necessary to examine the historiography of drones in material terms, a task that requires mentioning the state. According to Friedrich Engels, this fundamental factor is a structure of territorial units based on property relations that definitively displaced "the old society founded on kinship groups" (Engels, 1884, p. 1). This historical context and the consolidation of state social organization influenced the development of drones, their evolution and their modes of use.

Most of the important precedents mentioned below[11] occurred within the context of military campaigns and national security organizations. However, it is important to note that during the 20th century, drones also experienced significant growth in the private civil and scientific sectors.

The use of unmanned aircraft in combat dates back to 1849, according to Rachel Sïmon Rushby (2017), when the Austrian army used a fleet of unmanned hot air balloons in an attack on Venice. From that point onward, there was a clear surge in the application of technology for military purposes, particularly during the First and Second World Wars, when parties in conflict made efforts to develop unmanned combat aircraft. These advances were driven by states that recognized the potential of this technology for warfare and internal security (primarily surveillance and reconnaissance). Consequently, the deployment of drones progressed in lockstep with the consolidation of state-led technological development programs

One example of military use—among many in the 20th century—can be traced back to the Vietnam War with the "Firebee drones,"[12] which were used extensively by the United States of America (USA) in Vietnamese territory. However, the rapid evolution of computing since the late 20th century enabled armed drones to become far more sophisticated weapons. This evolution was so significant that they became the weapon of choice and a symbol of US policy during its "Global War on Terror"[13]—the name for the international military campaign led by the United States following the September 11, 2001, attacks on the World Trade Center in New York and other government buildings.

11 As the subtitle of this section indicates, not all precedents are cited, nor is the entire historiographical process surrounding this technology covered. Instead, a few key moments are highlighted to illustrate, in a more or less comprehensive manner, the complexity of this process.

12 The AQM-34L drone model was used in more than thirty attacks in North Vietnam. A sample of the vehicle can be seen at the US Air Force Museum: https://www.nationalmuseum.af.mil/Visit/Museum-Exhibits/Fact-Sheets/Display/Article/195747/teledyne-ryan-aqm-34l-firebee/

13 There are also other issues surrounding the "global war on terror" that are debated in international law. Rushby (2017) notes that "most legal commentators who have examined the U.S. concept of the 'global war on terror' conclude that it is not a legitimate interpretation of the concept of non-international armed conflict. It undoubtedly creates challenges when considering the application of IHL."

This strategic focus marked a watershed moment in the US development of drone technology and its widespread deployment.

In this century, the predominant justification for the development of armed drone programs in most countries with military operations is that drones are presented as "surgically precise and effective tools" with minimal drawbacks or collateral impacts. However, these claims are highly questionable when contrasted with the data and information collected by the media from areas where military drone operations have been carried out. For example, data from Pakistan shows that between June 2004 and mid-September 2012, drone strikes killed between 2,562 and 3,325 people. Civilian casualties accounted for 474 to 881 of these deaths, including 176 children, while the number of high-level targets killed was extremely low, estimated at only 2% of the total (International Human Rights and Conflict Resolution Clinic et al., 2012). Similarly, in Palestine, there have been a large number of civilian casualties[14] in drone strikes operated by the Israel Defense Forces (IDF). At the same time, Israeli settlers use drones in various sectors of Gaza (Abraham, 2025) to intimidate the Palestinian population.

Drones are also employed as a tool in international conflict mediation, often to gain leverage and dictate terms during negotiations. Regarding the context of the conflict between the Sahrawi Republic against the territorial occupation and annexation by Morocco, Sahrawi President Brahim Ghali, stated that his army would begin using armed drones against Moroccan forces, signaling a move towards total war if the occupation does not cease (Resumen Latinoamericano, 2025). These situations illustrate how technology is developed aligned with the needs of states, and the examples provided show how this often endangers the lives of civilian populations.

From the perspective of International Humanitarian Law (IHL) and International Human Rights Law (IHRL), armed drones are not expressly prohibited; however, their use must adhere to the principles of distinction, proportionality, military necessity and humanity. Rushby (2017, pp. 24-25) comments on this:

> There are no treaties or customary laws that prohibit the use of armed drones per se. In conventional IHL, the rules on the means of warfare are mainly contained in Articles 35 and 36 of Additional Protocol I of 1977 (Protocol I) to the four Geneva Conventions of 1949, relating to the protection of victims of international armed conflicts. While Protocol I applies only to international armed conflicts, the rules set out in Articles 35 and 36 are part of customary international law and thus apply equally to both international and non-international conflicts. Furthermore, weapons must be capable of complying with the principles of IHL, namely distinction, precaution and proportionality.

As technological development continues, regulatory proposals are also being put forward to address the situations arising from the military use of this device. It is worth mentioning that, as a paradigm, among the recommendations made at the 2013 IACHR hearing (Inter-American Commission on Human Rights, 2013)[15], international experts highlighted the importance of states facilitating the creation of civilian oversight of military and police operations using this technology. At that same 2013 hearing, the representative of the Robert F. Kennedy Human Rights Foundation listed the main reasons why the military use of this technology is booming in the region:

---

14 The BBC itself reported a statement made to AFP, in which a resident of southern Gaza said: "People are currently inside their homes because anyone who moves is attacked by Israeli drones."
See more at: https://www.bbc.com/mundo/articles/c3gg8dn55mdo

15 See more at https://www.youtube.com/watch?v=to0EImeza30&t=608s

> The reasons for accessing this technology are varied, but they can be summarized in three key arguments: the cost of these aircraft is lower than that of state-of-the-art alternatives; the acquisition of such technology by one country creates a perceived need for other states to acquire the same capabilities; and, given the tax cuts for most armed forces in the region, the military is eager to have new toys to maintain its institutional space[16].

Since the previous decade, international organizations have advocated for reducing and limiting surveillance programs, as stated in a joint communiqué by the United Nations (UN) Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression and the Special Rapporteur for Freedom of Expression of the Inter-American Commission on Human Rights (IACHR) of the Organization of American States (OAS), in accordance with international regulations:

> (...) , they prohibit arbitrary or abusive interference in private life, including communications, setting forth as well the right to state protection from such interference. In keeping with this, states must guarantee that the interception, collection and use of personal information, including all limitations on the right of the affected person to access this information, be clearly authorized by law in order to protect them from arbitrary or abusive interference with their private interests. The law must establish limits with regard to the nature, scope and duration of these types of measures; the reasons for ordering them; the authorities with power to authorize, execute and monitor them; and the legal mechanisms by which they may be challenged. (United Nations (UN) Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression & Special Rapporteur for Freedom of Expression of the Inter-American Commission on Human Rights of the OAS, 2013).

The current situation highlights the significant risk posed by the lack of transparent and independent oversight of state decisions in defense and internal security—fields with a long-standing tradition of secrecy regarding technological developments—not to mention the absence of regulated procedures for the use of drones in surveillance. This risk stems not only from their impact on civilian populations, but also from their potential to undermine democratic governance and violate human rights. As previously mentioned, the development of these devices tends to focus on military and state security purposes. An example of this can be found in the data collected by Grégoire Chamayou (2015, p. 13) regarding the situation in the United States:

> The use of this weapon has grown exponentially: the number of patrols by American armed drones increased by 1,200 percent between 2004 and 2012. In the United States today, more drone operators are trained than all the pilots of fighter planes and bombers put together. Whereas the defense budget decreased in 2013, with cuts in numerous sectors, the resources allocated to unmanned weapon systems rose by 30 percent.

While technology is reaching unprecedented levels of accessibility and efficacy, the historical development of drones is directly linked to military and surveillance interests. Given this, reviewing the historical process of drones requires considering states and their national and international policies.

16 See the intervention at:: https://youtu.be/to0EImeza30?si=7TS5Qqu2i7cHmSGZ&t=195

DRONES AND HUMAN RIGHTS IN THE DIGITAL AGE

CONCEPTUAL FRAMEWORK

The growing deployment of drones for surveillance, control and security tasks, whether by the state or private actors, has sparked profound tensions regarding human rights. While these technologies offer undeniable benefits in various contexts such as agriculture, environmental monitoring and emergency response, their use in urban environments and for social control raises serious concerns about privacy, autonomy, equality and fundamental freedoms (Gholami, 2024).

In particular, the use of drones for mass or selective surveillance can violate the right to privacy, as enshrined in the Constitution of the Republic of Paraguay—hereinafter, the National Constitution—(Art. 33), as well as in Article 12 of the Universal Declaration of Human Rights and Article 11 of the American Convention on Human Rights (Pact of San José). Moreover, the collection of images, sounds or personal data without consent or judicial control can constitute arbitrary interference[17] in people's private lives (United Nations, 2020; Risso, 2019).

Similarly, the extensive use of these technologies can have a chilling effect on the exercise of fundamental freedoms, such as freedom of expression and freedom of assembly, recognized in Articles 26 of the National Constitution, 19 and 20 of the Universal Declaration of Human Rights, and 13 and 15 of the American Convention, particularly when they are used to monitor demonstrations or protest spaces, an issue that will be discussed in greater detail in a later section.

This type of surveillance, perceived as a threat or a form of intimidation, restricts people's right to express themselves freely and assemble without fear of reprisals (Lara Castro, 2020). However, it is important to note that not all uses of drones inherently violate rights, and that each case must be analyzed individually, considering the context, purpose, technology used and the existence or absence of legal guarantees and control mechanisms (Gholami, 2024). For example, the use of drones to inspect crops does not raise the same concerns as their use to monitor a citizen protest.

On the other hand, it is also important to highlight the particular risk of discrimination when drones are disproportionately used in certain territories or targeted at specific populations, reinforcing patterns of stigmatization and selective surveillance (D'Ignazio & Klein, 2020). If left unregulated, these practices may conflict with national and international human rights instruments.

17 According to the Report of the United Nations High Commissioner for Human Rights titled The right to privacy in the digital age (A/HRC/48/31, 2021), any interference with the right to privacy must pursue a legitimate purpose and also be necessary and proportionate to achieve it. This requirement becomes especially relevant in the digital age, where technological advances enable increasingly sophisticated and intrusive forms of surveillance. The report warns that the lack of adequate safeguards can turn these practices into systematic violations of fundamental rights.

Furthermore, the issues associated with the use of drones must also be analyzed in the context of digital rights[18]. As Sequera and Lara Castro (2020) argue, these rights emerged to provide a legal framework for activities related to information and communication services. Although derived from traditional human rights, digital rights have their own technical and normative characteristics[19], which can be severely impacted by the use of drones equipped with data collection technologies, thermal sensors, high-resolution cameras and remote information transmission capabilities, especially when they operate without informed consent or clear regulatory boundaries.

This concern becomes even more relevant when we consider that rights such as freedom of expression, the right to information, and the right to assembly and protest in physical spaces are increasingly interconnected with the digital ecosystem. In this sense, the ability to communicate freely, exercise digital citizenship and protect the integrity of online identity is jeopardized when technologies like drones are deployed in an opaque or intrusive manner. Aerial surveillance can thus become a mechanism of social control, deterring critical discourse and undermining the right to democratic access to the knowledge society, as noted by the United Nations Special Rapporteur on the rights to freedom of peaceful assembly and association (UN, 2019).

In this context, it is essential to recognize that human rights must be considered in all their dimensions and areas of exercise, both physical and digital. While drones may appear to belong to a "material" plane, their operation is intrinsically dependent on technological and digital infrastructure, including the internet, software, AI systems, facial recognition algorithms and data analysis platforms, which enhance their capacity for surveillance and intervention, and consequently, their potential for interference with or exploitation of fundamental digital rights.

To illustrate more clearly how the use of drones can violate fundamental rights recognized both in Paraguayan law and in international human rights instruments, a comparative table is presented below. It summarizes the main rights affected, their legal basis, the level of risk identified (high or medium), and the possible ways in which their use can impact these rights, particularly in contexts of surveillance and social control.

However, it should be noted that the table should not be interpreted strictly, since, as has been previously noted, the impact of surveillance technologies is cross-cutting and can extend to multiple spheres of social, political and private life. Nevertheless, it seeks to systematically highlight those guarantees whose impact is most evident and documented in the context of the current use of drones for control or surveillance purposes.

18 An emerging category that acknowledges the need to safeguard fundamental freedoms in the digital environment and in the face of surveillance and control technologies. (Sequera & Lara Castro, 2020)

19 Such as the right to personal data protection, net neutrality, universal access and the right to encryption and anonymity.

