RESEARCH ON ELECTRONIC ANKLE MONITORS IN PARAGUAY

Technology & Human Rights

TEDIC

RESEARCH ON ELECTRONIC ANKLE MONITORS IN PARAGUAY

Technology & Human Rights

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

RESEARCH ON ELECTRONIC ANKLE MONITORS IN PARAGUAY

APRIL 2026

COORDINATION AND EDITING
Maricarmen Sequera

RESEARCH
Antonia Bogado
Araceli Ramírez

ASSISTANCE
Maricel Achucarro

COMMUNICATION
Camila Rolón

LAYOUT AND DESIGN
Horacio Oteiza

TABLE OF CONTENTS

1. PRESENTATION OF THE PROBLEM

In Paraguay, the growing public debate on gender-based violence coexists with a government response that increasingly incorporates technological solutions as part of its prevention and protection tools. These include electronic ankle monitors for aggressors and various forms of technological support for victims, such as apps, panic buttons, emergency hotlines, and alert systems.

These measures are often presented as "neutral" and "modernizing" tools, associated with the idea of better control and greater security. However, from a human rights perspective—and especially from a feminist perspective—it is essential to address the question that is frequently left out of institutional design: what kind of security is being built, and at the expense of which rights?

The problem is not the existence of technological tools per se, but rather the way they are integrated into the justice and public safety systems. Technology can become a substitute for comprehensive public policy, a visible response to public pressure, or even a means of expanding State control without sufficient accountability. The most delicate tension arises when "prevention" relies on surveillance and tracking mechanisms, such as geolocation technologies, which involve the processing of highly sensitive data and can amplify risks of exposure, data breaches, abuse, operational errors, or revictimization.

This study is based on a central hypothesis: technologies aimed at preventing gender-based violence should not be evaluated solely on the basis of their promise of safety, but rather on their actual functioning, the material conditions of their implementation, their governance, the role of the institutions involved, and their differential effects on women and gender-diverse persons. In other words: the question is not merely "does it work or not", but "what does it produce, for whom, at what cost, and who controls it".

2. OBJECTIVE OF THE RESEARCH

2.1. General Objective

To critically analyze the use of electronic ankle monitors and other technologies applied to the prevention of gender-based violence in Paraguay, describing their regulatory framework, practical implementation, institutional governance, associated public procurement, and their implications for the tension between security, privacy, and human rights, with an emphasis on the rights of women and gender-diverse persons.

2.2. Specific Objectives

To review the current legal framework that authorizes and regulates the use of electronic ankle monitors (SIMDEC) and related technologies for the prevention of gender-based violence, identifying government obligations, regulatory gaps, and internal contradictions.

- To describe the actual institutional implementation process: how a technological measure (ankle monitor, app, panic button, or alert) is requested, ordered, installed, monitored, responded to, and recorded.
- To systematize public procurement and contracting processes related to electronic ankle monitors and monitoring services, identifying contracting models, costs, providers, installed capacity, and operating rules.
- To collect and analyze available public information (AIP Portal) and assess the level of government transparency, identifying patterns of response, opacity, or absence of data.
- To produce qualitative evidence through interviews with at least three key authorities to understand decision-making criteria, operational capabilities, failures, and inter-institutional tensions.
- To incorporate international comparative analysis to anticipate scenarios of surveillance expansion, risks, minimum conditions for effectiveness, and advocacy opportunities.
- To develop concrete recommendations for State advocacy, aimed at guaranteeing rights, setting limits, ensuring transparency, incorporating a gender perspective, and establishing effective institutional frameworks for response and care.

2.3. Research Questions

To ensure that the research is useful for public advocacy, we structured it around questions that go beyond a simple "yes/no" assessment of effectiveness:

- What is understood as "prevention" within the Paraguayan State when adopting a technology? Is it prevention, control, risk management, or response?
- What data is collected and processed using ankle monitors, apps, or alert systems? Who accesses that information and under what rules?
- What safeguards exist to prevent secondary uses, data leaks, or unauthorized access?
- How is it implemented in practice: what happens when an alert is triggered, which institution responds, within what timeframe, with what resources, and what happens if the system fails?
- How is the burden of care distributed? Do these technologies protect victims or shift responsibility onto them (having a mobile phone, charging the battery, staying connected, reporting, etc.)?
- What procurement/service model was adopted, and what technological dependencies does it create (providers, licenses, maintenance, 24/7 monitoring, infrastructure)?
- What differentiated impacts are there on women, LGBTIQ+ people, rural populations, and people without internet access or digital literacy?
- What can be learned from international experiences (Spain, Australia, the United States, Argentina) regarding limitations, failures, and conditions for effectiveness?

These questions aim to support an analysis that goes beyond technological innovation to address the political core of the issue: surveillance as a means of producing security.

3. METHODOLOGY

This research adopts a qualitative, exploratory approach with a critical-interpretive orientation and a human rights, privacy, and gender perspective. The focus was not on statistically measuring the effectiveness of electronic monitoring, but rather on understanding how a technological policy for prevention and response to gender-based violence is configured in practice, what institutional rationales sustain it, what material conditions it requires to operate, and what tensions it generates at the intersection of security, surveillance, and the protection of rights.

From this perspective, the study was organized as an expanded case study of the institutional and technological ecosystem deployed in Paraguay around the Monitoring System by Electronic Control Devices (SIMDEC, for its Spanish acronym) and other associated tools, such as apps, alert systems, and institutional activation channels. The choice of this design responded to the need to analyze not only an isolated device, but the regulatory, operational, and political framework that makes it possible: the rules that enable it, the institutions that implement it, the infrastructures it depends on, the decision-makers, and the concrete ways in which responsibilities, risks, and care burdens are distributed.

The analysis combined various strategies for generating and cross-checking information. First, a review of documents and regulations was conducted to reconstruct the system's legal and operational framework. This included laws, decrees, rulings, protocols, forms, technical documents, and institutional materials related both to the operation of SIMDEC and to other state-run technologies for responding to gender-based violence. This review made it possible to identify what the system formally prescribes, its legal foundations, what obligations it assigns to each actor, and what gaps or gray areas persist regarding implementation, coordination, and safeguards.

Second, requests for access to public information were used as a central tool to gain insight into the system's actual functioning. Through these requests, we sought data on institutional capacities, monitoring processes, technical feasibility criteria, territorial coverage, public procurement, contracts, operating rules, available metrics, data processing, and response mechanisms. This aspect was key to comparing the formal design with actual practice, as well as to identifying opacities, gaps in information, and institutional or provider dependencies that are not always explicitly reflected in the regulatory framework.

Third, semi-structured interviews were conducted with authorities and key informants involved in the design, implementation, or operation of the system. These interviews made it possible to reconstruct decision-making criteria, day-to-day challenges, inter-institutional tensions, and specific ways of interpreting the concept of "prevention" within the State. Rather than simply gathering isolated opinions, the objective was to access the institutional rationales that shape technological policy: how certain decisions are justified, which problems are considered priorities, what limits are acknowledged, and how the functions of control, response, and care are distributed in practice.

As a complement, the study incorporated a dimension of international comparative analysis. This comparison was not intended to mechanically equate different national experiences, but rather to situate the Paraguayan case within a broader discussion on electronic monitoring, surveillance, and gender-based violence. A review of the literature from other countries allowed for the identification of recurring patterns, previously documented risks, minimum operating conditions, and relevant policy debates to interpret the local case with greater analytical depth.

The methodological strategy was, therefore, one of triangulation. The analysis was constructed by cross-referencing what is prescribed by regulations, what is administratively documented, and what is institutionally narrated by the actors directly involved. This triangulation made it possible not to limit the research to the wording of the regulations or to the technological promise of the device, but rather to examine the concrete framework that underpins public policy. In other words, the study sought to simultaneously observe what the system claims to do, what public information allows for verification, and how its functioning is described by those who participate in it.

4. INTRODUCTION

In December 2024, Paraguay took a significant step forward in its public safety policy with the effective implementation of the Monitoring System by Electronic Control Devices (SIMDEC)[1]. The first electronic ankle monitors[2] began to be placed[3] on perpetrators accused of domestic violence, marking the beginning of what authorities presented as a modernization of the justice system and an "innovative" response to the crisis of gender-based violence affecting the country. However, TEDIC considers it essential to question this narrative of technological progress and to critically examine what kind of security is being built, for whom, and at what cost in terms of human rights.

The urgency of the problem is undeniable. According to data from the Ministry of Women, Paraguay recorded 36 femicides in 2023[4], while the judiciary reported more than 31,000 complaints of domestic violence during the same period. These figures, which barely capture the surface of a phenomenon deeply rooted in more profound structural problems, generate understandable social and political pressure for effective responses. It is within this context of crisis that electronic ankle monitors and other technological measures emerge as seemingly quick and visible solutions, fueling what Evgeny Morozov (2013) calls "technological solutionism": the belief that complex social problems can be solved through the application of technology, without addressing their structural causes.

This research aims to explore the deployment of electronic ankle monitors and other technological alternatives in Paraguay and internationally, not from a technophobic standpoint, but from a digital rights perspective that recognizes both the potential and the risks of these technologies when integrated into justice and security systems. We start from the premise that technology is never neutral: it is situated within power networks that reproduce the logic of the system implementing it and can both protect and violate rights, depending on its design, governance, and conditions of implementation.

---

1 Implementation protocol available on the website of the Paraguayan Judiciary. Retrieved from: https://www.pj.gov.py/images/contenido/otp/Dispositivos-electronicos/4%20PROTOCOLO%20DEL%20SIMDEC%2030_12_2024.pdf

2 Throughout this study, the terms SIMDEC (Monitoring System by Electronic Control Devices), electronic monitoring system, and electronic ankle monitors are used interchangeably, in line with their widespread use in public discourse and in most of the institutional documents reviewed. However, it should be noted that, strictly speaking, these terms are not equivalent. The electronic ankle monitor refers to the hardware device—the physical bracelet worn by the defendant—while SIMDEC is the comprehensive system in which that device operates: it includes the monitoring platform, the victim interaction applications, the control center, and the communications infrastructure. The SIMDEC/OMDEC Protocol (2024) itself distinguishes between these two levels by defining the "electronic monitoring device" as the "technology used by SIMDEC for monitoring and interacting with the user and the victim, where applicable" (Art. 5, subpar. b). The interchangeable use of the terms in this study is for the sake of readability and does not imply a disregard for this conceptual distinction.

3 Electronic ankle monitors will be used in cases of domestic violence in Asunción. The article is available on the website of the newspaper ABC Color, Paraguay.

4 Read more at: https://mujer.gov.py/el-ano-2023-cierra-con-45-feminicidios-en-paraguay/

5. BETWEEN TECHNOLOGICAL PROMISES AND STRUCTURAL REALITIES

The introduction of electronic ankle monitors in Paraguay cannot be viewed simply as the arrival of a technical device in the judicial system. What is at stake is the establishment of a State surveillance infrastructure that is presented, among other things, as a response to gender-based violence, but which simultaneously reorganizes the relationships between punishment, care, control, and risk management. For this reason, this exploratory study is not merely interested in asking whether "the ankle monitor and other technological devices work", but rather what kind of protection they promise, what institutional conditions they require to operate, and what effects they have on rights, responsibilities, and forms of State intervention. The Protocol of the Monitoring System by Electronic Control Devices (SIMDEC) itself confirms this perspective: it defines the system not as an isolated device, but as a "set of resources, processes, procedures, and actions" that includes technical feasibility, monitoring, warnings, alarms, coordination, and police response. (CSJ, 2024)

In Paraguay, moreover, the use of ankle monitors was publicly justified through a threefold political framework[5]. On the one hand, as a tool to prevent domestic violence and femicides; on the other, as part of an agenda for institutional modernization of the Judiciary, the Ministry of the Interior, and the Ministry of Justice; and, at the same time, as a mechanism to reduce prison overcrowding, lower costs, and strengthen monitoring of alternatives to incarceration. This triple discourse appears both in the regulations and in media coverage by outlets such as ABC Color[6] and Última Hora[7], where electronic monitoring is simultaneously presented as protection, efficiency, innovation, and cost-saving. Precisely for this reason, this study starts from a critical premise: when the same technology is presented simultaneously as a humanitarian solution, a security tool, and a criminal justice management measure, it is necessary to carefully examine which State rationale is guiding its use and which issues are being excluded from public debate. (ABC Color, 2024; Última Hora, 2024; CSJ, 2025).