TABLE 1. Comparative table of affected rights and levels of risk

Right/ Guarantee	Constitution of the Republic of Paraguay	Universal Declaration of Human Rights	American Convention on Human Rights	Risk level	Possible Impact of Drones
Right to life	Art. 4 Right to life	Art. 3	Art. 4 - Right to life	HIGH	Armed drones in conflicts, lethal police use, accidents due to malfunction
Right to Liberty	Art. 9 - Liberty and Security of Persons	Art. 3 - Right to Liberty	Art. 7 - Right to Personal Liberty	HIGH	Restriction of movement due to mass surveillance, control of demonstrations
Right to Privacy	Art. 33 - Right to Privacy	Art. 12 - Protection against arbitrary interference	Art. 11 - Right to Privacy	HIGH	Unauthorized surveillance, recording of private activities, tracking of individuals
Right to Inviolability of the Home	Art. 34 - Right to Inviolability of Private Premises	Art. 12 - Protection of the home	Art. 11 - Right to Privacy	HIGH	Overflight of private property, recording of interiors, home surveillance.
Freedom of movement	Art. 41 - Right to movement and residence	Art. 13	Art. 22 - Freedom of Movement and Residence	MEDIUM	Flight restrictions that limit movement, identification and tracking of individuals.
Freedom of expression	Art. 26 - Freedom of Expression and of the Press	Art. 18 - Freedom of Thought, Conscience and Religion; Art. 19 - Freedom of Opinion and Expression	Art. 13 - Freedom of Thought and Expression	HIGH	Surveillance of demonstrations, identification of participants, deterrent or inhibiting effect.
Freedom of Assembly	Art. 32 - Freedom of Assembly and Demonstration	Art. 20 - Freedom of Assembly	Art. 15 - Right of Assembly	HIGH	Surveillance of meetings, identification of participants, dispersal through intimidation.
Right to Image	Art. 33 - Right to Privacy (protects private images)	Art. 12 - Protection against interference	Art. 11 - Right to Privacy	HIGH	Unauthorized recording, dissemination of images, facial recognition.

Data Protection	Art. 33 - Right to Privacy; Art. 34 Right to Inviolability of Private Premises	Art. 12 - Protection against interference	Art. 11 - Right to Privacy	HIGH	Mass collection of biometric data[20], profiling, unauthorized data storage.
Right to Security	Art. 9 - Liberty and Security of Persons	Art. 3	Art. 7 - Right to Personal Liberty (includes the right to personal security)	AMBIVALENT	May improve public safety but there are risks of excessive surveillance.
Due Process and Presumption of Innocence	Art. 17 - Procedural Rights	Art. 10 - Right to a Public Hearing; Art. 11 - Presumption of Innocence	Art. 7 Right to Personal Liberty; Art. 8 - Right to a Fair Trial	MEDIUM	Use of drone-collected evidence without judicial authorization. Potential for mass preventive surveillance that assumes guilt.
Non-Discrimination and Equality Before the Law	Art. 46 - Equality of Persons; Art. 47 .Guarantees of Equality	Articles 2 and 7	Art. 1 - Obligation to Respect Rights; Art. 24 - Right to Equal Protection	HIGH	Selective surveillance based on discriminatory profiles; false positives derived from biased or unrepresentative databases; unequal segmentation of public space.

Source: Own elaboration.

As the comparative analysis shows, drones are far from being a neutral technology. Their use can become a highly intrusive surveillance tool, with significant impacts on legally guaranteed human rights, especially when there are no clear limits or adequate control mechanisms in place. This concern is not abstract, given that there are numerous documented cases at the regional[21] and global levels where the use of these technologies has resulted in serious violations of rights.

In the specific case of the right to citizen security, understood as the "set of state actions aimed at guaranteeing the protection and well-being of the population" (Izquierdo-Alvear, 2024), it is essential that the use of surveillance technologies, including drones, does not justify forms of control or monitoring that generate fear or inhibit citizen participation.

20 Biometric data is "personal data obtained from specific technical processing relating to the physical, physiological or behavioral characteristics of a human being that enable or confirm their unique identification." (Vaninetti, 2020, Volume I, p. 177).

21 During mass events such as the Rio Carnival, Brazilian authorities have used drones equipped with facial recognition cameras to monitor crowds. In 2019, in Salvador de Bahía, this technology generated multiple false positives, including the unwarranted detention of individuals. A report by the Rede de Observatórios da Segurança revealed that 96% of alerts were ineffective and 90.5% of those detained were Black. These cases illustrate the risks of combining drones with biometric technologies, especially in festive public spaces, where they may infringe upon rights such as privacy, the presumption of innocence and non-discrimination. See: Lourenco, B. (2025, March 1). O reconhecimento facial no carnaval não protege, ele controla. Opinión. CartaCapital. https://www.cartacapital.com.br/opiniao/o-reconhecimento-facial-no-carnaval-nao-protege-ele-controla/.

The historical experience of our region, including Paraguay, serves as an example of the risks of normalizing surveillance mechanisms without transparency or guarantees, especially when these technologies are integrated into authoritarian or unequal frameworks. Therefore, any advancement in technology applied to security must be based on clear limits that respect human dignity. Technology can and must contribute to the common good, but never at the expense of eroding rights and guarantees that took decades of struggle and remembrance to achieve.

PRIVACY IN THE DIGITIZED PUBLIC SPACE

The expanding use of drones, by both public and private entities, poses serious challenges to the right to privacy, especially in contexts where regulatory frameworks do not evolve at the same pace as technological innovation. These challenges arise because drones "collect photographic, film and sound data from people in a peculiar way, from an aerial perspective and, in some cases, in ways that are normally undetectable." (Vaninetti, 2020. Volume I, p. 185).

In Paraguay, the right to privacy—broadly defined—has constitutional protection and is supported by international instruments such as Article 12 of the Universal Declaration of Human Rights and Article 17 of the International Covenant on Civil and Political Rights—both mentioned in the previous section. However, its effectiveness is limited by the absence of comprehensive legislation on personal data protection[22]. As TEDIC has repeatedly noted[23], while legal tools exist to invoke this right, their effectiveness depends on the presence of clear regulatory limits to govern practices like the capture of images and personal data without consent.

Although there is no specific case law on the use of drones in Paraguay, the National Constitution protects the inviolability of documentary heritage and private communications (records, writings, telephone calls, etc.). Access to this information can only be authorized by a court in cases expressly provided for by law and must be carried out with strict confidentiality regarding anything not related to the investigation. Additionally, Article 30 of the Constitution mandates that authorities ensure electromagnetic communication signals are not used to violate personal or family privacy. As Galli (2024) argues, the country's lack of comprehensive data protection legislation does not preclude the right to privacy from being legally invoked and defended in various contexts.

However, based on the institutional responses obtained through requests for access to public information, no state agency consulted has reported the existence of specific protocols that address the impacts of these technologies on privacy. While MITIC (2025) has stated that all drone operations require authorization from DINAC and documented legal justification, this requirement alone does not guarantee a thorough assessment of the impacts on human rights. For its part, the Ombudsman's Office has stated that it has no specific records of complaints related to the use of drones, which, rather than suggesting a lack of impact, highlights an institutional gap and the absence of effective monitoring mechanisms.

22 As of this writing, the Personal Data Protection Bill (Exp. D-2162170) was approved by the Chamber of Deputies on May 27, 2025, and is currently under review by the Senate. For more information, visit SilPy: https://silpy.congreso.gov.py/web/expediente/123459.

23 See: TEDIC. (2025, July 17). Paraguay needs a robust Personal Data Protection Law, with international standards and real safeguards [Blog post]. https://www.tedic.org/en/paraguay-needs-a-robust-personal-data-protection-law-with-international-standards-and-real-safeguards/

Even a superficial review of public sources reveals concerning signs regarding the use of surveillance technologies with intrusive potential. For example, on the website of the National Directorate of Public Procurement (DNCP), one can find Tender No. 471787, titled "Acquisition of surveillance drones and accessories for the ANNP" (National Administration of Navigation and Ports), whose stated objective is institutional security through day and night surveillance[24].

Nevertheless, the technical specifications of the tender detail the acquisition of drones with advanced capabilities, such as wide-angle cameras of at least 48 MP, optical zoom, thermal camera, 4K recording, and 3-axis mechanical stabilization. These features allow for precise and continuous image capture, even in low visibility conditions, which far exceeds basic facility monitoring. Thus, regardless of the stated purpose, public institutions are acquiring equipment with high surveillance capabilities, without any reports of impact assessments on fundamental rights such as privacy and personal data protection.

It is worth noting that drones can collect data with an unprecedented level of detail, from high-definition images to the possible detection of mobile phone signals (Boyle, 2020). This technical capability, combined with the absence of regulation, enables a model of persistent surveillance, where observation is carried out constantly, remotely and often silently. Surveillance is no longer episodic but has become an omnipresent possibility, progressively eroding the reasonable expectation of privacy in public spaces. As Balmaceda, Schleider, and Pedace (2021) warn, "surveillance is taking up more and more space in our lives. And, to occupy that space, it is taking away from privacy" (p. 23).

The Inter-American Court of Human Rights (IACHR) has recognized in its jurisprudence, specifically in the case of Tristán Donoso v. Panama[25] (2009), that while the right to privacy is not absolute, any limitation on it must be subject to a thorough analysis, which includes an examination of the proportionality of the adopted surveillance measures.

> The right to privacy [...] may be restricted by the States provided that their interference is not abusive or arbitrary; accordingly, such restriction must be statutorily enacted, serve a legitimate purpose, and meet the requirements of suitability, necessity, and proportionality which render it necessary in a democratic society.

Following this line of reasoning, the IACHR, in the case of Escher et al. v. Brazil[26] (2009), addressed the issue we have been highlighting in this paper: that technological advancements pose significant challenges to the right to privacy, which cannot be ignored.

> Today, the fluidity of information places the individual's right to privacy at greater risk owing to the new technological tools and their increased use. This progress [...] does not mean that the individual should be placed in a situation of vulnerability when dealing with the State or other individuals. Thus, the State must increase its commitment to adapt the traditional forms of protecting the right to privacy to current times.

24 See: DNCP. (2025, June 30). Call for Tender 471787. " Acquisition of surveillance drones and accessories for the ANNP." https://www.contrataciones.gov.py/licitaciones/convocatoria/1f047be6-591c-68b6-86f1-cf1a04e1d9e5.html#pliego

25 Inter-American Court of Human Rights. Case of Tristán Donoso v. Panamá. Judgment of January 27, 2009. Series C No. 193. https://corteidh.or.cr/docs/casos/articulos/seriec_193_ing.pdf

26 Inter-American Court of Human Rights. Case of Escher et al. v. Brazil. Judgment of July 6, 2009. https://www.corteidh.or.cr/docs/casos/articulos/seriec_200_ing.pdf

Considering this criterion, it should be noted that, in contemporary legal understanding, privacy no longer refers solely to solitary or individual seclusion; it now encompasses a range of factors that shape people's expectations of privacy when moving through public spaces. Even the activities individuals engage in within these spaces can be protected by a reasonable expectation of privacy[27]. Privacy is crucial to self-determination, as it defines how a person presents themselves to others and the types of social relationships they sustain within this framework.

A paradigmatic example in Paraguay was the case of aerial surveillance of a private residence linked to the current president, which sparked a brief debate on the limits of this technology and prompted requests for reports (El Nacional, 2025). However, such questions seem to arise only when individuals with public visibility are affected. This leads us to ask: what happens when the victims are ordinary citizens without access to institutional defense mechanisms? How many instances of silent and non-consensual surveillance must be reported before the normalization of mass monitoring is questioned?

Philosopher Shoshana Zuboff (2019), in her analysis of surveillance capitalism, warns about this trend, noting that drones, body sensors, neurotransmitters, digital assistants and other sensor-equipped devices are expected to become new sources of behavioral surplus in a model that "disregard social norms and nullify the elemental rights associated with individual autonomy" (p. 16).

Given this scenario, it is crucial to rethink the scope of the right to privacy beyond the domestic sphere. Privacy also encompasses the right to move, express oneself and assemble in public spaces without being subject to constant surveillance. Therefore, it is urgent to develop regulatory frameworks that not only limit the use of drones but also establish effective mechanisms for transparency, accountability and judicial oversight. These frameworks should include clear regulations on the access, use and storage of collected data, as well as penalties for abuse.

Ultimately, protecting privacy in the digitized public space is not just a technical or legal issue, but a fundamental defense of people's right to live without being observed, constantly subject to data extraction, or having their freedom conditioned by the fear of being surveilled.

FREEDOM OF EXPRESSION AND THE RIGHT TO PROTEST AMID THE THREAT OF AERIAL SURVEILLANCE

The use of drones in social protest contexts presents an ambivalent dynamic. On the one hand, they have been used by activists and community media as tools for documenting and reporting incidents of repression, broadening the capacity for citizen recording. On the other hand, their deployment by state forces poses serious risks to fundamental rights such as freedom of expression, assembly and the right to peaceful protest.

Although drones may offer operational advantages, such as providing real-time aerial views and facilitating risk detection, their use as a mechanism for selective surveillance and intimidation can have a chilling effect on citizen participation and dissent. These freedoms, essential pillars of any democratic society, not only guarantee the pluralistic expression of ideas but also enable social

27 The "reasonable expectation of privacy" is a legal standard established in the case Katz v. United States (1967), which holds that a person may expect certain actions or communications to remain private, even in public spaces, as long as this expectation is socially recognized as legitimate. For example, someone walking through a quiet park could reasonably expect not to be recorded or followed by a drone, unlike someone attending a public demonstration in front of Congress, where surveillance may be more justifiable, though not unlimited. This distinction is crucial when assessing whether an intervention infringes on the right to privacy.

oversight of public power. In this regard, the IACHR has emphasized that freedom of expression is a cornerstone of the structure of a democratic society, and that its erosion jeopardizes the fundamental principles that sustain such a system[28].

Cases such as Colombia during the social unrest of 2021 (Fundación Karisma, 2021) or Argentina in 2023 illustrate this dynamic: drones flying over demonstrations, capturing images of people without their consent and fostering a sense of constant surveillance. In the Argentine case, the images captured were even used to threaten protesters with cuts to social benefits, showing how surveillance can operate as a form of discipline and selective punishment (R3D, 2023).