The history of SIMDEC shows that this is neither a sudden nor a neutral measure. Law 5863 of 2017 established the legal framework for the system; Decree 466 of 2023[8] regulated its implementation; Law 7270 of 2024[9] amended and expanded that framework; and from late 2024 through 2025, protocols and agreements[10] were approved for its gradual deployment, first in Asunción and later with subsequent expansions. This sequence reveals more than just a technical evolution; it demonstrates the progressive consolidation of a public surveillance policy that has evolved from a regulatory promise into an effective operation, even as major processes remain to be defined. (Judiciary, 2017; Judiciary, 2023; Judiciary, 2024; CSJ, 2025).

5 The Supreme Court approves Resolution No. 1779 on electronic ankle monitors. News article available on the website of the Paraguayan Judiciary.

6 Electronic ankle monitors will be used in cases of domestic violence in Asunción. News available on the website of the newspaper ABC Color, Paraguay.

7 Government launches monitoring system for electronic ankle monitors. News available on the website of the Última Hora newspaper, Paraguay.

8 See decree at: https://www.pj.gov.py/images/contenido/otp/Dispositivos-electronicos/4%20PROTOCOLO%20DEL%20SIMDEC%2030_12_2024.pdf

9 See Law at: https://www.pj.gov.py/images/contenido/otp/Dispositivos-electronicos/6%20Ley%207270_11_06_2024.pdf

10 See rulings and protocols at: https://www.pj.gov.py/contenido/2695-observatorio-de-la-oficina-tecnica-penal-otp/3241

Added to this is an aspect that should not be left out of this introductory overview: the political economy of monitoring. The Paraguayan press reported that the implementation was marked by debates over costs[11], funding, providers, and public procurement. ABC Color reported that the tender for the provision and monitoring of ankle monitors reached a maximum amount of over G. 81 billion[12], and that the monthly cost per device would be around G. 2 million or more, to be paid by the beneficiary unless they declare insolvency. This is not a minor administrative detail. In surveillance technologies, the contractual infrastructure is also part of the infrastructure of power: it determines technical dependencies, potential opacities, audit margins, and actual operating conditions. In other words, technological protection is also defined in tender documents, in the contracts, and in the providers' black boxes. (ABC Color, 2024).

5.1. Gender-based violence as a structural phenomenon

To understand the implications of using ankle monitors and other technological devices in cases of gender-based violence, it is necessary to start with a conceptual framework that recognizes the structural and systemic nature of this violence. As established by the Belém do Pará Convention (1994), ratified by Paraguay, violence against women is "any act or conduct, based on gender, that causes death, physical, sexual, or psychological harm or suffering to women, whether in the public or private sphere" [13]. This definition, also adopted in Law 5777/2016 on Comprehensive Protection of Women against all forms of Violence[14], recognizes that gender-based violence is not a series of isolated incidents, but a manifestation of historically unequal power relations between men and women. (OAS, 1994; Ministry of Women, 2016).

TEDIC has been documenting how this structural violence manifests and is amplified in the digital space[15] (TEDIC, 2022 and 2024). Technology-facilitated gender-based violence (TFGBV) is not a phenomenon separate from "offline" violence, but rather part of a continuum that extends across all spaces where women live their lives. As noted in its research on digital violence against women politicians in Paraguay (TEDIC, 2024), TFGBV includes "any act committed, facilitated, aggravated, or amplified by the use of information and communication technologies or other digital media, that causes or may cause physical, sexual, psychological, social, political, or economic harm, and that is based on gender" (TEDIC, 2024). This definition is key to this study because it prevents technology from being understood solely as a neutral channel of protection: the same technical capabilities that enable alerting, tracking, or geolocation can also be used to surveil, control, and perpetrate violence. (TEDIC, 2024; UN, 2023).

This understanding of the online/offline continuum is key to analyzing electronic ankle monitors and other technological solutions, because these devices operate precisely at the intersection of the digital and the physical. They are physical objects that generate data and rely on telecommunications networks, computer systems, geolocation, databases, response protocols, and human decisions. Surveillance, in this context, does not exist solely on the Internet: it unfolds as a hybrid infrastructure that spans the home, the street, the workplace, the telephone, the courthouse, the monitoring center, and police intervention. Evaluating these technologies requires examining both the device and the ecosystem that supports it. (TEDIC, 2024; CSJ, 2024).

11 Retrieved from: https://www.abc.com.py/politica/2024/11/26/cinco-oferentes-pugnan-por-millonario-contrato-para-provision-de-tobilleras/

12 Retrieved from: https://www.abc.com.py/politica/2024/11/30/adjudican-a-empresa-mimada-la-millonaria-provision-de-tobilleras/

13 Organization of American States. (1994). Inter-American Convention on the Prevention, Punishment, and Eradication of Violence against Women "Convention of Belém do Pará". Retrieved from https://www.oas.org/juridico/spanish/tratados/a-61.html

14 Republic of Paraguay. (2016). Law No. 5777/2016 on Comprehensive Protection of Women against All Forms of Violence.

15 Technology-facilitated gender-based violence against female politicians in Paraguay. TEDIC (2024).

6. ELECTRONIC ANKLE MONITORS: GENEALOGY OF AN AMBIVALENT TECHNOLOGY

6.1. From behavioral experiment to mass criminal policy

The history of electronic monitoring reveals the tensions inherent in this technology. The first experiments date back to the 1960s in the United States, when brothers Ralph and Robert Schwitzgebel developed radio-telemetry devices at Harvard to monitor individuals on probation[16]. These early prototypes were shaped by the spirit of behaviorism of the time: the idea that criminal behavior could be modified through technological interventions based on monitoring and reinforcement.

However, the widespread adoption of electronic monitoring did not occur until the 1980s, in a very different context. As Mike Nellis (2013) documents in his comprehensive history of electronic monitoring, the expansion of these technologies coincided with a crisis in the U.S. prison system: prison overcrowding, rising costs, and political pressure for alternatives[17]. Electronic monitoring was thus presented not so much as a tool for rehabilitation, but as a pragmatic solution to criminal justice management problems.

This genealogy matters because it reveals the political ambivalence surrounding the ankle monitor. In the international literature, electronic monitoring is often associated with alternatives to incarceration. The United Nations Office on Drugs and Crime (UNODC) classifies it as one of the alternatives to imprisonment; at the same time, comparative evidence and the recommendations of the Council of Europe warn that its use can lead to "net-widening"—that is, the expansion of criminal control to individuals and spaces that were not previously subject to such supervision. The Council of Europe itself recommends special care during pre-trial stages to prevent such expansion and requires proportionality in duration and intrusiveness. In other words: a measure presented as less harmful[18] than prison can also function as an extension of the prison logic into the home, the community, and daily life. (UNODC, 2007; Council of Europe, 2014).

6.2. The arrival in Latin America: between modernization and precariousness

In Latin America, the adoption of electronic monitoring began in the 2000s, driven by a combination of factors: endemic prison crises, pressure from international organizations to "modernize" justice systems, and the availability of more affordable technology. Brazil was a pioneer in the region, followed by Argentina, Chile, and Colombia. However, as Paladines (2019) notes in his regional analysis, implementation in Latin America has been marked by improvisation, a lack of systematic evaluation, and the absence of public debate on its implications[19].

16 Schwitzgebel, R. K. (1969). "Issues in the use of an electronic rehabilitation system with chronic recidivists". Law & Society Review, 3(4), 597-611.

17 Nellis, M. (2013). "Surveillance, stigma and spatial constraint: The ethical challenges of electronic monitoring". En M. Nellis, K. Beyens, & D. Kaminski (Eds.), Electronically Monitored Punishment: International and Critical Perspectives (pp. 193-210).

18 UNODC. (2007). Handbook of basic principles and promising practices on Alternatives to Imprisonment. United Nations Office on Drugs and Crime.rnes.

19 Paladines, J. (2019). "El monitoreo electrónico en América Latina: Entre la modernización punitiva y la búsqueda de alternativas al encarcelamiento". Revista de Derecho Penal y Criminología, 20, 145-178

Paraguay joined this trend relatively late. Law 5863, which established SIMDEC, dates back to 2017[20], but its effective implementation did not begin until late 2024. This delay, far from being a disadvantage, offered an opportunity to learn from regional experiences and avoid their mistakes. However, the evidence available throughout this exploratory study suggests that the Paraguayan rollout is replicating problematic patterns observed in other countries: an emphasis on technology acquisition over institutional capacity building, a lack of transparency in procurement, and the absence of evaluation and accountability mechanisms.

6.3. The shift toward gender-based violence: protection or expansion of control?

The use of electronic ankle monitors specifically in cases of gender-based violence represents a significant shift in the history of this technology. It is no longer just a matter of monitoring house arrest or administering alternatives to prison, but of promising protection to victims through surveillance of the perpetrator, geolocation, and early activation of alerts. An international comparison[21] shows that this shift from offender-centered monitoring toward schemes that are also victim-oriented is not neutral: it redefines the political significance of the device and broadens its social legitimacy. Comparative experiences in Argentina, Spain, and England demonstrate precisely this transition toward "victim-oriented monitoring" models, in which protection comes to depend on tracking infrastructures, territorial exclusion, and institutional response. (Paterson, 2015; Ministry of Equality of Spain, n.d.).

In the Paraguayan context, this shift is part of a broader ecosystem of technological solutions for victims. Tools already existed, such as the Judiciary's Nendive app, launched in 2021 to report domestic violence in the capital, featuring geolocation and a panic button, and the "SOS Mujer" 137 emergency hotline, which operates with nationwide coverage and inter-institutional coordination. The introduction of ankle monitors does not, therefore, mark the beginning of the relationship between gender, security, and technology, but rather deepens a pre-existing State trend: responding to a structural problem through alert, monitoring, and response devices. The problem is not that technical tools exist, but that they end up replacing the debate on comprehensive policies for prevention, support, and redress. (Judiciary, 2021; Ministry of Women, n.d.).

20 Republic of Paraguay. (2017). Law No. 5863/2017 Establishing the implementation of electronic monitoring devices for persons under criminal prosecution or convicted persons. Gaceta Oficial.

21 Di Tella, R., & Schargrodsky, E. (2015). From offender to victim-oriented monitoring: a comparative analysis of the emergence of electronic monitoring systems in Argentina and England and Wales. urbe. Revista Brasileira de Gestão Urbana, 7(2), 155-166

6.4. Technologies for Victims: risk of revictimization and technological responsibilization

This issue becomes even more sensitive when protection depends materially on the victim or the domestic environment. Coverage of SIMDEC in Paraguay indicated that, in cases of domestic violence, the victim may receive a mobile phone or an app linked to the system[22], while the aggressor's device has a battery life of 48 to 72 hours, the charging of which is the user's responsibility. Added to this is the fact that technical feasibility[23] depends on specific conditions such as georeferenced address, signal coverage, and a regular supply of electricity. From a feminist and human rights perspective, these conditions are not mere operational details: they demonstrate how protection policies can lead to a form of technological responsibility, in which safety becomes dependent on connectivity, battery life, home infrastructure, and the ability to activate alerts. If something fails, the risk is that the burden will once again fall on those who were already exposed to violence. (Última Hora, 2024; CSJ, 2024; ABC Color, 2024).

The literature on technology-enabled violence in intimate relationships[24] helps to deepen this concern. Recent reviews[25] show that interpersonal violence today includes forms of tracking, harassment, surveillance, and control through digital devices, networks, and location systems. This calls into question any response that assumes that more technology automatically equals more protection. A victim-centered technology policy must avoid reproducing, through other means, the same logic of surveillance and control that characterizes many situations of violence. In other words: technological protection cannot become a tech-driven extension of the very problem it claims to address. (Rogers et al., 2022; TEDIC, 2024).

6.5. Technology, surveillance and effectiveness: why the device does not guarantee safety

Comparative evidence on electronic monitoring agrees on the following point: technology alone does not guarantee results. The systematic review by Belur and colleagues (Belur et al., 2020) [26] shows mixed effects on recidivism and emphasizes that outcomes depend on specific mechanisms, contexts, and institutional conditions. In this regard, in the United States, the National Institute of Justice (NIJ) evaluated GPS monitoring programs for domestic violence and found mixed results: a reduction in recidivism was observed only when the device was combined with active supervision and rapid response protocols (Padgett et al., 2006; NIJ, 2012). Carter and Grommon (2016) documented that police officers often lacked clarity regarding their roles in response to an alert and that there was confusion about whether the system operated as a preventive measure or as a control mechanism—an indicator that the technology was implemented without prior institutional redesign.

22 Government launches the monitoring system for electronic ankle monitors: How much will they cost and how will they work? News article accessed through the Última Hora website.