In Paraguay, agencies consulted in the course of this investigation, such as MITIC (2025) and the Ombudsman's Office (2025), have indicated that drones have not been used to monitor demonstrations or public gatherings. Likewise, the Ministry of the Interior (2025)—the institution responsible for coordinating internal security forces—did not provide an exhaustive response to the questionnaire submitted, which sought to determine whether police forces use drones to monitor protests or social mobilizations. Instead, the Ministry merely stated that "there are no drones in the technological departments of the Ministry of the Interior, nor are they used," without clarifying whether other subordinate units or forces have this type of technology or whether deployments have been carried out in coordination with other institutions[29]. Despite this, it is worth noting that TEDIC has documented forms of surveillance during demonstrations "through cameras with facial recognition and drones" (Ramírez, 2015)[30].

The chilling effect of these practices is not insignificant. As López and Torres (2021) warn, the excessive use of drones at protests can be perceived as mass surveillance, reducing the space for citizen expression and eroding the principle of freedom in democratic participation. In this sense, when individuals feel they are being watched, they may self-censor or refrain from attending demonstrations, particularly those belonging to historically stigmatized or repressed groups. In the words of García and Pérez (2023), any restriction on freedom of expression or assembly must be "proportionate" in accordance with international human rights standards. This implies that the mere possibility of disorder or the alleged need to maintain public order cannot, by itself, justify the intensive use of aerial surveillance technologies.

Globally, Russia has used drones to surveil pro-democracy protests since 2012, and the Russian National Guard employs this technology to monitor political demonstrations (Boyle, 2020). A more recent case in India eloquently illustrates the deterrent and repressive power of these technologies (Saaliq, 2024). In February 2024, police suppressed a farmers' protest by dropping tear gas from drones onto a crowd heading toward New Delhi. Such practices, in addition to violating the right to protest, illustrate a concerning use of aerial technologies that replaces human mediation and heightens the risks of excessive use of force.

---

28 See: Inter American Court of Human Rights (IACHR). (1985). Advisory Opinion OC-5/85 of November 13, 1985. Compulsory Membership in an Association Prescribed by Law for the Practice of Journalisms. (Arts. 13 y 29 American Convention on Human Rights). https://www.corteidh.or.cr/docs/opiniones/seriea_05_ing.pdf

29 To access the submitted document, see: Ministry of the Interior. (2025, July 10). Memorandum DGTYC No. 055/2025. Request 93397. Unified Public Information Portal. https://informacionpublica.paraguay.gov.py/#!/ciudadano/solicitud/93402https://informacionpublica.paraguay.gov.py/#!/ciudadano/solicitud/93397

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

The situation is further aggravated in authoritarian contexts or those with weak institutions, where anonymity in political dissent becomes a basic security requirement. As international literature warns, the advancement of technologies such as drones could make "anonymous dissent eventually impossible" by allowing governments to monitor, identify and punish protesters without the need for physical presence (Boyle, 2020). In these scenarios, the cost of political participation rises dramatically, consolidating surveillance regimes that undermine democracy at its grassroots level.

In view of the above, it is essential to emphasize that the use of drones in protest contexts must be governed by unwavering respect for human rights. These technologies cannot be transformed into instruments for criminalizing dissent, selectively monitoring dissident groups (Silva & Varón, 2021), or generating databases without informed consent (Vaninetti, 2020, Volume I, p. 180). A truly democratic society is defined not only by its capacity for innovation, but also by its commitment to protecting dissent. Along these lines, in 2020, the United Nations High Commissioner for Human Rights strongly warned that new technologies—such as drones with high surveillance capabilities—should not be used to track, intimidate or repress individuals exercising their right to peaceful protest (United Nations, 2020).

LEGALITY AND PROPORTIONALITY IN TECHNOLOGICAL SURVEILLANCE MEASURES

Any analysis of the challenges posed by drone use cannot be conducted in isolation. Instead, it must be framed within a broader context: the impact that emerging technologies, particularly those designed for surveillance, have on the law. In this regard, the deployment of drones for security purposes must be evaluated in accordance with human rights standards. Even in the absence of specific regulations, there are legal principles and tools—such as proportionality testing—that allow clear limits to be set on state and private power, ensuring that all technological interventions respect the democratic and rights-based framework.

In Paraguay, we do not have specific legislation on the use of drones with a focus on human rights, although its consideration has been proposed. At the operational level, instruments such as DINAC Resolution No. 2170/17[31] establish technical and aviation safety requirements, but do not address the impact on fundamental rights. However, this does not prevent us from stating that the implementation of these technologies can comply with legal criteria, as there is a regulatory framework that requires adherence to certain rules to protect human rights. In light of this, the legal foundations for justifying non-intrusive use of drones should always be observed.

According to the UN Human Rights Committee (1988)[32], any surveillance measure must be "clearly defined by law," comply with the principles of necessity and proportionality, and be subject to judicial oversight. In this regard, civil society organizations such as the Electronic Frontier Foundation (EFF)[33] have stressed since 2014 that all uses of surveillance technologies (in our case, drones) must

31 To access the resolution, see: DINAC. (2017). Resolution No. 2170/2017 which approves Regulation R1103 on Remotely Piloted Aircraft (RPAC) and Remotely Piloted Aircraft Systems (RPAS). National Directorate of Civil Aeronautics. https://www.dinac.gov.py/v3/index.php/documentos1/leyes-decretos-resoluciones-circulares/item/1814-resolucion-n-2170-2017-por-la-que-se-aprueba-el-reglamento-dinac-r-1103-reglamento-de-aeronaves-piloteadas-a-distancia-rpa-y-sistema-de-aeronaves-piloteadas-a-distancia-rpas

32 See: UN Human Rights Committee (HRC). (1988, April 8). CCPR General Comment No. 16: Article 17 (Right to Privacy), The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation. https://www.refworld.org/legal/general/hrc/1988/en/27539

33 See: EFF. (2014). Necessary and Proportionate: on the applications of human rights to communications surveillance. https://necessaryandproportionate.org/principles/

adhere to these principles, extending this obligation to private actors. Furthermore, the IACHR case cited above also emphasizes that surveillance measures—whether deployed by state actors or, by extension, by private entities engaged in mass or intrusive surveillance—must adhere to strict standards of legality and proportionality.

Considering these arguments, in the absence of specific regulations, the proportionality test—based on Robert Alexy's doctrine[34]—offers a robust analytical framework for assessing the legitimacy of the use of drones. This test helps determine whether a measure that affects fundamental rights can be considered constitutionally valid, through three sub-mandates: suitability, necessity and proportionality in the strict sense. According to Alexy's (1993) argumentative framework, if a state or private intervention fails any of these levels of scrutiny, it must be deemed disproportionate and, consequently, legally inadmissible. In this regard, the proportionality test not only assesses whether the use of technologies like drones serves legitimate purposes, but also whether it does so in a way that is compatible with a democratic order that prioritizes the protection of human rights. As outlined, the classic structure of this test requires the sequential verification of three specific sub-mandates:

1. **Suitability:** Does the measure effectively contribute to the proposed objective (e.g., public safety)?
2. **Necessity:** Are there less intrusive means, such as fixed cameras, greater human presence, or drones without biometric capture, to achieve the intended goal?
3. **Proportionality in the strict sense:** Does the benefit of the intervention justify the impact on fundamental rights such as privacy or freedom of assembly?

This examination is particularly important in contexts where there is a significant risk to human rights, such as protests or preventive patrols, where the use of drones can have chilling or discriminatory effects. According to the proportionality test, when the application of one principle—such as public safety—conflicts with another opposing principle—such as freedom of expression or privacy—it is necessary to assess whether the benefits of protecting the former justify the degree of restriction imposed on the latter (Pérez-Trech, 2022, p. 66). This balancing process is essential to prevent measures adopted in the name of order from eroding fundamental democratic guarantees. Likewise, the proportionality test is especially critical when drones are used by private actors, as the lack of clear limits exacerbates the power asymmetry between those who develop and implement intrusive surveillance technologies and those who are subjected to them.

In this context, the absence of safeguards such as impact assessments, citizen participation or clear legal boundaries not only compromises the legitimacy of mass drone deployment, but also creates opportunities for abuse under the justification of legitimate interests. Therefore, consistent with the arguments outlined at the beginning of this segment, the proportionality test should be understood as an essential tool for guiding institutional decisions from the outset. Its application should not be restricted to subsequent review but should be integrated into the early stages of the design, regulation and implementation of intrusive technologies in order to prevent violations of fundamental rights.

34 Robert Alexy is a renowned German legal scholar and philosopher whose theory of fundamental rights and the principle of proportionality has had a decisive influence on contemporary constitutional jurisprudence. His formulation of the proportionality test (comprising the sub-principles of suitability, necessity and proportionality in the strict sense) has become a key tool for assessing the legitimacy of restrictions on fundamental rights. This approach allows for a rational balancing of conflicts between principles and the establishment of legally justified limits on intrusive measures, making it a standard adopted by constitutional courts and international human rights instruments alike.

STATE SURVEILLANCE, SOCIAL CONTROL AND POWER STRUCTURES

This section aims to define the current context of state surveillance mediated by digital technologies, a phenomenon that has raised growing concern from a human rights perspective. As Secaf, Carrillo, and Paschoalini (2023, p. 12) point out, surveillance should not be understood as mere passive observation; rather, it is a systematic process involving three fundamental elements: observing, creating knowledge and intervening. In this context, technologies like drones enable focused and continuous monitoring of individuals or populations, with the capacity to identify behavioral patterns and, ultimately, shape behavior. Surveillance, defined in this way, ceases to be neutral and transforms into an active tool of social control.

Therefore, the use of drones and other similar technologies should not be analyzed in isolation, but rather as part of a broader framework that reproduces and amplifies historical dynamics of power concentration and the erosion of individual guarantees. These practices must be interpreted through the lens of contemporary concepts such as data extractivism, as theorized by Shoshana Zuboff (2019). From this perspective, digital technologies are not merely functional innovations, but modern forms of domination that transfer pre-existing logics of exploitation, hierarchy and inequality to the digital realm.

Data extractivism describes a systematic practice of mass, opaque, and often non-consensual collection of personal information—particularly sensitive data such as biometric and geospatial data—by state or corporate actors[35]. This form of extraction mirrors the colonial dynamics associated with the plundering of natural resources, but now it targets the informational domain[36]. In this model, citizens generate the data but have no control over its use, processing or final destination, highlighting a profound power imbalance.

The resulting architecture normalizes a type of omnipresent yet barely visible surveillance, justified in the name of seemingly unquestionable values such as security, efficiency or crime prevention, without adequate mechanisms for transparency or control. This structure institutionalizes the exception: measures introduced as extraordinary responses become consolidated as routine practices. As Pérez Trench (2024, p. 65) states, we are faced with a classic—though unresolved—tension between the state's interest in ensuring public safety and the constitutionally protected fundamental rights. "This is the classic tension between security and freedom [...] and, as any seasoned reader will realize, it is a problem that seems to have no solution."

What is concerning in the current context is that this tension is systematically resolved in favor of the expansion of state surveillance powers. The state justifies the expansion of its monitoring capabilities under the guise of its "police power,"[37] while progressively weakening citizens' ability to resist, question or even understand the true scope of such practices. This informational asymmetry constitutes a silent yet profound erosion of democratic control.

35 On this point, TEDIC has noted that these processes are often carried out without informed consent, without clear mechanisms for citizen oversight, and without transparency regarding who manages the data, for what purposes, for how long, and under what security conditions. See: TEDIC. (2025, July 23). Expo Paraguay 2025: Surveillance, Lack of Protection, and Exclusion of Citizens [Blog Post]. https://www.tedic.org/en/expo-paraguay-2025-surveillance-lack-of-protection-and-exclusion-of-citizens/

36 Data colonialism describes a new phase of systematic appropriation of personal information that reproduces colonial extractive logics in the digital environment, particularly on vulnerable populations.(Couldry & Mejias, 2019).

37 "Police power" is understood as the authority of the State to intervene in the lives of individuals in order to maintain public order and manage public affairs, even when this involves imposing limits or restrictions.

This pattern was clearly evident during the course of this investigation, particularly in the institutional responses obtained. The Ministry of the Interior replied briefly and evasively, while the National Anti-Drug Secretariat (SENAD) refused to provide information, citing vague "national security reasons." However, the inquiries did not seek operational or tactical details; they aimed to determine whether the Paraguayan state has acquired and deployed drones, in what institutional contexts, and under what legal and procedural safeguards. Paradoxically, some of this information is accessible on the DNCP website, where the award of Tender No. 435980 was published. This tender, for the "Acquisition of drones with accessories"[38] by that public entity—also awarded to DataSystems—was valued at over ₲150,000,000 and includes the DJI Matrice 300 RTK model.

This systematic refusal, combined with the lack of transparency in procurement and usage processes, not only confirms a concerning institutional opacity but also reveals, at its core, a political culture resistant to control and dismissive of the democratic value of public scrutiny. What Zuboff (2019) calls "surveillance capitalism" finds, in this context, a state-level parallel. This is characterized by the accumulation of data as a form of power, as political capital at the service of control, operating without transparency, without safeguards and without accountability.

Monitoring practices, such as the use of surveillance technologies like drones, once considered exceptional or even illegitimate, are now incorporated into bureaucratic routine, justified by discourses of modernization or efficiency. Far from genuinely enhancing citizen security, this technological surveillance architecture appears to signal the consolidation of a subtly authoritarian model, disguised as administrative innovation. We must not lose sight of the fact that what is at stake is not only the use of new tools but also how they reconfigure the relationship between the state and its citizens, between control and freedom.

THE DIGITAL PANOPTICON AND AERIAL SURVEILLANCE

Contemporary surveillance architecture finds its conceptual origins in the panopticon, a prison model devised by utilitarian philosopher Jeremy Bentham in 1791. Its architectural design allowed all inmates to be monitored from a central tower, minimizing the use of human and material resources while maximizing the effectiveness of control. Inspired by the Greek root panoptikon ("to see everything"), this model transcended its original prison function to become a powerful metaphor for new forms of state surveillance in the 21st century.

The genius of Bentham's panopticon lay not only in its operational efficiency, but also in its psychological dimension: prisoners, unable to determine when they were being observed, internalized surveillance as a constant presence. This dynamics of the "invisible but omnipresent gaze" is dramatically updated in the context of contemporary aerial surveillance technologies, where uncertainty about monitoring becomes a mechanism of widespread social discipline.

Within this conceptual framework, the deployment of drones equipped with thermal sensors, high-resolution cameras, and strategically illuminated lights during nighttime operations reflects a sophisticated evolution of the original panoptic logic. This technology operates under a dual strategy of power: on the one hand, "seeing without being seen"—the ability for remote and discretionary observation—and on the other, "strategically making oneself noticed" to remind the population that it is under the constant potential of surveillance.

38 DNCP. (2023, October 10). Call for Tender No. 435980 - " Acquisition of drones with accessories." https://www.contrataciones.gov.py/licitaciones/adjudicacion/435980-adquisicion-drone-accesorios-1/resumen-adjudicacion.html

This tactical duality represents a significant innovation over the classic panopticon. While Bentham designed an architecturally fixed and spatially delimited surveillance system, drones constitute a mobile, flexible and territorially expansive panopticon. Their capacity for three-dimensional movement and real-time operational reconfiguration allows the dynamics of prison control to be extended to urban, rural and border areas, potentially transforming the entire national territory into a space of latent surveillance.

These devices, which are increasingly autonomous, ubiquitous and economically accessible, can incorporate AI technologies such as facial recognition, predictive behavior analysis and remote biometric identification, exponentially intensifying the state's selective surveillance capabilities (Mobilio, 2023; Berle, 2020). This technological convergence not only amplifies the power of state observation, but also introduces elements of automation that can operate with minimal human intervention, creating the conditions for algorithmically mediated forms of social control.

The selectivity of this surveillance is particularly problematic from a human rights perspective. The ability of these systems to identify, track and catalog specific individuals—based on potentially discriminatory or politically motivated criteria—transforms surveillance from a general public security mechanism into a tool of differentiated political control.

In contexts of high political conflict and social unrest, such as that documented in Venezuela following the controversial presidential elections (Alarcón, 2024), the conspicuous presence of drones flying over citizen demonstrations and the official display of armed models—such as the ANSU 100 and 200, linked to Iranian technology transfer—(Bermúdez, 2022) signals a qualitatively concerning escalation towards forms of repression that are technologically mediated and potentially lethal.

This evolution marks a critical transition from surveillance to direct coercion. When observation devices incorporate offensive capabilities, the digital panopticon transforms into what we might call an "armed panopticon," where the threat of violence is structurally integrated within the surveillance architecture. This convergence between observation and automated lethal capability raises fundamental questions about the constitutional limits of state power and the mechanisms of democratic control over inherently dual-use technologies.

In scenarios characterized by the progressive militarization of public order, this convergence between ubiquitous aerial surveillance and automated offensive capabilities gives rise to what we might conceptualize as an "algorithmic territorial control regime." In this regime, the state's power of observation is systemically interwoven with the credible threat of force, frequently operating without clear guarantees of legality, proportionality or effective democratic oversight.

This model represents a problematic synthesis between the internal control dynamics characteristic of police states and the technologies of war developed for external conflicts. Its implementation in civilian contexts progressively erodes the boundaries between public security and military control, creating the institutional conditions for unprecedented forms of technologically enhanced authoritarianism.

DRONES AND THE MILITARIZATION OF CIVILIAN SPACE

The use of drones in security contexts has contributed to a growing militarization of civilian life, where technologies originally conceived for warfare are being transferred—without significant public scrutiny or specific regulation—to functions of population control, internal surveillance and repression. Following a logic of intensified security, these types of technologies have been integrated into the daily management of urban and rural airspace, blurring the boundaries between the civil and military functions and normalizing the exceptional.

In this context, the 2023-2028 Security Plan for Development[39] identifies airspace as an area of growing vulnerability and strategic interest, as it is one of the so-called "global commons" where the sovereign exercise of state control becomes more complex. Among the threats identified are drug trafficking, smuggling and other illicit aerial activities, whose proliferation jeopardizes both security and development. However, the authorities themselves recognize that structural deficiencies in radar, equipment and budget weaken the state's ability to exercise effective control, paving the way for the incorporation of new tools such as drones.

In the case of Paraguay, the actions of the Joint Task Force (FTC) in northern areas of the country clearly illustrate this phenomenon. Reports and journalistic investigations have documented the use of drones in operations against the Paraguayan People's Army (EPP)[40], often in contexts marked by limited transparency, lack of effective judicial oversight and with weak accountability mechanisms.

Similarly, in these areas of alleged EPP activity, multiple complaints suggest that this militarization serves private interests more than the social protection of communities[41]. This is reflected in a comment by Sindulfo Agüero, a resident of Alfonso Kue, Horqueta, regarding the ongoing presence of repressive forces in their communities and the abuse of power: "Opyta okyjyjepa lo mitã. Upevaera ojapo hikuei la ojapova. Omogyýje hagua (The people were left afraid. That's why they did what they did. To make people afraid)" (Benegas Vidallet, 2024).

39 To access the full document, see: National Defense Council (2023). Security Plan for Development 2023-2028. https://mdn.gov.py/wp-content/uploads/2024/11/Plan-Seguridad-para-el-Desarrollo-2023-2028.pdf

40 The Paraguayan People's Army (EPP) is a Marxist-Leninist armed insurgent group that has been operating in northern Paraguay since the 2000s. It has been identified by the Paraguayan state as responsible for kidnappings, attacks and activities linked to drug trafficking, and has been declared a terrorist organization by the Paraguayan government (Wikipedia, n.d.).

41 Among the most relevant precedents of the Joint Task Force (FTC) is the case of the deaths of 11-year-old girls María del Carmen and Liliana Villalba, which occurred on September 2, 2020, during an operation against the Paraguayan People's Army (EPP). Following an investigation, the United Nations Committee on the Rights of the Child concluded that the Paraguayan state committed serious human rights violations in relation to these events (Paraguay responsible for grave rights violations over deaths of two young girls, UN committee finds, 2025). See resolution at: https://www.ohchr.org/en/press-releases/2025/01/paraguay-responsible-grave-rights-violations-over-deaths-two-young-girls-un

In this context of opacity, the Paraguayan state seeks to "modernize" its repressive forces. An example of this is the recent training of some 40 Paraguayan Army soldiers in the use of drones[42] with search, rescue and offensive capabilities for border control (La Nación, 2025). Additionally, as reported by an international media outlet, the Paraguayan Navy has acquired EVO MAX 4N drones (Chinese technology), capable of multispectral and audio surveillance. The integration of these drones will continue with support from companies such as Datasystems, aiming for comprehensive monitoring in border areas under the supervision of state forces (Saba Manzo, 2024). These interventions consolidate a hybrid security model, where military entities and private companies expand their surveillance capabilities over the civilian population.

These reports align with the information available on the website of the National Directorate of Public Procurement (DNCP) regarding Tender No. 452492, titled "Acquisition of drones for the Paraguayan Navy."[43] According to this publication, ₲ 557,632,107 was invested through Contract No. 40/2024, awarded to the company DataSystems, for the provision of high-end drones. The technical specifications required include: a 50-megapixel wide-angle camera, a thermal camera with a resolution of 640x512, night camera with ISO sensitivity up to 300,000, transmission range up to 20 km, radar anti-collision system, compatibility with multiple GNSS systems (GPS, GLONASS, BeiDou, and Galileo), and minimum flight autonomy of 42 minutes. These features demonstrate the acquisition of equipment with high capture power, geolocation capabilities and the ability to operate in various environmental contexts, including night surveillance or extreme conditions.

Internationally, this phenomenon is not isolated. The United States has institutionalized the use of drones both in extraterritorial military operations—including targeted killings—and in domestic border surveillance (Amnesty International, 2013; Alston, 2010; García et al., 2024). Israel, for its part, has developed advanced air control systems, such as the Iron Dome, and regularly uses drones for surveillance and repression in the occupied territories, leading to complaints about excessive force and the systematic surveillance of civilians (Dworkin, 2013; Melzer, 2013).

In Latin America, Colombia presents a relevant precedent with the use of drones in counterinsurgency operations against the FARC (DeYoung, 2011). Mexico has documented the use of these technologies in border patrol, immigration control and support for military operations in urban areas (García et al., 2024). Honduras, for its part, has registered complaints about the use of drones by private agribusiness companies to intimidate more than 175 families from rural and land-defending communities (Forner, 2024).

42 As of this writing, the Paraguayan military had not responded to a request for access to public information seeking data and information on its regulations regarding drone operations and other related matters. See request at: https://informacionpublica.paraguay.gov.py/#!/ciudadano/solicitud/93452

43 See: DNCP. (2024, October 9). Call for Tender No. 452492, titled " Acquisition of drones for the Paraguayan Navy." https://www.contrataciones.gov.py/licitaciones/adjudicacion/1ef81a27-0ad0-69dc-9e86-f7c6d914c1a2/resumen-adjudicacion.html

Moreover, the concern is not limited to state use. The militarization of civilian space implies a profound transformation of the territory, as it is not merely a matter of intervention by armed forces, but rather the creation of an ecosystem based on constant surveillance, technological anonymity and mixed agents (state and private). In addition to the private sector, there is growing evidence of the use of drones by armed actors, such as insurgent groups or drug trafficking networks, who employ them for surveillance, intimidation or attacks. In fact, according to Frantzman (2021), numerous terrorist groups and non-state actors, such as ISIS, Hezbollah, the Houthis and Boko Haram, have developed or used UAVs, often by arming commercial drones.

In July 2025, the international media outlet Reuters reported that Pakistani Islamist militants used armed drones to attack security force positions, revealing the risks posed by this technology in the hands of actors without public accountability (Ali & Shahzad, 2025). Similarly, the use of "narco-drones" has been documented in countries such as Mexico (Bayoud, 2025), prompting repressive responses from both Mexican and US authorities (Muñoz Lima, 2025; El Financiero, 2025). These confrontational dynamics primarily affect the civilian population, which is left exposed to persistent surveillance and control from both sides.

Considering international experience, the eventual incorporation of drones in criminal or paramilitary operations in our country and region is also a concerning scenario, as it would give rise to parallel forms of territorial control without institutional guarantees. This process of aerial militarization—sometimes explicit, sometimes subtle and informal—challenges the principles of legality and proportionality in the use of force, and highlights the urgent need to establish regulatory frameworks that limit the use of these technologies in contexts that affect human rights and democratic ways of life.

INTERSECTIONAL PERSPECTIVE AND SELECTIVE SURVEILLANCE

GENDER, RACIALIZATION AND CONTROL TECHNOLOGIES:

As noted in previous chapters, the deployment of surveillance technologies, including drones, is far from a neutral practice. On the contrary, it tends to reproduce—and, in many cases, intensify—historical structures of inequality, domination and exclusion (Silva & Varón, 2021). In this regard, Ruha Benjamin (2019), drawing on the work of Michel Foucault, warns that technological exposure does not affect all people equally: certain bodies—racialized, feminized, impoverished, or non-conforming—are subject to disproportionate surveillance. This selective surveillance is shaped not only by the stated purposes of the technology, but also by the subjects it targets, their social conditions and their belonging to historically vulnerable groups.

Applied to the case of drones, this phenomenon translates into their intensified use in contexts such as migration control, the patrolling of low-income neighborhoods, protest management and the suppression of social demands.(Benjamin, 2019; García et al., 2024; D'Ignazio & Klein, 2020; Zuazo, 2018). In Latin America, the use of drones in social protests has been documented in Chile (Clarín, 2019) and Argentina (R3D, 2023), as well as in surveillance operations targeting indigenous communities in voluntary isolation in Brazil (Iglesias, 2022), rural populations in Panama (Front Line Defenders, 2025) and during LGBTIQ+ events, where non-conforming individuals are particularly susceptible to criminalization or recording without consent.

Internationally, there have also been reports of cases such as in Iran, where drones are used to identify and pursue women who do not comply with the dress code imposed by the regime (Foulkes & McArthur, 2025). As noted above, this type of surveillance not only violates fundamental rights such as privacy and freedom of expression, but also produces a chilling effect on the political and social participation of historically marginalized groups.