23 Electronic ankle monitors will now be used in domestic violence cases: How will they work? News article accessed through the Última Hora website.

24 Bailey, E., Boyle, M., Hardwick, D., Grzasko, N., Simkiss, L., Withers, S., & Taylor, A. (2023). Technology-facilitated abuse in intimate relationships: A scoping review. Trauma, Violence, & Abuse, 24(3), 1752-1771

25 Technology-facilitated gender-based violence (TEDIC; 2023). Consulted on March 20, 2026.

26 Belur, J., Thornton, A., Tompson, L., Manning, M., Sidebottom, A., & Bowers, K. (2020). A systematic review of the effectiveness of the electronic monitoring of offenders. Journal of Criminal Justice, 68, Article 101686

Similarly, the Council of Europe[27] warns not only of the risk of net-widening, but also of the need for monitoring—when it forms part of a supervision process—to be combined with other interventions and not to become a standalone measure disconnected from institutional support. This warning is particularly important in the case of Paraguay: in a context of gender-based violence, monitoring the perpetrator does not replace shelters, psychosocial care, legal aid, reparations, community networks, or an effective State response capacity. (Council of Europe, 2014).

In Paraguay, moreover, the system's effectiveness is hampered by material and territorial inequalities. The protocol itself requires technical feasibility studies[28] and forms that include precise geolocation, house numbers, victim information, and confirmation of a regular electricity supply. At the same time, the National Institute of Statistics (INE) reported[29] that in 2024 internet usage reached 81.6% of the population aged 10 and older, with a significant gap between urban (86.2%) and rural (73.7%) areas, as well as coverage limitations in certain territories and populations[30]. Although the ankle monitor does not always depend on the victim's smartphone, the ecosystem of alerts, contact, response, and monitoring does require physical infrastructure and connectivity. Therefore, technological surveillance does not operate on a homogeneous surface either: it produces segmentations and exclusions that must be analyzed from the beginning (CSJ, 2024; INE, 2025). This warning is not new: evaluations by the National Institute of Justice (NIJ; 2012) in the United States documented similar patterns: rural communities with poor connectivity, victims lacking information about how the system works, and populations in situations of structural vulnerability for whom the technological protection model functions poorly. This suggests that these gaps are not local contingencies but rather recurring structural constraints of electronic monitoring systems.

Within this conceptual framework, the question that opens this research can be formulated more precisely: when the Paraguayan State adopts electronic ankle monitors[31] and other technological solutions as a response to gender-based violence, what does it understand by prevention, and what regime of surveillance, care, and accountability is it constructing in practice? Our hypothesis is that technosolutionism (Morozov, 2013) [32] can function as an institutional shortcut[33]: it offers a rapid and visible response in a context of urgency, but runs the risk of omitting impact assessments, consultation with experts in technology and human rights, public evaluation, contractual transparency, and the strengthening of comprehensive policies[34]. For this reason, the analysis in this research will not stop on the promise of the mechanism, but rather on the normative, institutional, and material framework that sustains it: first, from a legal and human rights perspective; then, through interviews and the reconstruction of its actual functioning. (TEDIC, 2023; OHCHR, n.d.; Morozov, 2013).

27 Council of Europe. (2014). Recommendation CM/Rec (2014/4) of the Committee of Ministers to member States on electronic monitoring. Council of Europe.

28 SIMDEC Feasibility Form: Paraguayan Judiciary. (2024). Technical Feasibility Form - Monitoring System by Electronic Control Devices (SIMDEC). Criminal Technical Office. Available on the Paraguayan Judiciary's website.

29 News article available on the National Institute of Statistics (INE) website regarding internet use: National Institute of Statistics (INE). (March 2024). 8 out of 10 people use the internet in Paraguay.

30 ICT Report 2024: National Institute of Statistics (INE). (2024). 2023 Continuous Permanent Household Survey: Information and Communication Technologies (ICT).

31 Electronic ankle monitors: More security or a tool for surveillance? TEDIC article on electronic ankle monitors: (TEDIC; 2023).

32 Morozov, E. (2015). La locura del solucionismo tecnológico. Katz Editores.

33 A paradigmatic example is the widespread use of pre-trial GPS monitoring in the United States as a measure for early release, which expanded without first assessing the operational capacity to respond, turning the device into a substitute for pretrial decisions rather than a complement to protective measures (Gies et al., 2013).

34 International Covenant on Civil and Political Rights: United Nations. (1966). International Covenant on Civil and Political Rights. Office of the United Nations High Commissioner for Human Rights.

What is an electronic ankle monitor and how does it work in Paraguay?

Before delving into its legal, political, and social implications, it is important to pause and consider a basic question: what exactly is an electronic ankle monitor? In general terms, it is a body-worn monitoring device that is placed on a person's ankle—or, in certain designs, on the wrist—and is part of a broader remote surveillance system. It is not merely a physical bracelet. Its operation relies on a combination of hardware, software, geolocation, continuous data transmission, mobile connectivity, technical support, and a monitoring center responsible for interpreting events and triggering responses. The literature and regional management models[35] on electronic monitoring describe these technologies as socio-technical systems that combine a wearable device, a tracking platform, and institutional rules to define permitted zones, prohibited zones, and responses to non-compliance. (CNJ-UNDP, 2017; CNJ, 2020).

In the case of Paraguay, moreover, the terms of reference of the tender[36] confirm that the government did not procure an isolated "device," but rather a comprehensive on-demand service that includes devices, management and monitoring software, infrastructure for the Office for the Monitoring of Electronic Control Devices (OMDEC), facility upgrades, permanent support staff, technical support, and maintenance of the system as a whole. (PBC, 2024; CSJ, 2024).

In other words, an electronic ankle monitor does not provide protection on its own. It generates information about location, routes, proximity, and violations, and translate that information into events that must be processed by human institutions. For this reason, rather than speaking of an isolated device, it is more appropriate to speak of a monitoring infrastructure. This distinction is particularly relevant for Paraguay, where both the Protocol of the Monitoring System by Electronic Control Devices (SIMDEC) and the technical specifications[37] indicate that the system was conceived as an integrated system of monitoring, response, and infrastructure. The tender specifications establish that the minimum components of the electronic monitoring device are the Transmitter—the ankle monitor or wristband worn on the body—the Residential Base Unit (UBR)—a fixed device installed permanently at the home of the person wearing the ankle monitor when the transmitter's GPS signal is insufficient—and the Mobile Monitoring Unit (MMA), designed to receive alerts when the victim and aggressor are in close proximity and to transmit data to the monitoring software via a 3G or higher cellular network. (PBC, 2024; CSJ, 2024).

The Protocol itself defines the Monitoring System by Electronic Control Device (SIMDEC) as a "set of resources, processes, procedures, and actions" aimed at effectively monitoring the control regimes established by law. From the outset, therefore, Paraguayan legislation recognizes that it is not regulating merely a technical matter, but rather a broader institutional and operational network. (CSJ, 2024).

Electronic ankle monitor as part of an institutional framework

In Paraguay, the operation of electronic ankle monitors is not the sole responsibility of the Judiciary. The SIMDEC regulations[38] distribute functions among various institutions. The Office of Inter-institutional Oversight is composed of, among others, the Supreme Court of Justice, the Public Prosecutor's Office, the Ministry of the Interior, the Ministry of Justice, and the National Police. Within this framework, the Office for the Monitoring of Electronic Control Devices (OMDEC) serves as the Ministry of the Interior's

35 MJSP. (2017). A implementação da política de monitoração eletrônica de pessoas no Brasil. Departamento Penitenciário Nacional. Consulted on March 14, 2026.

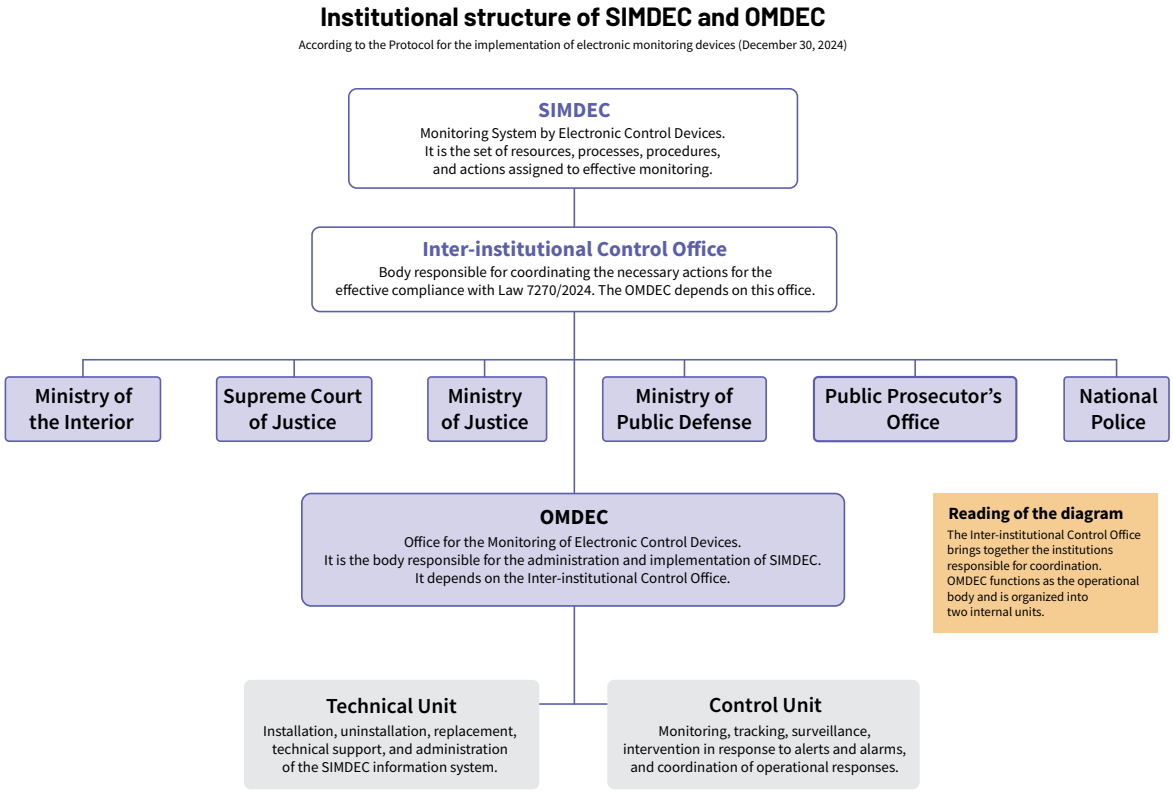
36 Terms and conditions for the procurement of electronic monitoring devices. Retrieved from the Paraguayan Government procurement portal.

37 Ibid.

38 Judiciary of Paraguay. (2024). Regulations of the Monitoring System by Electronic Control Devices (SIMDEC). Criminal Technical Office. Consulted on March 14, 2026.

agency responsible for the administration and implementation of SIMDEC. In turn, OMDEC reports to the Inter-institutional Oversight Office and comprises a Technical Division and a Control Division. The regulations also establish that the OMDEC's coordination leadership is represented by the head of the Department of Electronic Control Devices within the General Directorate of the 911 System of the Ministry of the Interior. (Ministry of the Interior et al., 2024).

- **Institutional structure of SIMDEC and OMDEC**



Source: own elaboration based on the Protocol for the Implementation of Electronic Control Devices, arts. 1, 2, 5, 6, 8, 11, and 12 (Judicial Branch / participating institutions, December 30, 2024).

This point is important because it shows that the use of ankle monitors in Paraguay should not be viewed solely as a judicial decision[39], but rather as an inter-institutional system of surveillance, data collection, communication, and response. The court requests or orders the measure, but its effective implementation involves OMDEC, the 911 System, the National Police, local police stations, and, in certain cases, the LINCE Motorized Tactical Operations Directorate. The "effectiveness" of the system, therefore, does not depend exclusively on the device functioning, but on the entire institutional network functioning in a coordinated and sustained manner. (Ministry of the Interior et al., 2024; CSJ, 2024).

39 Ibid.

- **System actors and their main roles**

Judiciary	OMDEC / SIMDEC	Provider Company	POLICE / 911 / LINCE	Victim and User
■ Court orders the measure ■ Preliminary review of legal grounds ■ Grants or denies the request ■ Notifies the termination of the measure	■* Receives request ■ Assesses feasibility ■ Installs and monitors ■ Manages alerts	■ Provides hardware ■ Maintains software ■ Stores data ■ Technical support	■ Receives activation ■ Dispatches field personnel ■ On-site intervention ■ Closes the case	■ Accepts/rejects MMA ■ Meets both legal and infrastructure requirements ■ Carries device ■ Charges battery/ data

Source: Authors' own elaboration based on SIMDEC/OMDEC Protocol (CSJ, 2024); Decree No. 466/2023

The start of the process: judicial decision and technical feasibility

According to the SIMDEC/OMDEC Protocol, the ankle monitor is not installed automatically. First, the court must request a technical feasibility report from the OMDEC. This request must include, among other elements, the identification of the person to be monitored, the specific details of the case, and the necessary data to define the inclusion zone—that is, the geographic space in which the person must remain—and/or the exclusion zone—the space they are prohibited from entering. The protocol adds a particularly relevant detail for restraining order cases: when the legal measure is a restraining order, the exclusion zone "shall be that indicated by the victim". (CSJ, 2024).

The official feasibility form provides a more detailed look at the information the system requires to function. It asks for the address, house number, city, neighborhood, geolocation (latitude, longitude, and altitude), a photo of the home's facade, the homeowner's mobile phone number, the victim's mobile phone number, the radius of the exclusion zone in meters, and confirmation of a regular electricity supply. It even includes the category of "fee" and distinguishes between free service, paid service, or insolvency. This shows that the system is not built on a blank slate: it requires a series of prior technical, housing, and administrative conditions. (OMDEC, 2024). The protocol also provides for a significant decision point: if no devices are available at the time of the request, the OMDEC must inform the requesting judge of this situation, without needing to conduct a feasibility study. In other words, the physical availability of equipment determines access to the measure from the outset. (CSJ, 2024).

Installation: device activation and zone configuration

If the installation is technically feasible and the court orders it, the court order is forwarded within the OMDEC to the Control Unit and the Technical Unit, which are responsible for coordinating the effective installation of the device. Technical staff install and activate the ankle monitor, while the Control Unit determines and configures the corresponding inclusion and exclusion zones in the computer system. Then, once at the location specified by the court, both units coordinate the geolocation and on-screen display of the monitoring system to verify the device's location "in real time". Once these adjustments are made, continuous tracking and monitoring are the responsibility of the Control Unit. (CSJ, 2024).

This point helps explain why the ankle monitor cannot be reduced to a digital shackle. Its operation depends on the translation of a judicial decision into concrete technical parameters: meters of distance, zones loaded into the system, coordinates, maps, real-time visualization, and operational monitoring criteria. The judicial measure becomes technically operational only when it enters this configuration and control system. (CSJ, 2024; CNJ, 2020).

Continuous monitoring: notifications, warnings and alarms

Once the device is activated, the OMDEC Control Unit assumes the task of continuous monitoring[40], tracking, and surveillance through the system's software. The Protocol[41] classifies potential events into three main categories. The first are notifications, related to technical issues affecting the device's operation or loss of signal coverage by the tracking system. The second category consists of deterrent warnings, which are triggered when the monitored individual approaches an exclusion zone or leaves an inclusion zone. The third category consists of immediate-response alarms, which require the implementation of urgent preventive measures and notification of the incident to the competent authority. (CSJ, 2024).

The distinction between these categories is not merely technical. It organizes different levels of State intervention. A notification implies, in principle, an incident that may require contact with the user and restoration of service; a deterrent warning implies that a problematic movement in relation to the judicial order has already occurred; and an immediate-response alarm indicates a situation that must trigger more severe operational mechanisms. This passage clearly illustrates how a change in location is transformed into a chain of institutional decisions. (CSJ, 2024).

- **Response flow to system events and alerts**

NOTIFICATION	DETERRENT WARNING	IMMEDIATE-RESPONSE ALARM
Technical incident that may affect device functionality or location tracking ■ Critical device battery level ■ Loss of GPS signal or network coverage ■ Failure of communication with the monitoring center ■ → Operator contacts the user to restore service ■ → If not resolved, the issue is escalated to technical supervision	*The monitored person approaches a prohibited zone or leaves a permitted zone* ■ The system detects proximity to an exclusion zone ■ The operator issues a mandatory warning to the monitored person ■ Up to three successive deterrent warnings are issued ■ Simultaneously (in cases of GBV): the operator calls the victim to alert her and confirm her location ■ If not complied with → escalation to an Immediate-response alarm	*Perimeter breach or tampering with the device* ■ Confirmed violation of the exclusion zone ■ Exit from the inclusion zone without compliance ■ Tampering with or damage to the device ■ The operator verifies real-time geolocation ■ Police response is activated via the operational radio channel ■ The victim (MMA) is contacted and provided with self-protection guidance

Source: Authors' own elaboration - Art 8, Decree N.° 466/2023

40 Judiciary of Paraguay. (2024). Regulations of the Monitoring System by Electronic Control Devices (SIMDEC). Criminal Technical Office. Consulted on March 14, 2026.

41 Ibid

What happens if the aggressor approaches or violates the restriction?

When a deterrent warning is triggered, the Control Unit operator must verify the situation and issue a mandatory warning to the user, informing them that they are approaching an exclusion zone or are outside the inclusion zone and that they must cease the action and return to the corresponding perimeter. The protocol[42] expressly requires three consecutive warnings. If the user does not comply, the operator immediately reports the incident to the Electronic Monitoring Devices Division of the National Police Security and Emergency Center (CSJ, 2024).

In cases of domestic violence or comprehensive protection for women against all forms of violence, the protocol includes an additional step: the operator must call the victim to ensure her safety, determine her location, and provide self-protection guidance. This point is key because it shows that, even when the system is presented as surveillance of the aggressor, it also incorporates a direct component of victim management: contact, location, guidance, and eventual coordination for protection. It is not, therefore, a technology that merely "monitors the aggressor", but rather an infrastructure that also incorporates the victim into its operational chain. (CSJ, 2024). If the three deterrent warnings are exhausted or if an immediate-response alarm is directly triggered, the operator must verify the georeferenced location in real time and promptly report the exit from the inclusion zone or the violation of the exclusion zone. From there, the police response is activated. (CSJ, 2024).

On-scene response: Police, 911 and tactical support

The protocol[43] is not limited to triggering on-screen alerts. It also regulates an on-scene response. Once the alarm is triggered, the operator must contact, via the operational radio communication channel, personnel from the nearest police station or personnel from the Motorized Tactical Operations Directorate (LINCE). Simultaneously, they must summon another patrol unit from the local police station to provide protection to the victim. Additionally, they may request the intervention of other agencies within the 911 System depending on the severity of the incident. (CSJ, 2024; Ministry of the Interior et al., 2024).

- **Police response to alarms**

POLICE RESPONSE – triggered by the immediate-response alarm		
Deployment:	**Protection of the victim:**	**Recording:**
■ Nearest police station to the aggressor's location	■ Additional patrol unit from the jurisdictional police station	■ All interventions are logged in the system software
■ LINCE Unit (M otorized Tactical Operations Directorate)	■ Simultaneous contact with the victim (MMA/Empower)	■ The operator documents the closure of the incident
■ Other 911 System resources, depending on the scale of the incident	■ Real-time self-protection guidance	■ Traceability of communications and dispatched units

Source: Compiled by the authors based on a public information report provided by the Ministry of the Interior.

42 Ibid.

43 Ibid.

This clearly illustrates the mitigation logic that underpins SIMDEC: spatial delimitation, continuous monitoring, warning alerts, simultaneous contact with the victim, and dispatch of police. The system is designed to act before the proximity escalates into a completed assault, but it does so through a chain of detection and response, not through automatic physical neutralization of the risk. Therefore, its actual operation depends on concrete factors such as the availability of mobile phones, communication coverage, dispatch response times, and on-site coordination capacity. (CSJ, 2024).

The "victim device" within the SIMDEC protocol

One aspect that has received little public discussion is that the SIMDEC protocol itself includes, in an annex, a specific device for the victim. It describes a unit consisting of a mobile phone and an app called Empower[44], designed to ensure the victim's safety. According to the annex, this app allows the user to send messages to the Control Unit, displays signal strength and battery level, and features a "Main Control Center Panic button" that triggers an SOS alarm. It also includes a button to call the Control Unit in case of questions or problems with the device. The same annex emphasizes that the user must carry the phone at all times and charge its battery at least once a day. It should be noted that the app is only available for devices running the Android operating system. (CSJ, 2024).

This point is important for two reasons. The first is descriptive: it shows that, within the SIMDEC design itself, the victim is not completely excluded from the technological circuit, but can also become the bearer of a device connected to the system. The second is analytical: it demonstrates that the protection promised by the system depends in part on everyday practical actions—carrying the phone, keeping the battery charged, maintaining a signal coverage—which fall upon the person the system is meant to protect. Later, in the critical analysis, this will compel us to consider the risks of revictimization and technological responsibility onto the victims. (CSJ, 2024).

Nendive: a different tool, but part of the same ecosystem

It is important not to confuse SIMDEC with Nendive[45]. Although both are part of Paraguay's institutional ecosystem for technological responses to domestic violence, they serve different functions. Nendive was introduced by the Judiciary as a mobile app to facilitate reports or requests for assistance in cases of domestic violence, initially for the Central Department, through the Office of Permanent Assistance and the Justices of the Peace. According to the official description, the app is available only for Android; it allows users to register with georeferenced home location data and includes a panic button that automatically generates an urgent case and sends an alert to the Office of Permanent Assistance. Upon receiving this alert, judicial officials contact the victim, and depending on the nature of the report, an assistance protocol may be activated involving law enforcement and notification to the on-duty court. (Judiciary, 2021).

The official statement also mentions that Nendive includes buttons to call emergency hotlines 137 (Ministry of Women) and 911 (National Police), it allows officials to upload information for case tracking, and provides the option to incorporate evidence—such as audio recordings, videos, and images—sent by the victim through other platforms like WhatsApp or Telegram. In this sense, Nendive does not function as a tool for spatially restricting the aggressor, but rather as a channel for reporting, georeferencing, alerting, and institutional follow-up. (Judiciary, 2021).

44 App available only for devices running the Android operating system.

45 Judiciary of Paraguay. (2021). Application to assist victims of domestic violence. Consulted on March 14, 2026.

Taken together, both of these tools demonstrate two distinct approaches to mitigation. The ankle monitor, according to the SIMDEC protocol, seeks to operate through spatial restriction, monitoring, and police response to perimeter violations. Nendive, on the other hand, functions as a remote reporting channel and mechanism for institutional intervention based on the victim's action. Both technologies operate at the intersection of surveillance, data, and security, but they do so from different points within that circuit. (CSJ, 2024; Judiciary, 2021).

6.6. A system that generates data, responsibilities and gray areas

Reconstructing this operational process also reveals which aspects are clear in public documents and which are not. Based on the protocol[46] and official documentation, it can be stated that SIMDEC involves real-time geolocation, the configuration of inclusion and exclusion zones, event classification, communication with the victim in certain cases, and coordination with the Police and the 911 system. It can also be affirmed that Nendive involves user registration, georeferencing of home addresses, generation of urgent cases, and the potential incorporation of evidence. However, these documents do not publicly detail—at least in the information gathered for this investigation—fundamental aspects such as data retention periods, independent audit standards, storage architecture, access controls, usage logs, or public performance metrics. This lack of detail is not a minor issue: it precisely highlights the area where legal and transparency analysis must proceed. (CSJ, 2024; Judiciary, 2021).