In contexts like Paraguay, characterised by high ethnic, linguistic and cultural diversity[44], and drawing on internationally reported cases, it can be expected that the integration of aerial surveillance technologies could result in significantly higher error rates for individuals with dark skin tones, indigenous or non-Eurocentric features, as well as women, older people and transgender people, intensifying patterns of exclusion and discrimination.

44 According to the National Indigenous Census (National Indigenous Institute, 2022), approximately 2% of the population identifies as indigenous, belonging to 19 indigenous peoples organized into five linguistic families. Added to this is the growing visibility of the Afro-descendant community and a majority of the population that identifies as mestizo. Furthermore, 77% of the Paraguayan population claims to be bilingual in Guaraní and Spanish, which highlights the centrality of indigenous cultural identity in the country's daily life (DGEEC, 2022). This ethnic, cultural and linguistic plurality requires differentiated approaches to prevent algorithmic biases and guarantee respect for human rights.

Given this circumstance, it is important to remember that technological discrimination does not operate in isolation. Therefore, these debates must be approached from an intersectional perspective[45]—considering the interaction between gender, race, class, sexual orientation and other categories—since the effects of using drones with surveillance capabilities can become even more harmful when multiple forms of vulnerability overlap.

This is evident in the case of facial recognition, a technology that, when integrated into drones, can amplify pre-existing algorithmic errors. Research by Buolamwini and Gebru (2019) showed that commercial facial recognition systems have significantly higher intersectional error rates, affecting black women particularly severely, who are up to 44 times more likely to be misclassified than white men.

These disparities are not accidental failures, but rather a reflection of technical and political decisions integrated into the design and training of algorithms. As D'Ignazio and Klein (2020) warn, "better detection of faces of color" does not necessarily imply an improvement if its use is aimed at expanding repressive practices. Along these lines, Safiya Noble (2018) conceptualizes "technological redlining" as the process by which digital infrastructures reproduce historical logics of exclusion, shifting practices similar to racial profiling to the algorithmic level. Thus, drones, as AI-powered devices, far from being alien to these dynamics, can become active nodes of structural discrimination.

The gender dimension embedded in these technologies cannot be ignored either. According to the GIFT Group (2021), digital artifacts are not neutral; they reflect—and often reinforce—gendered social imaginaries. Technologies "actively collaborate in the establishment of sexual division and difference" (p. 11) and are permeated by the values, interests and biases[46] of those who design them (p. 8). This sociotechnical inscription of inequality manifests itself, for example, in the fact that multiple algorithmic configurations can offer similar technical performance but have disparate impacts on different demographic groups.

As Black, Koepke, Kim, Barocas and Hsu (2024) point out, the discriminatory consequences of a system are not inevitable but rather the result of design choices that do not prioritize equity. Thus, rather than correcting inequalities, technological development may end up consolidating them. For example, the use of drones equipped with visual, thermal or biometric sensors in security, verification or automated patrol operations poses a risk of selective surveillance of racialized and feminized bodies (Silva & Varón, 2021).

To contrast conceptual analysis with institutional practice, this research involved filing public information requests to various Paraguayan state entities. The goal was to determine whether there are protocols, assessments or precedents regarding the use of drones with a focus on human rights, gender or differentiated impacts on vulnerable populations. The findings reveal a concerning absence of specific regulatory frameworks and evaluation mechanisms. MITIC (2025) acknowledged that it does not have protocols or guidelines with a human rights or gender focus in relation to the use of drones.

---

45 The concept of intersectionality was developed by African-American scholar Kimberlé Crenshaw (1989) to explain how multiple forms of discrimination—such as racism, sexism and class inequality—intertwine and generate specific experiences of oppression, particularly for Black women. In the field of technology, this approach allows us to analyze how impacts are not distributed evenly, but rather impact more intensely those who find themselves at the intersection of multiple vulnerabilities..

46 In this paper, the term bias refers to systematic errors in technologies such as drones equipped with surveillance algorithms or automated decision-making. These biases can have statistical, social or institutional roots (Bellamy, 2019) and, in the case of technologies applied to security, can lead to patterns of unequal surveillance or erroneous profiling of certain populations. Although often unintentional, they usually originate from unrepresentative data or poorly defined variables, which contributes to amplifying inequalities by disproportionately impacting vulnerable groups (Barocas & Selbst, 2016).

Similarly, the MAG (2025) responded that it is not currently deploying this technology in rural, peasant or indigenous communities, nor has it conducted studies on its social or cultural impacts. The Ombudsman's Office (2025), for its part, indicated that it has no record of complaints or interventions related to possible rights violations due to the use of drones. Finally, the Public Prosecutor's Office (2025) reported that it has not carried out any operations using drones to monitor protests, nor are there any official records of requests for authorization to do so filed with the National Directorate of Civil Aeronautics (DINAC).

These institutional responses—characterized more by omission than by foresight—not only reflect an absence of regulatory frameworks but also a structural lack of sensitivity towards the differentiated impacts of these technologies. The absence of records, assessments or specific guidelines in the Paraguayan state does not equate to an absence of risks; on the contrary, it presents a scenario where institutional opacity can normalize forms of discriminatory, silent and persistent surveillance. This systematic omission is not neutral; it has material and symbolic effects that translate into unequal impacts on different social groups.

In this context, the differentiated effects of the use of drones—and surveillance technologies in general—crystallize in forms of invisibility, hypervisibility, exclusion and persecution (Benjamin, 2019). These effects have concrete consequences in areas such as access to rights, political participation and freedom of movement in public spaces. Taking this into account, in the absence of a robust legal framework that regulates the processing of biometric data or the oversight of technologies applied to public security, there is a high probability that tools such as drones will disproportionately affect vulnerable or historically excluded groups. This impact can manifest itself both through identification errors and automated decisions that reproduce social stigmas.

This is exacerbated when technological design does not consider the inclusion of diverse communities in its development processes. In contexts such as Latin America—including Paraguay, where technology development often relies on models imported from global centers of power—there is a risk of reproducing technological architectures built on external data, values and logics (D'Ignazio & Klein, 2020; Criado Perez, 2020). As the GIFT Group (2021) warns, technology encodes worldviews, design decisions and structural exclusions. In their words, the next step in trying to influence the development of technologies with a gender perspective is

to include intersectional human resources in the teams that develop technology. We need diverse work teams that are as similar as possible to the society for which digital technologies are being created. It is necessary to include in both technical and decision-making positions people whose intersections are not usually represented in technology development, such as women who identify with Indigenous peoples, trans men, migrants, or people with disabilities, among many other intersections. (Grupo GIFT, 2021, p. 14).

Ignoring these recommendations carries the risk of consolidating more sophisticated mechanisms of exclusion under the guise of innovation, efficiency or modernization. Arguments that appeal to the supposed lack of trained intersectional personnel are untenable, particularly when, as the GIFT Group (2021) also points out, "the number of highly trained human resources expands when considering the multidisciplinarity required to develop technology." (p. 14).

Given the context described above, the implementation of intrusive technologies like drones over vulnerable communities should not be promoted without mechanisms for prior consultation, informed participation or human rights impact assessment. The debate on their adoption must be grounded in an intersectional and feminist perspective, one that moves beyond demanding technical transparency to also challenge the political responsibility of those who design, promote or implement these tools.

ASYMMETRIES IN ACCESS TO AND USE OF TECHNOLOGIES

As demonstrated by the analysis of the authors reviewed—including Benjamin (2019), Criado Perez (2020), Noble (2018), Eubanks (2018), Lara Castro (2020) and Zuazo (2018)— the profound asymmetries in access, design and application of technologies such as drones cannot be addressed solely through technical solutions. On the contrary, structural interventions are needed, combining legal regulation, conscious technological redesign and social mobilization. From evaluating the governance of technologies with the potential to impact human rights, to implementing independent audits and regional regulatory frameworks, technology must be reimagined as a space for political contestation, not as a neutral or apolitical environment.

In this sense, having a governance framework that prioritizes equity over efficiency, as well as incorporating diversity in design processes and strengthening community participation, are key steps to prevent these technologies from deepening historical inequalities. Furthermore, democratizing knowledge about technology is a vital strategy to ensure that its advances align with democratic values and social justice (Benjamin, 2019, p. 87), rather than reinforcing opaque control regimes or deepening structural exclusion.

As Ruha Benjamin (2019) warns, digital technologies often land on unequal social structures which, far from being neutralized by innovation, tend to be reproduced or even amplified. Unequal access to devices, connectivity or training is not merely a technical or infrastructure issue, but a reflection of power relations rooted in historical inequalities of gender, class and race (Noble, 2018, p. 18). Therefore, discussing the digital divide in purely quantitative terms, i.e., focusing on access to computers, software and Internet connectivity, may be insufficient or even misleading if its structural roots are not addressed (pp. 19-23).

In Paraguay, although Internet access has increased considerably in recent years, significant disparities remain. According to the National Institute of Statistics (INE), in 2024, 86.2% of the urban population uses the Internet, compared to 73.7% in rural areas[47]. Furthermore, the main use of the Internet continues to be instant messaging and social networks (INE, 2024), raising questions about the quality and depth of access and its potential for emancipation. As Eubanks (2018) notes, vulnerable populations such as people of color, migrants and the poor not only have less access, but are also the first to become subjects of monitoring and testing for automated technologies like drones or predictive algorithms.

47 For detailed information on the data reported, see: National Institute of Statistics (INE). (June 2025). Information and Communication Technology in Paraguay. EPHC 2024. https://www.ine.gov.py/publication-single.php?codec=280

This issue is exacerbated when the state, instead of facilitating equal access to technologies, deploys them selectively for surveillance or control, without ensuring spaces for participation, training or social appropriation. Such is the case in Paraguay, where, despite the existence of a National Technology Plan 2022–2030[48] that mentions digital inclusion, there are no specific programs for training or promoting the use of drones in peasant and indigenous communities, or in rural cooperatives. According to the official response from the Ministry of Agriculture and Livestock (2025), the use of drones has not been accompanied by impact assessments or guidelines aimed at rural producers.

However, regional experiences demonstrate that the democratized use of this technology is possible. In both Brazil and Peru (Collyns, 2018), Amazonian indigenous communities use drones to report oil spills and monitor their territories; in Bolivia, an Aymara woman is leading agricultural modernization processes with these devices (NTN24, 2024). These examples should not be seen as exceptions or curiosities, but rather as models of redistributing access to technology and the opportunities it provides.

Ultimately, asymmetries in access, design and use of drones cannot be resolved simply by expanding digital coverage. They require a paradigm shift that views technology as a field of political dispute, not as a preformatted solution. Democratizing their development and use, incorporating diversity into technical teams and promoting community ownership are essential steps to ensure that these tools do not reinforce hierarchies, but instead serve as means of redistributing power and guaranteeing rights.

48 The document is available at: MITIC. (2022). National ICT Plan 2022-2030. https://mitic.gov.py/plan-nacional-de-tic-2022-2030/

GLOBAL GOVERNANCE, GEOPOLITICS AND REGULATION

The advancement and proliferation of drones represent not only a technological innovation but also, as Frantzman (2021) notes, a substantial reconfiguration of the global balance of power, accelerating the race for dominance. Far from being limited to their civilian applications—such as those mentioned in the previous sections—drones have become strategic tools for geopolitical influence, defense, security and surveillance.

This situation has also influenced emerging regulatory frameworks, shaping who regulates, for what purposes, and for whom. A notable example is the Executive Order signed by Donald Trump in 2025, which underscores the need to ensure "U.S. dominance in drones" by strengthening domestic production chains and reducing reliance on foreign components (Trump, 2025). This measure is part of a broader strategy of technological reshoring[49], aimed at countering China's growing influence in the global RPAS (Remotely Piloted Aircraft Systems) market.

This context has given rise to a new type of "covert militarization" of technologies that are nominally civilian, enabling their integration into policing, immigration control or domestic intelligence functions without specific legal frameworks. This raises substantial concerns about the principle of legality and due process, especially in democratic contexts. In the absence of binding standards, this instrumentalization increases the risk of regulatory fragmentation on a global scale, in an international environment already strained by strategic rivalries, the erosion of multilateralism and unilateral responses to real or perceived threats (Cocchini & Bermejo García, 2020; Boyle, 2020). This is further compounded by complex dynamics such as the conflict between Israel and Gaza, the use of drones in Ukraine, and the growing militarization of borders in the Americas and Europe (Korać, 2023).

From a Latin American perspective, this scenario poses a significant dilemma, as the importation of strategic surveillance technologies without a solid regulatory architecture imposes technical frameworks and operational dynamics designed by exporting jurisdictions (Access Now, 2021). As the Access Now report warns, this asymmetry limits recipient countries' ability to develop regulations that align with their constitutional and sociopolitical realities. This issue, as will be explored in the following subsection, is particularly relevant in the case of Paraguay.

In fact, according to the analysis in the aforementioned report, in countries with weak institutions and technological dependence—such as Paraguay—this tension manifests at multiple levels. The importation of aerial surveillance infrastructure without adequate democratic oversight involves not only the acquisition of hardware, but also the implicit transfer of usage models, operational protocols and conceptions of the balance between security and fundamental rights.

49 Reshoring is the practice of bringing back to the country productive activities that were previously carried out abroad. In the US, the government has promoted this strategy, especially in key technology sectors.