46 Judiciary of Paraguay. (2024). Regulations of the Monitoring System by Electronic Control Devices (SIMDEC). Criminal Technical Office. https://www.pj.gov.py/images/contenido/otp/Dispositivos-electronicos/5%20Reglamento%20SIMDEC%2030_12_2024.pdf

- **Technological ecosystem for responding to gender-based violence in Paraguay**

SIMDEC / Ankle monitor	EMPOWER (App)	NENDIVE (App / Judiciary)	Emergency Hotline SOS MUJER 137
Function: ■ Monitoring of the aggressor + alert to the victim when the aggressor is nearby ■ Requires a prior court order	**Function:** ■ Device provided to the victim (MMA mobile phone) ■ Panic button → direct communication with OMDEC ■ Real-time alerts when the aggressor is nearby ■ Expand the complaint without going to a police station	**Function:** ■ Remote reporting of domestic violence ■ Panic button → emergency situations ■ Activation of the Office of Permanent Assistance	**Function:** ■ 24-hour phone support ■ Guidance and referrals to services ■ No smartphone or mobile data required
Coverage: ■ Nationwide (starting in August 2025) ■ Requires electricity and network coverage	**Coverage:** ■ Nationwide (linked to SIMDEC) ■ Android only · requires active mobile data ■ Voluntary use—cannot be imposed on the victim	**Coverage:** ■ Central Department ■ Android only · requires active mobile data	**Coverage:** ■ Nationwide ■ No digital connectivity required
Responsible institution: ■ Ministry of the Interior—OMDEC ■ Provider: Track Consortium (Contract 13/2024)	**Responsible institution:** ■ Ministry of the Interior—OMDEC ■ Same Provider as for the ankle monitor (Track Consortium)	**Responsible institution:** ■ Judicial Branch ■ Office of Permanent Assistance	**Responsible institution:** ■ Ministry of Women
Key limitations: ■ Burden on the victim (battery life, mobile data usage, portability) ■ No specific data protection framework ■ Private provider access to sensitive data	**Key limitations:** ■ The victim must carry the device at all times ■ The victim must charge the battery at least once a day ■ Must have mobile data enabled at all times ■ If the victim refuses to use the device, the system monitors only the aggressor ■ The government provides the mobile phone, but the day-to-day operational burden falls on the victim	**Key limitations:** ■ Available only for Android ■ Georeferencing of the victim's address is stored ■ No documented public data protection policy	**Key limitations:** ■ No documented formal integration with SIMDEC ■ Depends on institutional response capacity ■ No public data on effectiveness available

Source: Compiled by the authors based on documents provided through the Portal of Access to Public Information by the Ministry of the Interior and the National Police.

7. TOWARD A LEGAL ANALYSIS

Understanding how electronic ankle monitors or other technological devices function in practice is essential to evaluating their regulatory framework. It is not enough to know that a law or protocol exists: it is necessary to observe what data circulates through the system, which institutions are involved, who makes decisions at each stage, what substantive obligations fall on the individuals involved, and what gray areas emerge between the promise of protection and the system's actual operation. Therefore, once this technical and institutional framework has been reconstructed, the next step is to assess whether the Paraguayan legal system adequately regulates core issues such as legality, necessity, proportionality, due process, data protection, transparency, access to information, and accountability. This is where the legal analysis becomes essential: not to repeat how the system should function, but to ask whether the current rules are capable of controlling the risks that this very functioning produces.

7.1. Paraguayan regulatory framework: what the State authorizes and what the law requires

To conduct documentary research in Paraguay, we must also reconstruct the legal framework underpinning the implementation of the Monitoring System by Electronic Control Devices (SIMDEC). This legal analysis will be approached from a critical perspective. The aim is not only to establish what the law permits, but also what it requires, what tensions it generates, and, especially, what remains unresolved.

To this end, the analysis is structured in hierarchical layers, as required by Article 137 of the Constitution of the Republic of Paraguay (hereinafter, the Constitution), which establishes constitutional supremacy and the incorporation of international human rights treaties as part of the applicable legal framework. This hierarchy also defines the State's binding obligations and the standard by which any public policy must be evaluated, including, in this case, the implementation of SIMDEC.

The chapter is organized into four sections: the international human rights framework ratified by Paraguay; the constitutional framework and the specific legal structure of SIMDEC; the substantive framework on gender-based violence within which the system operates; and the applicable personal data regime. The guiding question for this section is not whether SIMDEC has a legal basis—it does—but whether that legal basis is sufficient to ensure that the system operates with a rights-based approach: effectively protecting victims, respecting the rights of the accused, safeguarding the data of both parties, and enabling public accountability.

International human rights framework: binding obligations of the Paraguayan state

Based on the international human rights framework, we must recall that Paraguay has ratified the main international human rights instruments, which impose specific legal obligations on the country. In this regard, the Universal Declaration of Human Rights (United Nations, 1948) serves as the foundation from which the other instruments derive. For the purposes of this study, particular relevance lies in the right to life, liberty, and security of the person (Article 3), the principle of equality before the law (Article 7), and the right to privacy (Article 12), which protects individuals against arbitrary interference in their private lives.

The International Covenant on Civil and Political Rights (ICCPR) (United Nations, 1966.a), ratified by Law No. 5/1992, and the International Covenant on Economic, Social and Cultural Rights (ICESCR) (United Nations, 1966.b), ratified by Law No. 4/1992, complete the universal normative framework. The ICCPR is most directly relevant to this study, as it protects the right to life (Article 6), liberty and security of the person (Article 9), privacy against unlawful interference (Article 17), and equality before the law (Article 26). The ICESCR complements this framework from the perspective of the rights that make possible a life free from violence: access to health care, education, and minimum material conditions of well-being.

For its part, the American Convention on Human Rights (ACHR), known as the Pact of San José, Costa Rica (1969), was the first international human rights treaty ratified by Paraguay following the advent of democracy. This treaty protects rights that the SIMDEC is intended to guarantee, but also rights that the system itself must respect, and this dual function creates the first fundamental legal tension within the system.

From the victim's perspective, the ACHR guarantees the right to life (Article 4), personal integrity (Article 5), judicial protection (Article 25), equality before the law (Article 24), and the right to privacy and protection of Honor and Dignity (Article 11). These rights provide the legal basis for the State's obligation to adopt active measures to protect women in situations of violence. From the perspective of the accused, the same Convention guarantees the presumption of innocence (Article 8.2), due process guarantees (Article 8), and also the right to privacy. Precisely because SIMDEC affects rights protected under the ACHR—both those of the accused and those of the victim—its implementation must meet the test of legality, necessity, and proportionality that the Convention itself and the jurisprudence of the Inter-American Court require for any restriction of rights.

Similarly, the Additional Protocol to the American Convention on Human Rights in the Area of Economic, Social, and Cultural Rights (San Salvador Protocol, 1999), ratified by Paraguay through Law No. 1,040/1997, complements this framework by recognizing rights that shape the material conditions necessary for the protection of victims.

It should be noted that the Inter-American Commission on Human Rights (IACHR), in its report on the use of pretrial detention, has recommended the adoption of alternatives to detention, a position that was subsequently taken up by the Organization of American States (OAS) in its 2017 report. In particular, the report highlights the recommendation to implement less restrictive mechanisms, expressly including "the monitoring of the accused through an electronic device for tracking or determining their physical location" (OAS, 2017, para. 122). This recommendation formally endorses the legal framework of SIMDEC as a measure compatible with inter-American standards. However, it is important to note that both reports address the issue in general terms, focusing on reducing prison overcrowding and safeguarding the rights of persons deprived of liberty, without specifically addressing the use of these technologies in contexts of gender-based violence[47]. This absence of specific guidance for the gender context constitutes a significant interpretive gap that the national regulatory framework must address.

47 In Paraguay, however, the system has been publicly presented in a different light than that of an alternative precautionary measure to incarceration. Statements made by the Minister of the Interior to the press positioned it as a tool for directly addressing gender-based violence—particularly physical violence—and for preventing its most serious consequences (Ministry of Justice, n.d.; ABC Color, 2023). This discursive framing is significant: it shifts the rights-based logic of electronic monitoring toward a logic of risk control, in which technology is presented as a visible response to an urgent social demand. This reconfiguration of the system's political meaning has consequences for the expectations it generates, the criteria used to evaluate its effectiveness, and the institutional pressure to expand it, regardless of the available evidence concerning its actual performance.

To complement the international framework, there is the legal instrument most directly relevant to this study: the Inter-American Convention on the Prevention, Punishment, and Eradication of Violence against Women, known as the Belém do Pará Convention (1994), ratified by Paraguay through Law No. 605/1995. It is frequently cited as a model binding treaty in this area, reflecting its paradigmatic nature within the inter-American system. This convention establishes the right of every woman to a life free from violence, both in the public and private spheres (Article 3), and provides that States must guarantee the full exercise of women's civil, political, economic, and social rights, including the right to a simple and rapid remedy before the courts for protection against acts that violate those rights (Article 4, subparagraph g). In this regard, SIMDEC can be understood as a realization of this right to effective protection.

Second, Article 7 establishes the State's obligation to adopt, "by all appropriate means and without delay, policies aimed at preventing, punishing, and eradicating such violence". This mandate to adopt all appropriate means constitutes the strongest international legal basis for the implementation of SIMDEC in cases of gender-based violence. The Convention also obligates the State to act with due diligence to prevent, investigate, and punish violence (Article 7, subparagraph b). The standard of due diligence requires not only that measures exist in law, but that they be effective in practice. An electronic monitoring system that functions poorly—whether due to a lack of infrastructure, inadequate response times, or operational errors—does not meet this standard, even if it has formal legal backing.

Third, the Convention establishes specific mechanisms for international accountability; that is, individuals and groups have the right to file petitions before the IACHR when States have failed to adopt the necessary measures to prevent, punish, and eradicate violence against women. This means that failure to comply with the obligations arising under the Convention constitutes a source of the State's international responsibility.

Another key international instrument for this analysis is the Convention on the Elimination of All Forms of Discrimination against Women (CEDAW), ratified by Paraguay through Law No. 1,215/1986, which imposes on States the obligation to adapt their legislation and public policies to ensure equality and non-discrimination for women in all spheres of life. Its Optional Protocol, ratified by Law No. 1,683/2001, recognizes the CEDAW Committee's competence to receive individual communications from victims of violations once internal remedies have been exhausted, thereby expanding the mechanisms available for enforcement.

For this analysis, two General Recommendations of the CEDAW Committee are particularly relevant. General Recommendation No. 19 (Committee on the Elimination of Discrimination against Women [CEDAW], 1992) establishes that States may be held responsible for private acts if they fail to take measures with due diligence to prevent rights violations, investigate and punish acts of violence, and compensate victims. This positions the State as an active actor in prevention and underpins the legitimacy of electronic monitoring measures aimed at that purpose. General Recommendation No. 35, which updates and expands upon No. 19 (CEDAW, 2017), moves in the same direction and urges States to adopt effective technological measures for protection and monitoring. These recommendations are binding and must be implemented by all the branches of government, an aspect that is often underestimated in Paraguay's institutional framework and which in itself constitutes a compliance issue.

CEDAW is also important when considering women's participation in the design of policies that affect them, an aspect that is often overlooked when evaluating public policies concerning this group[48]. A system like SIMDEC, designed without consulting women's organizations and without a gender-specific assessment of its impacts, falls short of these international standards.

In short, the international framework ratified by Paraguay unambiguously supports the implementation of SIMDEC as a legitimate public policy tool aimed at protecting women. Yet that same framework does not permit just any form of implementation. It demands real effectiveness, not merely regulatory existence. That is why the tension between formal legitimacy and practical impact is the central theme of the remainder of this analysis.

7.2. Constitutional basis of SIMDEC

The Constitution contains the legal provisions necessary to both underpin and limit the implementation of policies such as SIMDEC. Accordingly, it is necessary to assess whether the resulting tensions are sufficiently addressed in the regulatory framework.

From the perspective of the rights that justify the system, the Constitution protects the life and physical integrity of individuals (Article 4), individual liberty and security (Article 9), and, more specifically, protection against violence within the family. Article 60 explicitly provides that "the State shall promote and guarantee the protection of the family" and prohibits violence in family relationships, thereby imposing a positive obligation on the State to act. This provision, together with the principles of formal equality enshrined in Articles 46 through 48, constitutes the constitutional basis for the mandate to protect women who are victims of violence.

At the same time, the very same constitutional text that provides the basis for SIMDEC also gives rise to tensions that must be resolved for its effective implementation. The right to privacy—protected under Articles 33 and 36 of the Constitution—is directly affected by the real-time geolocation system that characterizes electronic monitoring. This impact is not necessarily illegitimate: the constitutional text itself permits restrictions on rights when they are necessary, proportionate, and grounded in law. However, this conditional authorization requires that the SIMDEC's regulatory framework clearly justify what data is collected, for what purposes, for how long, and under what controls[49].

48 Women's participation in the design of measures such as SIMDEC is not a minor procedural requirement. A system designed without considering the material and digital conditions of its intended users may, under the guise of protection, reproduce the very inequalities it aims to correct. Activating the panic button, for example, assumes that the victim has a working smartphone, an active data plan, network coverage, and sufficient digital literacy to use the app under pressure—conditions that cannot be taken for granted for women in situations of economic vulnerability, those living in rural areas, or those with limited access to connectivity. An intersectional approach to the system's design is the only way to identify these gaps before they become real risks.

49 Geolocation constitutes personal data whose collection and real-time processing, within the framework of SIMDEC, involves not only the accused but also the victim. While the explicit logic of control applies to the accused, the victim is equally exposed to constant surveillance: her location, movements, and contact information are accessible in real time to all institutional actors operating SIMDEC. This asymmetry is not addressed in any current regulatory instrument. The legal framework justifies the surveillance of the accused but does not examine or limit the degree of the victim's exposure as a condition for the system's operation. The victim does not choose to be monitored; she is monitored as a necessary consequence of being protected.