Without a contextualized regulatory framework, there is a risk of consolidating intensive surveillance practices as de facto norms, bypassing public debate, legislative control or judicial review. Indeed, authors Frantzman (2021) and Boyle (2020) have warned that the widespread use of commercial drones, such as those from DJI—acquired by state entities in our country, as reported above—has raised concerns about potential surveillance by China, since there have been reported incidents of hacking that compromised drone transmissions, including those of the MQ-1 Predator and MQ-9 Reaper.

On an international scale, although there is no explicit and binding regulatory regime specifically governing the civil and military use of drones, authors Cocchini and Bermejo García (2020) argue that "the rules that apply to armed drone operations are the same as those that apply to other weapons" (p. 104). In this sense, instruments such as the International Covenant on Civil and Political Rights (ICCPR) and the American Convention on Human Rights (ACHR)—which guarantee rights such as privacy, life and due process—are applicable, especially when the deployment of drones threatens fundamental rights. However, the effective implementation of these standards faces persistent tensions in complex geopolitical scenarios, continuing to pose a significant regulatory challenge.

Similarly, various other international instruments provide important regulatory frameworks. In contexts of armed conflict, the 1949 Geneva Conventions[50] impose principles such as distinction, proportionality and military necessity. The Johannesburg Principles on National Security and Freedom of Expression (1995)[51] offer non-binding but very important interpretive guidelines, such as the requirement that any restrictive measure must be legal, proportional and subject to effective judicial control.

For its part, the UN Special Rapporteur on privacy has repeatedly warned about the risks associated with the widespread use of drones without proper oversight or accountability mechanisms. The IACHR has developed standards on state surveillance and human rights, while UNESCO and the Organization for Economic Cooperation and Development (OECD)[52] have proposed ethical principles on emerging technologies, promoting frameworks focused on rights and principles such as transparency and fairness.

50 The 1949 Geneva Conventions and their Additional Protocols form the core of international humanitarian law. These four international treaties establish rules to limit the effects of armed conflict and protect those not directly involved in hostilities—such as civilians, medical and humanitarian personnel—as well as those no longer participating, such as the wounded, sick, shipwrecked, or prisoners of war. For the full text and official commentaries, see: International Committee of the Red Cross (ICRC). The Geneva Conventions and their Commentaries – Useful Links.
Available at: https://www.icrc.org/en/law-and-policy/geneva-conventions-and-their-commentaries#text940076

51 ARTICLE 19. (1996). The Johannesburg Principles on National Security, Freedom of Expression, and Access to Information. https://www.article19.org/wp-content/uploads/2018/02/joburg-principles.pdf

52 The UNESCO Recommendation on the Ethics of Artificial Intelligence (2021) was adopted by consensus by all 193 Member States, including Paraguay. This instrument sets out principles and guidelines for the responsible design and use of emerging technologies, including specific safeguards for the protection of human rights, inclusion and social justice. For its part, the OECD has developed a set of principles on artificial intelligence (Principles on AI, 2019) that promote respect for human rights, transparency, accountability and human-centered development. Although not binding, both frameworks constitute key international references for the ethical and democratic governance of technologies such as drones and automated systems.

Finally, Delegated Regulation (EU) 2023/659 of the European Commission[53], which addresses the risks posed by civilian drones, also serves as an example of a regional regulatory response It proposes preventive measures in traceability, export control and cross-border cooperation. However, it also reveals the difficulties of coordinated governance in contexts marked by security agendas. For its part, no similar regulations have been identified within MERCOSUR.

Ultimately, documented cases—especially in armed conflict scenarios—show that the existence of applicable regulatory frameworks does not in itself guarantee effective compliance. Their concrete implementation depends on factors such as political will, institutional capacity and regulatory adequacy to the local context. However, this difficulty should not be interpreted as an excuse to ignore the validity of legal standards applicable to the intrusive use of surveillance technologies. In this sense, Paraguay—and the region—face the unavoidable challenge of translating these principles into robust and effective regulatory frameworks.

THE PARAGUAYAN CASE: REGULATORY FRAGMENTATION AND TECHNOLOGICAL SOVEREIGNTY

In Paraguay, the regulation of drone use is fragmented and still in its early stages, with a legal framework that primarily addresses technical and operational aspects. The current regulations are structured around three main instruments[54]:

- Law No. 1860/2001—Paraguayan Aeronautical Code, which generally regulates civil air navigation;
- DINAC Resolution No. 2170/2017, which approves Regulation R1103 on Remotely Piloted Aircraft (RPAC) and Remotely Piloted Aircraft Systems (RPAS), establishing requirements for registration, classification, authorizations, flight altitudes, weather conditions and insurance;
- The 1944 Chicago Convention[55], Article 8 of which establishes that all unmanned aircraft require special authorization to fly over national territory.

In terms of their specific scope of application, these three instruments constitute the current regulatory framework, albeit with obvious limitations concerning rights and guarantees. As evidenced by several of the cases analyzed in this paper, the current framework omits critical dimensions associated with the state's use of drones for surveillance, territorial control, internal security or intelligence activities. Specifically, express provisions are required regarding privacy, personal data protection, accountability, judicial oversight and fundamental rights impact assessments. This is necessary to prevent the use of these technologies—particularly by the state—in a legal gray area that is unregulated and potentially harmful.

53 See: Commission Delegated Regulation (EU) 2023/659 of 2 December 2022 amending Regulation (EU) No 452/2014 as regards the technical requirements and administrative procedures related to air operations of third country operators. https://eur-lex.europa.eu/eli/reg_del/2023/659/oj/eng

54 To consult the relevant regulatory documents, you can access the official DINAC website in the section "Laws, Decrees, Resolutions and Circulars": https://www.dinac.gov.py/v3/index.php/documentos1/leyes-decretos-resoluciones-circulares

55 See: https://www.dinac.gov.py/downloads/stai/convenio_chicago.pdf

In turn, this regulatory gap must be analyzed in the context of weak, centralized and fragmented institutions, where the governance framework tends to be reactive, dispersed and lacking in effective multisectoral participation. This situation is further exacerbated by recent attempts to redefine the governance of the digital environment from a security and national defense perspective[56].

In fact, the current debate on cybersecurity in Paraguay clearly illustrates this conflict. The National Cybersecurity Strategy 2025–2028[57], led by MITIC, sets as its central objective "to protect the country's critical infrastructure and strengthen national cybersecurity." While the strategy proposes inter-institutional governance, it also incorporates the Ministry of National Defense, the Armed Forces and the National Intelligence Secretariat as central actors. This "operational integration" is presented as necessary in the face of hybrid threats, but it shifts governance from a civilian to a militarized approach.

In this regard, TEDIC (2024) has warned that this approach contradicts international best practices[58], which recommend that cybersecurity frameworks—and by extension, the regulation of emerging technologies such as drones—be led by civilian agencies, with mechanisms for transparency, multisectoral participation and respect for the rule of law. The proposal to assign stewardship of the national cybersecurity system to the Ministry of National Defense—currently under legislative debate—illustrates this trend towards the securitization of the digital ecosystem, with direct consequences for democratic legitimacy and the protection of rights in technological environments.

At the same time, the Strategic Security Plan for Development 2023–2028[59], approved by the National Security Council, promotes an approach of "unprecedented urgency" to address hybrid threats. This rhetoric—which justifies "extraordinary and urgent actions and investments"—paves the way for the normalization of the use of intrusive technologies such as drones in contexts without judicial oversight or a clearly defined regulatory framework.

In this context, the acquisition and deployment of drones by both public and private entities occur in environments marked by low transparency, lack of parliamentary oversight[60] and weak judicial control. The absence of specific national legislation regulating the use of drones for surveillance—especially within internal security operations—stands in stark contrast to the international standards previously analyzed, which stress that all surveillance technologies must be governed by law, proportional to their intended purpose and subject to rigorous judicial control.

For its part, the adoption of the Chicago Convention entails minimum international commitments but does not replace the need for comprehensive national legislation. Likewise, DINAC Regulation R1103, focused on operational criteria, cannot address the requirements of constitutionality, transparency, and the protection of rights in the state's use of drones.

---

56 See: Sequera Buzarquis, M. (2025, June 24). The Evolution of Cybersecurity in Paraguay: MITIC as a Strategic Pillar. TEDIC. https://www.tedic.org/en/the-evolution-of-cybersecurity-in-paraguay-mitic-as-a-strategic-pillar/

57 Full document available on the MITIC archive platform. https://drive.mitic.gov.py/s/ZS7YXfEJrxfgdia?dir=/&editing=false&openfile=true

58 See: Sequera Buzarquis, M. (2025, June 23). Cybersecurity in Paraguay: between urgency and legislative improvisation. TEDIC. https://www.tedic.org/en/cybersecurity-in-paraguay-between-urgency-and-legislative-improvisation/

59 Full document available at https://mdn.gov.py/wp-content/uploads/2024/11/Plan-Seguridad-para-el-Desarrollo-2023-2028.pdf

60 At the time of writing this report, the D-2478767 File, corresponding to the bill "Creating the Drone Registry and Regulating its Use in the Republic of Paraguay," presented in 2024 by Congressman Luis Federico Franco, is still under review. However, no significant progress has been made in its legislative processing. See: Silpy (n.d.). https://silpy.congreso.gov.py/web/expediente/134187

Given the current situation, the state's use of drones in Paraguay remains a discretionary practice, without clear limits or adequate oversight mechanisms. In the absence of effective safeguards, the airspace could turn into a new zone of legal exception, where opacity prevails over the rule of law. It is therefore urgent to establish a legal framework that combines international standards, constitutional guarantees and democratic oversight mechanisms in the use of aerial surveillance technologies.

TABLE 2. Regulatory frameworks applicable to drone technology

Regulatory instrument	Relevant content
Law No. 1860/2001 – Paraguayan Aeronautical Code	Establishes general principles on civil aviation. Does not specifically regulate the use of drones or aspects related to fundamental rights.
DINAC Resolution No. 2170/2017, which approves Regulation R1103 on Remotely Piloted Aircraft (RPAC) and Remotely Piloted Aircraft Systems (RPAS)	Classifies and regulates technical aspects of drones (RPAS), such as flight altitudes, insurance and restricted areas.
1944 Chicago Convention on International Civil Aviation (Article 8)	Requires special authorization for unmanned aircraft to fly over national territory.
National Cybersecurity Strategy 2025–2028	Includes the integration of the Ministry of Defense into digital governance, which could be seen as a risk of militarization of previously unregulated areas and a weakening of rights guarantees.
Strategic Security Plan for Development 2023–2028	Proposes urgent responses to hybrid threats and justifies high-tech acquisitions. Does not include controls on the state use of drones.

Source: Own elaboration

LIMITATIONS OF THE STUDY

Like all exploratory research addressing sensitive issues related to security, state surveillance and human rights, this study faces a number of limitations that must be acknowledged.

First, significant restrictions on access to public information persist. These difficulties arise, on the one hand, from the lack of active transparency within state institutions and, on the other, from the classification of certain data under the category of "national security" or, directly, from the absence of systematic records on the use of aerial surveillance technologies such as drones. Although formal requests for access to information were submitted—as detailed in the body of the report—the responses obtained were, in many cases, partial, ambiguous or simply nonexistent. Specifically, at the time of completion of this study, key entities such as the Ministry of Defense had not responded to inquiries, which limits the traceability of institutional practices and complicates the identification of responsibilities.

Second, at the methodological level, we recognize the inherent difficulty of quantifying the impact of these technologies on rights such as privacy, especially in contexts where there are no registration mechanisms or citizen oversight protocols. Furthermore, as this is a desk study based mainly on public and secondary sources, it is possible that not all relevant use cases have been mapped, especially considering that in the Paraguayan context there is no systematic monitoring of this type of technology, as is the case in conflict zones at the international level.

Finally, these limitations do not invalidate the findings presented, but they do require a cautious and contextualized reading of the results. In this regard, efforts have been made to strengthen the validity of the analysis through triangulation of sources, methodological transparency and constant critical reflection on the scope and limits of the available evidence.

RECOMMENDATIONS

Given the increasing use of drones in Paraguay and their implications for fundamental rights, we recommend the following:

- Strictly regulate their use, guided by the precautionary principle, to prevent misuse and ensure that civil liberties are not compromised. International precedents, such as the reversal of facial recognition policies due to non-compliance with security and human rights standards, provide lessons that can be applied to unmanned aerial systems.

- Strengthen institutional control mechanisms and public awareness of regulations, ensuring adequate specialized legal advice for all actors in the drone lifecycle—from engineers and designers to distributors, pilots and end-users.

- Improve monitoring and traceability systems, from manufacturing to device operation. This should include regular inspection of workshops, enforcement of technical standards and effective control over the supply chain to prevent the circulation of irregular or unregistered drones.

- Design clear, accessible and up-to-date regulations that include safeguards for privacy, data protection, due process and other fundamental rights, in alignment with international standards.

- Implement educational campaigns and training materials aimed at both operators and public and private institutions. These should include practical guides, workshops and audiovisual materials that clearly explain legal requirements, no-fly zones, privacy obligations, and the legal consequences of misuse.

- Establish transparency and accountability mechanisms for the state's use of drones, especially in security operations. This includes creating public information platforms, proactively publishing data on deployments and acquisitions, and establishing effective channels for reporting, monitoring, and redressing potential abuses.

CONCLUSIONS

The use of drones presents challenges and opportunities that must be addressed urgently from a democratic perspective, with a focus on human rights and technological justice. Despite their potential benefits—in areas such as logistics, agriculture and environmental monitoring—their deployment in surveillance and security contexts, without robust regulatory frameworks, can result in intrusive, opaque and disproportionate practices.

Paraguay faces a critical situation: a fragmented legal framework, weak institutions and a growing trend towards the securitization of the digital environment. In this context, the regulatory gap enables the discretionary use of aerial surveillance technologies, without sufficient guarantees of transparency, oversight or redress.

Therefore, it is urgent to move towards comprehensive regulation of drone use, combining technical standards with principles of legality, proportionality and democratic control. Only in this way can we prevent these devices, originally designed for innovation, from becoming instruments of control that erode the fundamental freedoms that sustain our rule of law.

EPILOGUE

At the end of this journey, in which we have critically examined the implications of drone use from a legal, ethical and social perspective, it is worth revisiting poetry as another powerful form of resistance and denunciation. To this end, we turn to this excerpt from the poem The Drone, by writer Clint Smith[61], which confronts us with the paradoxes of technological development, its ability to camouflage itself and cross borders. Beyond regulatory frameworks and technical analyses, many more insights and dialectical problems surrounding drones remain to be explored:

> "...the drone has learned to disguise itself as a shard of sky the drone's soft hum is a disembodied echo the drone was mistaken for a star once the drone renders itself celestial the drone scoffs at sovereignty the drone asks *what is a border if you can fly right over it?* he drone was built by a man the drone killed a man & a woman & a child the drone killed a child & did not see her face the drone does not see a face the drone sees a body & then the body is gone".

61 Smith, C. (2018). *the drone.* Poetry Foundation. https://www.poetryfoundation.org/poetrymagazine/poems/147872/the-drone

BIBLIOGRAPHY

1. Abraham, Y. (2025, July 18). “Como un videojuego”: Israel lleva a cabo evacuaciones en Gaza con drones lanzagranadas. *Viento Sur.* https://vientosur.info/como-un-videojuego-israel-lleva-a-cabo-evacuaciones-en-gaza-con-drones-lanzagranadas/

2. Access Now. (2021). *Surveillance Tech in Latin America: Made Abroad, Deployed at Home*. https://www.accessnow.org/wp-content/uploads/2021/08/Surveillance-Tech-Latam-Report.pdf

3. Aguado-Guadalupe, G. (2021). Privacidad frente al uso de drones con fines periodísticos. Marco regulador de Estados Unidos y Europa. *Revista de Comunicación, 20*(1), 11-27.

4. Alarcón, Á. (2024, August 28). Venezuela’s many means of surveillance and control. *Access Now.* https://www.accessnow.org/the-many-means-of-surveillance-and-control-in-venezuela/

5. Alexy, R. (1993). *Teoría de los derechos fundamentales*. Madrid: Centro de Estudios Constitucionales.

6. Alexy, R. (2019). *Ensayos sobre la teoría de los principios y el juicio de proporcionalidad.* Lima: Palestra Editores.

7. Ali, M., & Shahzad, A. (2025, July 21). Pakistani Islamist militants use drones to target security forces, officials say. *Reuters*. https://www.reuters.com/world/asia-pacific/pakistani-islamist-militants-use-drones-target-security-forces-officials-say-2025-07-21/

8. Amnesty International. (2013). *“Will I be next?”: US drone strikes in Pakistan.* London: Amnesty International Publications. https://www.amnestyusa.org/sites/default/files/asa330132013en.pdf

9. Balmaceda, T., Schleider, T., & Pedace, K. (2021). Bajo observación: inteligencia artificial, reconocimiento facial y sesgos. *ArtefaCToS. Revista de estudios sobre la ciencia y la tecnología, 10*(2), 21–43. https://doi.org/10.14201/art20211022143

10. Barocas, S., & Selbst, A. D. (2016). Big data’s disparate impact. *California Law Review, 104*(3), 671–732. https://doi.org/10.2139/ssrn.2477899

11. Bayoud, A. (2025, June 16). ‘Narcodrones’: la nueva amenaza criminal en México. *France 24*. https://www.france24.com/es/américa-latina/20250616-narcodrones-la-nueva-amenaza-criminal-en-méxico

12. Bellamy, R. K. E. (2019). AI Fairness 360: An extensible toolkit for detecting and mitigating algorithmic bias. *IBM Journal of Research and Development, 63*(4/5), 4:1–4:15. https://doi.org/10.1147/JRD.2019.2942287

13. Bentham, J. (1791). *Panopticon: Or, the inspection-house.* Dublin: Thomas Byrne.

14. Benegas Vidallet, J. (2024). E’a | Con la militarización en el Norte se intentó destruir la agricultura familiar. *E’a Periodico Informativo.* https://ea.net.py/con-la-militarizacion-en-el-norte-se-intento-destruir-la-agricultura-familiar/

15. Bermejo García, R., & Cocchini, A. (2020). Los drones a la luz del Derecho Internacional Humanitario (DIH). *Anuario Español de Derecho Internacional, 36*, 27-104. https://doi.org/10.15581/010.36.27-104

16. Bermúdez, Á. (2022, November 30). Cómo Venezuela se convirtió con la ayuda de Irán en el "único país latinoamericano que cuenta con drones armados". *BBC Mundo*. https://www.bbc.com/mundo/noticias-america-latina-63670715

17. Black, E., Koepke, J. L., Kim, P. T., Barocas, S., & Hsu, M. (2024). Less discriminatory algorithms. *Georgetown Law Journal, 113*(1), 1–68. https://doi.org/10.2139/ssrn.4590481

18. Boyle, M. J. (2020). *The drone age: How drone technology will change war and peace.* Oxford University Press.

19. Browne, R. (2015, June 25). A Drone Is Flying Abortion Pills From Germany to Poland This Weekend. *Vice*. https://www.vice.com/en/article/a-drone-is-flying-abortion-pills-from-germany-to-poland-this-weekend/

20. Castleman, T., & Toohey, G. (2025, January 9). Drone crash disabled a firefighting plane. Many irate with 'shameful' operator. *Los Angeles Times*. https://www.latimes.com/california/story/2025-01-09/drone-collides-with-firefighting-aircraft-over-palisades-fire-faa-says

21. Chocarro, S. (2017). *International standards on freedom of expression: A basic guide for legal practitioners in Latin America and the Caribbean.* CIMA. https://www.cima.ned.org/wp-content/uploads/2019/02/CIMA-LatAm-Legal-Frameworks-Guide_English_web-150ppi.pdf

22. Clarín. (2019, November19). Por qué los manifestantes chilenos usan punteros láser en las marchas. https://www.clarin.com/mundo/manifestantes-chilenos-usan-punteros-lasers-marchas_0_FeU7smoT.html

23. Collyns, D. (2018, February 16). Perú: comunidades indígenas usan drones para vigilar el ambiente en la Amazonia. *Nodal*. https://www.nodal.am/2018/02/comunidades-indigenas-usan-drones-vigilar-ambiente-la-amazonia/

24. Diario Constitucional (2021, February 17) Corte de Rancagua desestima recurso de nulidad contra sentencia que absolvió a cuatro acusados en juicio donde se presentó prueba ilícita obtenida con un dron. . . https://www.diarioconstitucional.cl/2021/02/17/corte-de-rancagua-desestima-recurso-de-nulidad-contra-sentencia-que-absolvio-a-cuatro-acusados-en-juicio-donde-se-presento-prueba-ilicita-obtenida-con-un-dron/

25. Couldry, N., & Mejias, U. A. (2019). *The Costs of Connection: How Data Is Colonizing Human Life and Appropriating It for Capitalism.* Stanford University Press.

26. Crenshaw, K. (1989). Demarginalizing the intersection of race and sex: A Black feminist critique of antidiscrimination doctrine, feminist theory and antiracist politics. *University of Chicago Legal Forum, 1989*(1), 139–167.

27. Criado Pérez, C. (2020). *Invisible women: Exposing data bias in a world designed for men.* Penguin Random House UK.

28. Custodio, J., & Abeledo, H. (2023). Drone-Based Environmental Emergency Response in the Brazilian Amazon. *Drones, 7*(9), 554. https://doi.org/10.3390/drones7090554

29. DCD. (2025, January 22). Alemania despliega un dron submarino para patrullar el mar Báltico. https://www.datacenterdynamics.com/es/noticias/alemania-despliega-un-dron-submarino-para-patrullar-el-mar-baltico/

30. DCD. (2025, February 26). Pilotos de Vodafone utilizan drones equipados con nodos Taara para conectividad de emergencia. https://www.datacenterdynamics.com/es/noticias/pilotos-de-vodafone-utilizan-drones-equipados-con-nodos-taara-para-conectividad-de-emergencia/

31. ECLAC. (2021). *Afro-descendants and the matrix of social inequality in Latin America: Challenges for Inclusion*. Economic Commission for Latin America and the Caribbean (ECLAC). https://repositorio.cepal.org/server/api/core/bitstreams/d9d10dfc-7b53-4497-84a3-76d87a426e0b/content

32. General Directorate of Statistics, Surveys and Censuses (DGEEC). (2022). *Encuesta Permanente de Hogares: Características de la Población*. https://www.ine.gov.py

33. D'Ignazio, C., & Klein, L. F. (2020). *Data feminism.* MIT Press.

34. De Vega, L. (2025, June 9). Dentro de un taller de drones camuflado, a un paso del frente en Ucrania. *El País.* https://elpais.com/internacional/2025-06-09/dentro-de-un-taller-de-drones-camuflado-a-un-paso-del-frente-en-ucrania.html

35. DeYoung, K. (2011, March 23). WikiLeaks: Colombia began using U.S. drones for counterterrorism in 2006. *Washington Post.* https://www.washingtonpost.com/world/wikileaks-colombia-began-using-us-drones-for-counterterrorism-in-2006/2011/03/23/AB0nTjLB_story.html

36. Dilawar, A. (2024, December 19). Anti-genocide activists target Israeli drone manufacturer in Brooklyn. *Truthout*. https://truthout.org/articles/anti-genocide-activists-target-israeli-drone-manufacturer-in-brooklyn/

37. Dworkin, A. (2013). *Drones and targeted killings: Defining an EU position (Policy Brief)*. European Council on Foreign Relations. https://ecfr.eu/archive/page/-/ECFR84_DRONES_BRIEF.pdf

38. Edmonds, J., & Bendett, S. (2023, March 31). *Russia's use of uncrewed systems in Ukraine (Report No. DRM-2022-U-034223-Final)*. Center for Naval Analyses. https://www.cna.org/analyses/2023/05/russias-use-of-drones-in-ukraine

39. El Financiero. (2025, February 18). CIA usa drones 'antiterroristas' en México para espiar cárteles mexicanos, revela CNN. https://www.elfinanciero.com.mx/nacional/2025/02/18/cia-usa-drones-antiterroristas-en-mexico-para-espiar-carteles-mexicanos-revela-cnn/

40. El Nacional. (2025, January 29). Solicitan informes a Dinac sobre uso de drones en zona de residencia de Peña en San Bernardino. https://elnacional.com.py/politica/solicitan-informes-dinac-sobre-uso-drones-zona-residencia-pena-san-bernardino-n80602

41. Engels, F. (1884). *The Origin of the Family, Private Property and the State.* Marxist Internet Archive. https://www.marxists.org/archive/marx/works/download/pdf/origin_family.pdf

42. Foulkes, I., & McArthur, T. (2025, March14). Iran using drones and apps to enforce women's dress code. *BBC News.* https://www.bbc.com/news/articles/c0kg15jkpdeo

43. Forner, G. (2024, August 26). María Alemán (campesina): "Cada noche me vigilan cuatro drones". *El Salto.* https://www.elsaltodiario.com/honduras/maria-aleman-defensora-tierra-cada-noche-me-vigilan-cuatro-drones

44. Frantzman, S. J. (2021). *Drone wars: Pioneers, killing machines, artificial intelligence, and the battle for the future* (eBook). Bombardier Books.

45. Front Line Defenders. (2025, June 3). Panama: Concern over violent repression against Ngäbe-Buglé Indigenous communities amid social protests. https://www.frontlinedefenders.org/en/statement-report/panama-concern-over-violent-repression-against-ngabe-bugle-indigenous-communities

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

47. García, A., Alarcón, Á., Quijano, H., Kruger, K., Narváez, S., Alimonti, V., Flores, V., Mendieta, X. (2024, December). *Privacidad en el desplazamiento migratorio*. Coalición Latinoamericana #MigrarSinVigilancia. https://www.accessnow.org/wp-content/uploads/2024/12/Privacidad-en-desplazamiento-migratorio-Dic13-2024.pdf

48. Gholami, A. (2024). Exploring drone classifications and applications: A review. *International Journal of Engineering and Geosciences, 9*(3), 418–442. https://doi.org/10.26833/ijeg.1428724

49. GIFT Group (Balmaceda, T., Pedace, K., Lawler, D., Pérez, D., & Zeller, M.). (2021, November). *Thinking digital technology with a gender perspective.* Latam Digital.

50. Guerra, J., Castrillón, A., & Sepúlveda, M. J. (2024). *Reflexiones feministas para el desarrollo de inteligencia artificial*. Derechos Digitales.