The procedural guarantees provided in Articles 16 and 17 of the Constitution—the presumption of innocence and the right to due process—also form part of this analysis, particularly in light of the amendments introduced by Law No. 7270/2024 (which will be addressed later) that eliminated the prohibition on applying the system to individuals charged with crimes and removed the requirement of non-recidivism. These changes are not necessarily unconstitutional, but they do require a solid legal justification regarding the proportionality criteria governing the judicial decision to impose an electronic ankle monitor as a precautionary measure.

From a formal standpoint, the Constitution authorizes SIMDEC as a mechanism compatible with its values and mandates. However, that compatibility depends on whether the regulatory and institutional design actively resolves the tensions generated by the constitutional text itself. A public policy that invokes the protection of women without resolving those tensions may create a system that provides formal safeguards but fails to offer comprehensive protection in practice.

7.3. Legal architecture of SIMDEC: from regulatory design to operational protocols

SIMDEC is governed by a comprehensive set of regulations ranging from formal law to day-to-day operational protocols. Understanding this legal framework is essential to evaluating its actual functioning and its implications for the rights of the individuals involved.

This framework begins with Law No. 5863/2017, which created SIMDEC with the aim of implementing its use in the context of judicial proceedings. In its original form, the system was conceived primarily as an alternative measure to deprivation of liberty; in other words, a tool to reduce the use of pretrial detention and humanize the criminal justice response. The specific focus on gender-based violence was not the center of that initial design. The first amendment, introduced by Law No. 6345/2019, was later repealed by Law No. 7270/2024, which constitutes the most significant normative change to the system to date. This latter law expanded Articles 2, 3, 4, 5, 6, 7, 8, 10, and 11 of the original statute, introducing amendments that warrant careful analysis.

In Article 2, which defines the scope of application, Law No. 7270/2024 expressly incorporates Law No. 5777/2016 on Comprehensive Protection of Women against All Forms of Violence. This change has fundamental legal and political significance, as it formalizes the connection between SIMDEC and the regulatory framework on gender-based violence, which until then had been merely a matter of interpretation. As of 2024, the electronic monitoring system is explicitly designed to operate in cases of violence against women.

Meanwhile, Article 3, which regulates the conditions of applicability, was amended in two ways. The previous law prohibited the application of SIMDEC to individuals charged with crimes; the new provision removes that prohibition. It also removes the requirement of non-recidivism for access to the measure. Both changes broaden the range of individuals to whom the system can be applied as an alternative to imprisonment.

Finally, Law No. 7270/2024 provided for its regulation within sixty days of its enactment. However, that law does not have its own exclusive regulatory decree; instead, its implementation is governed by the regulatory framework consisting of Law No. 5863/2017, its amending Law No. 7270/2024, and Decree No. 466/2023, which had been issued prior to the legislative amendment. This situation warrants attention as the regulatory provisions that operationalize the system were designed for the previous law and do not necessarily incorporate the standards required by the 2024 expansion, particularly regarding cases of gender-based violence.

In fact, Decree No. 466/2023 is the provision that implements the legal mandate. It is also, in many respects, the most revealing provision for legal analysis, because it is here that the system sets out its concrete institutional architecture, defines its actors, establishes its technical characteristics, and regulates the processing of the information generated.

With regard to the stakeholder map, the Decree distinguishes between several institutional components, ranging from the service provider company, responsible for providing monitoring support services (Article 1, subsection e); the SIMDEC operators (Article 8, subsection f), responsible for the continuous monitoring of the devices; to the Inter-institutional Control Office, which coordinates the actions of the various agencies involved. The latter body, pursuant to Article 4 of the Decree, may request the contracting of services in accordance with the provisions of Law No. 7021/2023 on Public Procurement and Contracting[50]. For our analysis, it is important to take into account this legally significant reference, which links the operation of SIMDEC to the public procurement regime and, therefore, to the obligations of transparency and accountability that this regime imposes.

Concerning the technical features that have implications for rights, the Decree stipulates that SIMDEC must "reflect users' georeferenced location in real time, indicating the date and time" (Article 3, subsection b), and "issue alerts in cases of proximity between the user and the victim" (Article 3, subsection e), including the obligation to inform the victim of the user's proximity to an exclusion zone (Article 11, subsection a). These functionalities are not technically neutral, as they involve the real-time collection and processing of geolocation data for both the accused and the victim, which constitutes the processing of personal data of both parties from the moment the system is activated. The fact that these functions are established by law in the Decree provides a legal basis for data collection; however, the Decree does not specify who has differentiated access to that information, under what conditions it may be consulted or shared, nor what happens to it when the system detects an error or a false alarm.

The third normative layer of SIMDEC regulations consists of Supreme Court of Justice (CSJ) rulings and the SIMDEC/OMDEC Protocol. These lower-level regulations are, however, the ones that most directly determine the actual experience of the system, as they define who can request the measure, how its technical feasibility is assessed, what information is required from the victim, and how an alert is managed.

Ruling No. 1779/2025 approved the "Protocol for the Application of Electronic Ankle Monitors: First Phase Implementation". Its explanatory text is revealing in itself: the protocol was created to provide judges with an appropriate procedural tool that allows them to ensure the correct application of SIMDEC, "in order to ensure and optimize the control, surveillance, as well as the location and movements of individuals and the precautionary measures applied". The protocol limits the first phase to the ordinary criminal jurisdiction, specifically to criminal guarantee judges of the capital city, and establishes that, initially, the measure applies to cases of domestic violence. It also provides that criminal guarantee judges, when applying the measure, must hear and inform victims of all proceedings regarding the ankle

50 According to information provided by the Ministry of the Interior in Note DGS911 No. 53/2026, in response to a request for access to public information, the company awarded the contract for the provision and operation of the system is Track Consortium, under National Public Tender No. 02/2024 (ID 451113), formalized through Open Contract No. 13/2024. (Unified Public Information Portal). Request #100405. (February 23, 2026). https://informacionpublica.paraguay.gov.py/#!/ciudadano/solicitud/100405)

monitors placed on the accused, and notify them of all hearings and rulings related to the case[51]. This last provision deserves special mention as it incorporates the victim as an active participant in the proceedings, not merely as a recipient of the system's decisions. However, its practical scope depends on the courts' actual operational capacity to comply with it, an issue that the ruling does not address.

For its part, Ruling No. 1801/2025 expanded the protocol along the same lines, gradually broadening the system's scope. The SIMDEC/OMDEC Protocol, approved on December 30, 2024, and implemented in accordance with the regulatory framework, is the system's most operational document and contains four elements that warrant specific attention.

First, the Protocol explicitly limits the first phase of implementation to the territorial jurisdiction of the city of Asunción. This geographical limitation is not merely a matter of capacity: it creates unequal protection for women victims of violence based on their place of residence, raising questions regarding compliance with the constitutional and international mandate of equal protection. It is worth noting that Note No. 53/2026 DGS911, obtained through a request for access to public information[52], records active devices outside the capital city between January 2025 and January 2026, suggesting that in practice the implementation may have extended beyond the Protocol's territorial scope.

Second, Article 5 (subsection b) of the Protocol defines the "electronic monitoring device" as the "technology used by SIMDEC to monitor and interact with the user and, where applicable, the victim". This definition is significant because it explicitly acknowledges that the device not only monitors the accused but also interacts with the victim. This interaction necessarily involves the collection of the victim's data.

Third, Article 7 regulates the technical feasibility report, which is the procedure by which it is assessed whether it is technically possible to apply SIMDEC in a specific case. To conduct this assessment, when the exclusion zone is conceived as a restraining order, the victim must provide her address, georeferenced location, and other relevant data (subparagraph e). This turns the victim into a mandatory source of data for the operation of the system that is meant to protect her. The Protocol does not establish any mechanism for informed consent or specific protection of that information.

Fourth, the Protocol stipulates that, in the event of an alert related to domestic violence or the comprehensive protection of women, the operator in the Control Unit must simultaneously call the victim "to ensure her safety, as well as to determine her location, and provide appropriate guidance" (relevant article, subsection c). Likewise, Article 15 regulates the panic button: "in cases where the Panic Button is activated by the Mobile Monitoring Unit (MMA) in the system, the Control Unit operator must answer the victim's call to verify the situation that triggered the alarm and act in accordance with the information received". These mechanisms are positive in terms of protection. However, their actual effectiveness depends on conditions that, upon a simple reading of the document, are not guaranteed. That is, the

51 The obligation to hear and inform the victim, as established by the Protocol, is a step forward that should not be overestimated. In its current form, it is a procedural reference that does not define the minimum content of that information, the timing of its provision, or the accessible format in which it must be communicated. Effectively informing a victim about the implications of SIMDEC is not merely notifying them that an ankle monitor has been placed on the accused; it is explaining what data about them will be collected, how the alert system works and what is expected of them, what technical limitations it has and what to do if it fails, and who to contact if the system does not respond. For this information to be meaningful and not merely a formality, it must also take into account the specific circumstances of each victim, including their digital literacy, access to connectivity, and emotional state at the time of receiving it. The obligation to inform should be regulated as a substantive requirement for the validity of the measure, not as an administrative step within the case file.

52 Unified Public Information Portal. Request #100405. (February 23, 2026). https://informacionpublica.paraguay.gov.py/#!/ciudadano/solicitud/100405

victim must have a mobile phone, that phone must be charged and have signal coverage, the victim must know how to use the device, and the operator must be able to respond in real time. The transfer of responsibilities to the victim—who must have a device, remain connected, and activate the system—is not critically examined at any point in the regulatory framework.

In short, the SIMDEC regulatory framework establishes a legally grounded system, but one with significant gaps in data protection, territorial coverage, operational effectiveness, and the distribution of responsibilities. These gaps reflect the structural limitations of a public policy designed under apparent urgency and without a prior impact assessment.

7.4. Substantive laws on gender-based violence

Law No. 5777/2016 "on Comprehensive Protection for Women against All Forms of Violence" constitutes the central substantive framework of the system for the protection of women in Paraguay. Its purpose is to guarantee women a life free from violence, recognizing the structural nature of gender-based violence and the State's obligation to act in all areas, from prevention, care, punishment, and reparation, with a differentiated approach. The law defines in Article 3 the different types of violence against women, implying that the electronic monitoring system may be applicable to a much broader range of situations than visible physical violence alone.

The explicit inclusion of Law No. 5777/2016 within the scope of SIMDEC has an important interpretive implication: the electronic monitoring system is subject to the principles of non-revictimization, access to justice with a gender perspective, protection of victims' privacy, and gender mainstreaming across all measures adopted. These principles should guide implementation so as to prevent the system from shifting operational burdens onto the victim, exposing her data to unnecessary risks, or operating in a way that discourages reporting.

On the other hand, Law No. 1600/2000 is the basic procedural instrument through which victims of domestic violence access the system of protective measures in Paraguay. It establishes the complaint procedure, the jurisdiction of the Justices of the Peace, and the measures that may be ordered, which include, through its articulation with SIMDEC, electronic monitoring measures. Law No. 6568/2020, which amended Law No. 1600/2000, expanded the scope of protective measures and the possibility of enforcing them through technology, thereby creating the regulatory link between the domestic violence regime and SIMDEC.

Along the same lines, Article 229 of the Criminal Code defines domestic violence as a crime offense, punishable by imprisonment for one to six years for anyone who, taking advantage of the family setting, commits acts of physical or psychological violence against a spouse, common-law partner, romantic partner, or a person with whom they have refused to resume a romantic relationship, as well as against relatives up to the fourth degree of consanguinity. The provision explicitly clarifies that the relationship includes both current and former relationships, and that cohabitation is not a requirement. This last clarification is particularly relevant for the application of SIMDEC, given that the threat may come from partners or former partners who do not live with the victim, making proximity monitoring operationally more complex and requiring a precise definition of the zones to be included and excluded.

The sentence may be increased to up to eight years if the offender is a repeat offender, if the act is committed against children or adolescents or in their presence, if the offender uses a weapon, or when the acts take place at the victim's home. These aggravating factors are precisely the types of situations that Law No. 7270/2024 authorized to be monitored via electronic ankle monitors, by eliminating the previous exclusion of individuals charged with crimes and the requirement of non-recidivism. However, questions arise here regarding the fact that this expansion was not accompanied by standards of proportionality or an impact assessment.