51. ICAO. (2011). *Unmanned Aircraft Systems (UAS)*. ICAO. https://www2023.icao.int/Meetings/UAS/Documents/Circular%20328_en.pdf

52. ICRC. (2013). The use of armed drones must be subject to law—ICRC. https://www.icrc.org/es/doc/resources/documents/interview/2013/05-10-drone-weapons-ihl.htm

53. Iglesias, A. (2022, November 23). Drones espías y asesinatos en el día a día de los indígenas más aislados del mundo. *El País*. https://elpais.com/planeta-futuro/3500-millones/2022-11-23/drones-espias-y-asesinatos-en-el-dia-a-dia-de-los-indigenas-mas-aislados-del-mundo.html

54. Inter-American Commission on Human Rights. (2013, November 1). Audiencia: Utilización de drones y su impacto sobre los derechos humanos en las Américas. https://www.youtube.com/watch?v=to0EImeza30

55. IACHR. (2019). Inter-American Commission on Human Rights. Office of the Special Rapporteur for Freedom of Expression. *Protest and human rights* (III; II, p. 129). IACHR.

56. Inter-American Court of Human Rights, caso “Baena, Ricardo y otros. Excepciones preliminares”, sent. Del 2/2/2001 [serie C, n. 72, párr. 124], Serie C No. 61 (IACourtHR 2001). https://www.corteidh.or.cr/tablas/fichas/baenaricardo.pdf

57. International Human Rights And Conflict Resolution Clinic, Stanford Law School And Global Justice Clinic, & NYU School of Law. (2012). *Living Under Drones: Death, Injury, and Trauma to Civilians From US Drone Practices in Pakistan* [Data set]. Stanford International Human Rights and Conflict Resolution Clinic. https://doi.org/10.1163/2468-1733_shafr_SIM260090013

58. Isikoff, M. (2013). Justice Department memo reveals legal case for drone strikes on Americans. *NBC News*. http://www.nbcnews.com/news/investigations/justice-department-memo-reveals-legal-case-drone-strikes-americans-flna1B8246490

59. Izquierdo-Alvear, D. E. (2024, August 6). Derecho a la privacidad frente al uso de drones como mecanismo de seguridad propuesto en el Ecuador. *KAIRÓS, Revista de Ciencias Económicas, Jurídicas y Administrativas, 8*(14), 126–148. https://doi.org/10.37135/kai.03.14.07

60. Jokura, T. (2021, February). Drones mapean los bosques brasileños. *Pesquisa Fapesp*, (300). https://revistapesquisa.fapesp.br/es/drones-mapean-los-bosques-brasilenos/

61. JOUAV. (2025, May 21). *Types of drones: A complete guide to choosing the right UAV.* JOUAV. https://www.jouav.com/blog/drone-types.html

62. Kardoudi, O. (2025, June 5). La brutal batalla de drones que Ucrania libra contra Rusia explicada desde dentro. *El Confidencial.* https://www.elconfidencial.com/tecnologia/novaceno/2025-06-05/guerra-ucrania-rusia-drones-tacticas-combate_4145363/

63. Korać, S. T. (2023). Is drone becoming the new ‘apparatus of domination’?: Battlefield surveillance in the twenty-first century warfare. *Philosophy and Society, 34*(3), 377–398. https://doi.org/10.2298/FID2303377K

64. La Nación. (2025, July 8). Militares paraguayos fueron capacitados en manejo de drones para control fronterizo. https://www.lanacion.com.py/politica/2025/07/08/militares-paraguayos-fueron-capacitados-en-manejo-de-drones-para-control-fronterizo/

65. La Quadrature du Net. (2022, January 21). Les drones policiers autorisés par le Conseil constitutionnel. La Quadrature du Net. https://www.laquadrature.net/2022/01/21/les-drones-policiers-autorises-par-le-conseil-constitutionnel/

66. Lara Castro, M. (2020). *Vigilancia y derechos: recomendaciones para una regulación democrática.* TEDIC. https://www.tedic.org/uso-de-drones-covid19/

67. López, M. (2020). Proporcionalidad y vigilancia: El uso de drones en la seguridad pública. *Revista de Estudios Jurídicos, 28*(4), 67-89. https://revistadeestudiosjuridicos.com/2020/proporcionalidad-vigilancia-drones

68. Lovera, D. (2017). *Privacidad: La vigilancia en espacios públicos.* (Informe anual sobre derechos humanos en Chile 2017.). Centro de Derechos Humanos, Facultad de Derecho, Universidad Diego Portales. https://derechoshumanos.udp.cl/cms/wp-content/uploads/2020/12/9-derecho-a-la-privacidad.pdf

69. Luján, E. (2015). *Drones: Sombras de la guerra contra el terror* (First Edition). Virus Editorial.

70. Márquez, J. G. (2025, January 7). El reordenamiento regional en Oriente Medio. *Descifrando la Guerra.* https://www.descifrandolaguerra.es/reordamiento-regional-oriente-medio/

71. McMullan, T. (2015, July 23). What does the Panopticon mean in the age of digital surveillance? *The Guardian.* https://www.theguardian.com/technology/2015/jul/23/panopticon-digital-surveillance-jeremy-bentham

72. Melzer, N. (2013). *Human rights implications of the usage of drones and unmanned robots in warfare (Study No. EXPO/B/DROI/2012/12)*. European Parliament, Directorate-General for External Policies of the Union. https://www.europarl.europa.eu/RegData/etudes/etudes/join/2013/410220/EXPO-DROI_ET(2013)410220_EN.pdf

73. Ministry of Agriculture and Livestock (MAG). (2025, July 11). Uso de drones en agricultura y programas rurales y respuesta a solicitud de información pública nº 93399. Unified Public Information Portal. https://informacionpublica.paraguay.gov.py/#!/ciudadano/solicitud/93399

74. Ministry of Information and Communication Technologies (MITIC). (2025, July 4). Uso de drones en Paraguay, tecnología transversal y cooperación. Solicitud Nº 93400. Unified Public Information Portal. https://informacionpublica.paraguay.gov.py/#!/ciudadano/solicitud/93400

75. Ministry of the Interior. (2025, July 10). Memorándum DGTYC Nº 055/2025. Solicitud 93397. Unified Public Information Portal. https://informacionpublica.paraguay.gov.py/#!/ciudadano/solicitud/93402https://informacionpublica.paraguay.gov.py/#!/ciudadano/solicitud/93397

76. Mobilio, G. (2023). Your face is not new to me - Regulating the surveillance power of facial recognition technologies. *Internet Policy Review, 12*(1). https://doi.org/10.14763/2023.1.1699

77. Muñoz Lima, R. (2025, April 10). ¿Podría usar drones EE. UU. contra los cárteles mexicanos? *DW*. https://www.dw.com/es/podría-usar-drones-estados-unidos-contra-los-cárteles-mexicanos/a-72201012

78. National Directorate of Civil Aeronautics (DINAC). (2025, June 24). Uso de drones en Paraguay. Solicitud 93403. Unified Public Information Portal. https://informacionpublica.paraguay.gov.py/#!/ciudadano/solicitud/93403

79. National Directorate of Civil Aeronautics (DINAC). *Regulation R1103 on Remotely Piloted Aircraft (RPAC) and Remotely Piloted Aircraft Systems (RPAS), DINAC R 1103 (2017)*. https://www.dinac.gov.py/v3/index.php/documentos1/leyes-decretos-resoluciones-circulares/item/1814-resolucion-n-2170-2017-por-la-que-se-aprueba-el-reglamento-dinac-r-1103-reglamento-de-aeronaves-piloteadas-a-distancia-rpa-y-sistema-de-aeronaves-piloteadas-a-distancia-rpas

80. National Indigenous Institute. (2022). *Censo Indígena Nacional.* https://www.ine.gov.py/censo2022/documentos/Revista_Censo_Indigena.pdf

81. NTN24. (2024, June 24). Así es como una mujer indígena usa drones de alta tecnología para hacer más eficiente el agro en Bolivia. https://www.ntn24.com/noticias-ciencia-y-tecnologia/asi-es-como-una-mujer-indigena-usa-drones-de-alta-tecnologia-para-hacer-mas-eficiente-el-agro-en-bolivia-497985

82. OHCHR. Paraguay responsible for grave rights violations over deaths of two young girls, UN committee finds. (2025). OHCHR. https://www.ohchr.org/en/press-releases/2025/01/paraguay-responsible-grave-rights-violations-over-deaths-two-young-girls-un

83. Ombudsman's Office. (2025, July 9). Observaciones y recomendaciones sobre uso de drones y derechos humanos. Solicitud 93402.Unified Public Information Portal. https://informacionpublica.paraguay.gov.py/#!/ciudadano/solicitud/93402

84. Pardo, P. (2025, June 9). Ucrania convierte a los drones en la 'bomba atómica de los pobres'. *El Mundo*. https://www.elmundo.es/internacional/2025/06/08/6845a234e85ecee0108b45a1.html

85. Pérez Trench, N. (2022). Los sistemas de reconocimiento facial: una mirada a la luz del examen de proporcionalidad. *Revista Internacional de Derechos Humanos, 12*(1). https://doi.org/10.26422/RIDH.2022.1201.per

86. Ramírez, A. (2023, May 10). *Nosotres Ocupamos Internet. Episodio 2: Drones* [Podcast]. TEDIC. https://www.tedic.org/podcast/nosotres-ocupamos-internet-episodio-2-drones/

87. Resumen Latinoamericano. (2025, August 4). Sáhara Occidental. El supuesto dron saharaui que "cambiará el juego" y preocupa a Marruecos. *Resumen Latinoamericano*. https://www.resumen-latinoamericano.org/2025/08/04/sahara-occidental-el-supuesto-dron-saharaui-que-cambiara-el-juego-y-preocupa-a-marruecos/

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

89. Risso Feerrand, M. (2019). Derecho a la propia imagen y expectativa de respeto a la privacidad. *Estudios Constitucionales, 17*(1), 119–150. http://dx.doi.org/10.4067/S0718-52002019000100119.

90. Saaliq, S. (2024, February 13). La policía de India reprimió una protesta de agricultores con drones que lanzan gases lacrimógenos. *Infobae*. https://www.infobae.com/america/mundo/2024/02/13/la-policia-de-india-reprimio-una-protesta-de-agricultores-con-drones-que-lanzan-gases-lacrimogenos/

91. Saba Manzo, G. (2024, December 17). Drones, una herramienta de sigilo y furtividad para el control fronterizo en Paraguay. *Zona Militar*. https://www.zona-militar.com/2024/12/17/drones-una-herramienta-de-sigilo-y-furtividad-para-el-control-fronterizo-en-paraguay/

92. Secaf, H., Carrillo, E., & Paschoalini, N. (2023). *Technologies and human rights in the triple border area. An exploratory study of the security programmes Muralha Inteligente (Brazil) and the Automated Migratory System for Facial Recognition (Paraguay).* Associação Data Privacy Brasil de Pesquisa; TEDIC. https://www.tedic.org/en/human-rights-in-border-area/

93. Silva, M. R., & Varón, J. (2021). *Reconhecimento facial no setor público e identidades trans*. Coding Rights.

94. Chamayou, G. (2015). *A Theory of the Drone.* The New Press.

95. TEDIC. (2024, December). *Not with my face. Implementation of facial recognition cameras by the Paraguayan State* (Research by Graciela Galeano, Gerardo Paciello y Leonardo Gómez Berniga). https://www.tedic.org/wp-content/uploads/2025/04/Not-with-my-face-web.pdf

96. Trump, D. J. (2025, June 6). *Unleashing American drone dominance* [Executive order]. The White House. https://www.whitehouse.gov/presidential-actions/2025/06/unleashing-american-drone-dominance/

97. United Nations. (2019). *Report of the Special Rapporteur on the rights to freedom of peaceful assembly and of association* (A/HRC/41/41). https://documents.un.org/doc/undoc/gen/g19/141/02/pdf/g1914102.pdf

98. United Nations. (2020, June 25). Las nuevas tecnologías no pueden servir para rastrear y atacar a quienes protestan pacíficamente. https://news.un.org/es/story/2020/06/1476572

99. United Nations. (2021, May 30). Drones deliver blood to prevent maternal death in Botswana. https://news.un.org/en/story/2021/05/1092512

100. United Nations. (2024). *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression* (A/HRC/56/31). https://documents.un.org/doc/undoc/gen/n24/271/19/pdf/n2427119.pdf

101. United Nations. (2025, February 11). En Ucrania, los drones de corto alcance se convierten en el arma más peligrosa para los civiles. Naciones Unidas - Noticias. https://news.un.org/es/story/2025/02/1536406

102. Vaninetti, H. A. (2020). *Derecho a la intimidad en la era digital* (Tomo I, 1ra ed.). Hammurabi.

103. Wille, B., & Jacobsen, K. L. (2023, July 7). The data of the most vulnerable people is the least protected. *Ada Lovelace Institute.* https://www.adalovelaceinstitute.org/blog/data-most-vulnerable-people-least-protected/

104. World Bank. (2024). *Drones for Development: Overview of Opportunities in Latin America and the Caribbean.* World Bank. https://documents1.worldbank.org/curated/en/099092024163042596/pdf/P176634139ee990f819d48149ff8e1e8c75.pdf

105. Zuazo, N. (2018). *Algorithms and inequalities.* Derechos Digitales. https://www.derechosdigitales.org/wp-content/uploads/algoritmo_desigualdad_eng.pdf


Technology
& Human
Rights