In short, the substantive framework on gender-based violence within which SIMDEC operates provides the legal basis that justifies its use and defines the principles with which it must be consistent. But this framework also raises questions: how is coordination between the various competent authorities ensured, how is the victim protected during the system's activation process, and how is the technology prevented from becoming an additional burden on those who already bear the consequences of violence? Furthermore, does the victim who initiates the process receive adequate information about the implications of applying an electronic ankle monitor to the aggressor? Does she know that the system will require her geolocation data? Is she in a position to evaluate the benefits and risks of this measure compared to other available alternatives? The SIMDEC/OMDEC Protocol stipulates that the victim must be informed and heard, but it does not define the minimum content of that information nor does it establish mechanisms to ensure that it is understandable and accessible to people with different levels of digital literacy.

7.5. The personal data regime: privacy as a right subordinated to the security discourse

The processing of personal data is perhaps the least visible aspect of SIMDEC, overshadowed by the prevailing security discourse and the urgency of protecting the lives and physical integrity of victims. However, this circumstance is not fully justified from a legal standpoint. A careful reading of the law and the implementation protocols reveals that, from the moment SIMDEC is activated, it generates and processes data relating to at least two individuals: the accused person, whose geolocation is monitored in real time, and the victim, whose contact information, address, and location are incorporated into the system as a condition of its operation. Privacy here is not an abstract value in tension with security, but rather a condition of security itself.

Since personal data is involved in the implementation of the system, inadequate protection could pose significant risks, including exposing the victim to the perpetrator, the leakage of information to unauthorized third parties, or the secondary use of the data for purposes other than those stated. Given this risk, SIMDEC must include a legal framework for the protection of personal data as a fundamental component.

In November 2025, Law No. 7593/2025 on the Protection of Personal Data was enacted in Paraguay. The approval of this law represents a significant institutional step forward in a country that, until then, lacked a comprehensive framework governing the processing of data by the government and private actors. However, the law itself establishes a transitional period of 24 months before it fully enters into force, subject to its regulation. During this interval, the legal framework governing the processing of data generated by the system is sector-specific and fragmented.

In the case study, this transitional period means that the Paraguayan government can continue to expand a surveillance system on data of vulnerable individuals without the principles, safeguards, and oversight mechanisms that a general data protection law should provide: data minimization, specific purpose, storage limitation, rights of access and rectification, an independent supervisory authority, and a regime of administrative sanctions[53]. The absence of such a framework does not mean that SIMDEC operates in a complete legal vacuum; it means that it operates under a scattered set of sector-specific regulations that cover partial aspects but do not guarantee comprehensive protection.

In the absence of a general law, data processing within the SIMDEC framework is governed by a set of sector-specific regulations that were not designed specifically for this system and which, as a result, fail to address critical aspects of its operation. Decree No. 466/2023, Articles 17 through 19, is the regulation most directly applicable to SIMDEC with regard to data protection. Article 17 authorizes the use of information generated by the system for statistical or criminal policy purposes, provided that this does not violate the specific circumstances for the processing of personal data. Article 18 establishes a retention period of five years from the judicial notification of the termination of the measure, after which the information must be destroyed[54]. Article 19 classifies the improper use or disclosure of the information as evidence of the commission of the criminal offense of disclosure of a private secret under Article 147 of the Criminal Code, without prejudice to other administrative sanctions. These provisions serve as a starting point but have certain limitations; for example, they do not regulate access based on the institutional role of each actor or define who is authorized to audit compliance with these rules[55].

Law No. 6,534/2020 on the Protection of Personal Credit Data is a sector-specific regulation aimed at the financial and credit ecosystem. However, in the absence—until the new regulation fully enters into force—of a general personal data protection regime[56], its definitions and principles are applicable as an interpretive reference by analogy to data processing in other contexts, including data processing in the SIMDEC. In this context, the data processed in SIMDEC—in particular the accused person's geolocation data and the victim's contact and location data—must be considered personal data requiring protection and safeguards at the time of processing, even in the absence of a fully effective regulation, given its intrusive nature and the risks associated with its use.

---

53 The principles mentioned above are part of any modern data protection regime. Data minimization requires that only the data strictly necessary for the stated purpose be collected. The principle of purpose limitation prohibits the use of data for purposes other than those that justified its collection: data collected to monitor a precautionary measure cannot be used, for example, to build risk profiles or feed police databases. The retention limitation requires that data be retained only for as long as necessary and deleted once its purpose has been fulfilled. The rights of access and rectification ensure that individuals whose data is processed can know what information exists about them and correct it if inaccurate. The independent supervisory authority is the state body—separate from those operating the system—responsible for overseeing compliance with these rules and receiving complaints. Finally, the administrative sanctions regime establishes specific consequences for non-compliance.

54 On this point, it is noteworthy that Decree No. 466/2023 stipulates that the information must be destroyed five years after the measure has been terminated. The Terms and Conditions (T&C) of National Public Tender No. 02/2024 (ID 451113), through which SIMDEC was awarded and implemented, state, however, that the information "shall be delivered to the OMDEC" upon contract completion, without mentioning destruction. They are not necessarily contradictory, but they are not consistent either. The terms and conditions do not provide for any destruction protocol, which leaves open the question of what happens to the data once it is transferred and whether the retention period specified in the Decree is actually applied.

55 The terms and conditions of Tender No. 451113/2024 state that "SIMDEC shall be the data controller, as the owner of the database, and the Service Provider shall be the data processor". This distinction between the data controller and the data processor is correct in terms of data protection, but the terms and conditions do not specify what specific obligations the company assumes as the data processor. Without an independent technical audit, without contractually enforceable security standards, and without unrestricted access by the government to its own data, the distinction is more formal than substantive.

56 Law No. 7,593/2025 expressly repeals, through Article 59, various provisions of Law No. 6,534/2020, including the definitions of personal data and sensitive personal data (Art. 3, subsections a and b), as well as the prohibition on the disclosure of sensitive data (Art. 4). However, given that the new law has not yet fully entered into force, a regulatory transition period has arisen in which the previously applicable definitions have lost their formal basis, while the new regime is not yet fully applicable. This situation requires reliance on systematic interpretations and international standards to ensure an adequate level of protection for personal data.

For its part, Article 10 of Law No. 4,868/2013 on Electronic Commerce stipulates that providers of intermediation and data hosting services[57] must store connection and traffic data generated during the provision of the service for a minimum period of six months, solely for the purpose of facilitating the location of the terminal equipment used to transmit the information. The law expressly prohibits the use of such data for purposes other than those permitted by law and requires the adoption of security measures to prevent its loss, alteration, or unauthorized access. This provision is relevant to SIMDEC because the company providing the system operates, in practice, as an intermediary service provider that stores and transmits connection and geolocation data in real time. Its regulatory Decree No. 1,165/2014, in Article 11, adds the duty to inform the users about the purpose and processing of their personal data, who will receive it, and who will be responsible for its safekeeping, thereby reinforcing the principle of transparency in data processing. However, it could be argued that these regulations constitute a framework that, taken together, amounts to a patchwork measure in the absence of comprehensive protection, thereby compromising the integrity of the system and the effective protection of the individuals involved.

Similarly, the National Telecommunications Commission (CONATEL) establishes requirements for the registration and retention of traffic data in connection with the provision of communications services. Thus, Board Resolution No. 0700/2025[58]—which amends Resolution No. 2583/2024—requires internet service providers to retain connection records for a minimum period of six months, including information such as IP addresses, ports, date, time, and subscriber identification (Article 1). Likewise, Law No. 7549/2025[59] reinforces this framework by establishing a minimum retention period of twelve months for traffic data (Art. 7), with a purpose strictly limited to the identification of users in the context of specific criminal investigations (Articles 1 and 2).

However, these regulations follow a sector-specific and narrow approach focused on traffic and connectivity data, and do not address the processing of real-time geolocation data or other categories of information such as those processed and stored by SIMDEC. As a result, their applicability is, at best, analogical and limited. In this context, the establishment of a single five-year retention period for SIMDEC data, as provided for in the regulatory decree, exceeds existing sectoral standards and raises questions regarding proportionality, especially given the lack of differentiated criteria based on the type of data involved or clear mechanisms for the storage, review, and verifiable deletion of information. We thus have, on the one hand, a model of minimal and purpose-limited data retention and, on the other, a regime of prolonged data storage proposed by the SIMDEC regulatory framework, without equivalent governance to ensure its proper handling[60].

57 It should be noted that providers of electronic monitoring systems, such as the ankle monitors used in the SIMDEC program, do not strictly fall under the category of data intermediation or hosting service providers as defined in Law No. 4,868/2013. However, given that these systems involve the continuous transmission, storage, and processing of geolocation data via telecommunications networks—including data traffic and signals associated with connectivity—the retention, security, and purpose-limitation obligations established in that legislation may be considered an analogous framework for data governance.

58 National Telecommunications Commission. (2025). Board Resolution No. 0700/2025 amending Board Resolution No. 2583/2024 on the retention of connection records. Retrieved April 14, 2026, from https://www.conatel.gov.py/wp-content/uploads/2025/07/res-0700_2025_modif-res-2583_2024_conservacion-de-registros-de-conexion-internet-3.pdf

59 Paraguay. (2025). Law No. 7,549/2025 establishing the mandatory retention of data to combat child and adolescent pornography and related criminal offenses. Retrieved April 14, 2026, from https://silpy.congreso.gov.py/web/descarga/ley-146014

60 It may seem that these discussions about how data is stored are secondary to a much more urgent goal, such as preventing violence and protecting the lives of victims. However, precisely because the system is designed to protect, it is essential that it functions properly and securely. If data is stored for too long, without clear rules about who can access it or how it is deleted, the very system intended to protect may end up creating new risks. That is why, when designing a public policy like SIMDEC, it is not enough to simply incorporate technology; it is also necessary to define how the data that technology produces is used, stored, and protected.

The first gap is the absence of a protocol for differentiated access to data. SIMDEC involves multiple stakeholders, ranging from judges, prosecutors, system operators, police, service providers, to staff at the Ministry of Women, who have distinct roles and who, logically, should have different levels of access to the information generated. However, no current regulation establishes who can view what, under what conditions, with what access logs, and under what accountability. This is not a mere technical detail but a condition that facilitates the misuse of information—whether intentionally or unintentionally—and prevents any meaningful audit of data management.

The second gap is the lack of regulation regarding interoperability between systems. SIMDEC does not operate in isolation but interacts—or should interact—with the 911 system, the Prosecutor's Office, and eventually the police alert system. Each of these systems has its own databases, its own access protocols, and its own data retention rules. The absence of an interoperability framework means there are no clear rules regarding what data can be shared between these systems, in what format[61], with what safeguards[62], and under what controls. In practice, this can lead to both unnecessary duplication of information and a lack of coordination in emergency situations.

The third gap is the lack of an independent technical audit. The company that provides the SIMDEC system operates the system's infrastructure, including the servers where geolocation and interaction data are stored[63]. No current regulation specifies where these servers must be located—whether in Paraguay or in a foreign provider's cloud—what technical and legal security standards they must meet, or who has the authority and technical capacity to audit such compliance. Delegating data infrastructure to a private provider, without independent auditing, constitutes a black box from the perspective of public governance.

The fourth gap concerns the liability regime for security breaches. Article 19 of Decree No. 466/2023 classifies the misuse of information generated by SIMDEC as evidence of a criminal offense. But this reference to the Criminal Code is essentially reactive: it takes effect only after the damage has occurred. There is no administrative mechanism for preventive control, no obligation to notify affected individuals in the event of a security breach, and no defined timeframe for the institutional response to incidents of this type. In the context of SIMDEC, where a leak of a victim's location data can have direct consequences for her physical safety, the absence of a preventive and notification regime is particularly serious.

61 In fact, it is striking that the Terms of Reference of Public Tender No. 02/2024 (ID 451113) stipulate that system data—including stored locations and geofences—may be delivered on a USB flash drive, external hard drive, or CD/DVD. Transferring geolocation data of victims and defendants on portable physical media, without the tender specifications establishing any encryption standards or chain-of-custody protocols, poses a significant security risk. The mention of CDs/DVDs also reveals a technological gap that is by no means minor when it comes to critical surveillance infrastructure.

62 It is worth noting here that, upon reviewing the Terms of Reference of Public Tender No. 02/2024 (ID 451113), daily backups of system data are required, which is a positive development. However, it does not establish any technical standards regarding how this should be carried out: encryption, secure storage, restricted access, or integrity verification. A daily backup without defined security standards offers a formal guarantee without verifiable technical content.

63 A review of the Terms of Reference of Public Tender No. 02/2024 (ID 451113) confirms that the document does not establish any requirements regarding the physical location of the servers on which the information generated by SIMDEC is stored. The only relevant mention requires that they operate in "high-availability mode" because it is a mission-critical system, but it does not specify whether they must be located within the national territory, under which legislation they operate, or whether the State has the right to audit them. This omission is significant, as the location of the servers determines which legal framework governs the stored data, which authorities can access it, and what happens to that information if the contract is terminated or the company faces legal issues in its country of origin.

The fifth gap is the lack of a proportionality justification in the data retention regime. Article 18 of Decree No. 466/2023 stipulates that information generated by SIMDEC must be destroyed five years after the termination of the measure. This time limit is not accompanied by any justification of proportionality, nor differentiated according to the type of data (geolocation, contact information, alert records), nor adjusted according to the severity of the case or the outcome of the judicial proceedings. A uniform five-year time limit for all data, for all individuals, in all cases, does not satisfy the principle of data minimization that international data protection law requires as a standard.

Taken together, these gaps are not exceptions to the system's normal operation. SIMDEC currently operates within a legally inadequate data protection framework. This situation disproportionately affects victims of gender-based violence, who have the most to lose if the information they provide to the system ends up being accessible to the very person who should be kept away from them.

An examination of SIMDEC's legal framework now makes it possible to formulate an overall assessment. Not a mere inventory of rules, but a critical evaluation of the system's regulatory architecture in light of the standard that constitutional and international law itself demands for any measure that restricts or interferes with fundamental rights: the test of legality, necessity, and proportionality[64]. This test is not an external tool applied to the system from the outside; it is the benchmark that the very framework ratified by Paraguay imposes as a condition for the validity of any State intervention affecting rights.

The first threshold of the test asks whether the measure has a sufficient legal basis: whether it is provided for in a regulation that is accessible, precise, and predictable in its effects. The answer in this case is affirmative, in general terms. As noted, SIMDEC has a formal legal basis in Law No. 5863/2017, its amending Law No. 7270/2024, Regulatory Decree No. 466/2023, and the implementation protocols. However, the requirement of legality is not satisfied merely by the existence of regulations, as it also demands that these regulations be sufficiently precise so that the individuals subject to them can foresee the consequences of their application. In this regard, the gaps identified regarding personal data—such as the absence of rules for differentiated access, the lack of independent auditing, and the lack of clarity regarding the location of servers—weaken the quality of the system's legality. A rule that authorizes the processing of personal data without defining who has access to it or under what conditions does not fully meet the standard of precision required by the principle of legality.

The second threshold asks whether the measure pursues an objective that is compatible with human rights and articulated with sufficient clarity. Here, the answer is also affirmative. The protection of women who are victims of gender-based violence and the alternative to pretrial detention are objectives that are not only compatible with the human rights framework but are required by it.

Now, the third threshold asks whether the measure is necessary: whether the intended objective cannot be achieved through less intrusive measures, or whether its selection over available alternatives is at least rationally justified. Here, the answer is only partially affirmative. Comparative international evidence—which is examined in later chapters of this study—shows that electronic monitoring can be a useful tool under certain conditions, but that its effectiveness depends on a set of institutional factors that the

64 This test has its roots in German constitutional theory and was systematized by the legal scholar Robert Alexy in his work Theory of Fundamental Rights (1985). Its original formulation is known as the principle of proportionality, of which legality, necessity, and proportionality in the strict sense are sub-requirements; that is, not three independent tests but three levels of the same analysis. The Inter-American Court of Human Rights has incorporated this standard into its jurisprudence, and in judicial practice and Latin American legal literature, its elements are often presented as autonomous criteria—a usage that this study follows without disregarding their common origin. What matters, in any case, is the function that the analysis serves: to compel the State to rationally justify why a restriction of rights is authorized, necessary, and does not cause more harm than it seeks to prevent.

Paraguayan regulatory framework does not guarantee, such as adequate response times, operational capacity for continuous monitoring, and integration with victim assistance services. More importantly, SIMDEC was implemented without a prior impact assessment and without a systematic comparison with other, less intrusive protective measures. The need for a measure cannot be taken for granted; it must be demonstrated, and that exercise is absent from the SIMDEC implementation process.

The fourth threshold is the most demanding and the one that creates the greatest tension in the case of SIMDEC. Proportionality asks whether the means employed are appropriate to the intended purpose, without disproportionately sacrificing rights. SIMDEC presents a structural problem here that the regulatory framework has not resolved: in order for the system to function, it requires the victim to provide her contact information and geolocation, to be available for contact in the event of an alert, to have a working mobile device, and to bear the operational responsibilities that the panic button entails. This burden is not proportionally justified in any regulatory instrument, nor has it been assessed whether the system's benefits for victims outweigh the risks generated by their participation in it. A protection system that turns the protected person into a subject of personal data collection, without clear guarantees regarding how that information will be protected, raises a question of proportionality that the current legal framework does not address.

Finally, accountability must be incorporated as an additional dimension of the analysis, in line with the approach set forth in the International Principles on the Application of Human Rights to Communications Surveillance (Necessary and Proportionate Principles, 2013), which explicitly establish that independent oversight and accountability are autonomous conditions of legitimacy for any State surveillance system[65], beyond the classical proportionality test.

In this regard, the regulatory framework underpinning SIMDEC is predominantly reactive and punitive. Sanctions for the misuse of data do exist, but they only apply once harm has already occurred. There is no independent technical audit, no obligation to publish periodic statistics on the system's operation, no impact assessment linked to the renewal of service contracts, and no mechanisms for the participation of women's organizations in the monitoring of the system[66]. Accountability cannot be merely a legal remedy to be sought after harm has occurred; rather, it must be a structural condition of the system's operation.

Here, it should be clarified that the identified weaknesses are not a condemnation of the system, but rather a legal diagnosis. It is clear that SIMDEC has a legal basis and pursues legitimate purposes, but it has certain shortcomings regarding precision legality, demonstrated necessity, proportionality in the processing of victims' data, and structural accountability. These weaknesses can be corrected through regulatory adjustments and concrete institutional decisions. And it is precisely through their identification that the recommendations of this study can be legally grounded and politically operational.

---

65 On this point, it is important to recall the report by the United Nations High Commissioner for Human Rights, The Right to Privacy in the Digital Age (A/HRC/48/31, 2021), which emphasizes that independent oversight and accountability mechanisms constitute autonomous conditions of legitimacy for State surveillance systems and cannot be considered satisfied merely by meeting the proportionality test.

66 A review of the Terms and Conditions of Tender No. 02/2024 clarifies some of these points. Regarding the technical audit, the terms require that the software include "auditing and event logging" (software security criterion 12), but this audit is internal to the system and operated by the supplier itself, not by an independent body. Regarding government oversight of the data, the contracting agency's access to the production database is conditional on it being "requested by the Contracting Authority" and limited to read-only access, meaning that the government does not have unrestricted or permanent access to the information generated by the system. Regarding penalties, the terms of reference provide for contractual sanctions in the event of failure to meet technical service levels, but do not include specific penalties for data security breaches or the misuse of sensitive information. Finally, the terms of reference contain no obligation to produce periodic public reports on the system's operation, nor any mechanism for accountability to the public.

The following chapters examine aspects that the legal framework alone cannot reveal: how the system works in practice, the level of transparency surrounding the procurement and contracting processes that underpin it, and what other international experiences teach us about the limits and conditions for the effectiveness of electronic monitoring in contexts of gender-based violence.

7.6. Empirical findings: implementation, analysis, and institutional tensions

To complement the normative analysis and reconstruct the actual functioning of these technologies in Paraguay, this research incorporated an empirical strategy based on two approaches. First, three requests for access to public information were submitted through the Unified Portal for Access to Public Information, addressed to the Ministry of the Interior, the Ministry of Women, and the National Police, all sent on February 23, 2026. On the other hand, semi-structured interviews were conducted with two key actors directly linked to the system's operation or activation: a representative of the Ministry of Public Defense and the Executive Secretary of Criminal Technical Unit of the Supreme Court of Justice and representative to SIMDEC. Additionally, three attempts were made to contact representatives of the Ministry of Women, which were unsuccessful. However, a response was provided through the public information request process.

The responses received were uneven. The Ministry of the Interior provided a detailed reply that allowed for a more comprehensive understanding of SIMDEC's operational functioning, its usage statistics, technical feasibility criteria, and several aspects of the contracted infrastructure. In contrast, the Ministry of Women responded in more general terms, providing basic information about its institutional tools without submitting the requested technical documentation.

In the case of the National Police, although the request was initiated in a timely and proper manner, the substantive response was not received within the timeframe originally set for the investigation: the reply, channeled through the TRACK Consortium, the service provider of the INTELLITRACK system, arrived approximately one and a half months after the request was submitted, via Note D.T.A. No. 56/2026, dated March 31, 2026, addressed to Commissioner Inspector General Rafael Candia, Director of the CSE of the National Police and representative to the SIMDEC Inter-institutional Control Office. Despite its late arrival, it was decided to incorporate this data into the analysis because it provides a level of quantitative and operational detail that none of the other sources had provided, especially regarding quarterly series of alerts, specific technical incidents, staff training, and criteria for classifying false alarms. This asymmetry in the quality, timeliness, and depth of the responses constitutes, in itself, a finding regarding the state of public transparency surrounding these technologies.

The actual implementation of the system is heavily conditioned by material infrastructure

One of the clearest findings of this research is that the implementation of SIMDEC does not depend solely on a judicial decision, but on a series of physical and technical conditions without which the measure cannot become operational. In the interview with the Judiciary, the representative to SIMDEC, Dr. Silvana Luraghi, explained that, before granting the measure, the judge issues a request for a technical feasibility study, and that many initial reports were negative because the accused persons lived in areas with precarious electrical connections or poor signal coverage. In her words, "many initial reports were negative because the accused lived in vulnerable areas (flood-prone neighborhoods) with clandestine connections or no signal", while at the time of the interview, there were "163 positive reports".

This assessment is supported by the official response from the Ministry of the Interior, the institution responsible for operating the system. According to the response provided through a request for access to public information, 196 technical feasibility requests were received in 2025, out of which 161 were approved and 35 were deemed "not feasible". Among the reasons are the lack of regular electrical infrastructure, the absence of an ANDE (National Electricity Administration) meter, insufficient cellular or satellite signal, the inability to correctly locate the address, denial of access to the site, and the existence of judicial orders with incomplete data or outdated addresses. The response itself emphasizes that the lack of regular electricity and poor signal coverage are the critical factors limiting the effective implementation of SIMDEC in rural areas, peripheral zones or informal urban settlements.

The response from the TRACK Consortium, as the technical operator of the INTELLITRACK system contracted by the National Police, adds another layer to this assessment. The report details a series of technical incidents following the installation of the devices that confirm the material fragility on which the system's daily operation depends: permanent loss of communication in devices that "stopped transmitting data permanently, making remote monitoring impossible"; charging issues or lack of charging mostly attributed to "improper use by the beneficiary, including mishandling or damage to the connection port during the charging process"; and the absence of positioning data linked to failures in the device's GPS module affecting the transmission of geolocation data. In addition, a specific incident documented on February 7, 2026, consisting of the temporary unavailability of the alarm management module between 11:30 a.m. and 12:00 p.m., which, while it did not interrupt real-time monitoring, prevented the registration of new devices during that interval.

This fact is crucial because it challenges the notion of the ankle monitor as a universal, immediate, and self-sufficient solution. In practice, access to this measure depends on electrical infrastructure, connectivity, accurate geolocation of the residence, minimum technical feasibility, and, furthermore, the operational continuity of a platform managed by a private service provider. The promise of constant monitoring rests on a deeply unequal material foundation and on a technological architecture that also experiences occasional failures. This confirms that the policy of technological surveillance does not operate within a homogeneous territory, but rather over a landscape of preexisting inequalities and on a contracted infrastructure that, like all infrastructure, fails.

Added to this is a significant financial barrier: individuals interested in accessing this measure must cover the cost themselves, and, as the specialized public defender himself noted, there are only a limited number of devices provided free of charge for the criminal division of the Public Defender's Office. In this scenario, the ankle monitor ceases to be merely a measure of protection or control and is revealed as an alternative to prison that is differentially accessible depending on the economic capacity of those who request or need it. Furthermore, this shows that the State's capacity to "prevent" crime through technology depends not only on basic living conditions and public infrastructure, but also on the material ability to afford access to the measure itself.

A gradual implementation shaped by material and economic constraints

Another important finding is that the implementation of SIMDEC was neither linear nor uniform, but rather gradual, limited in its initial stage, and later accelerated in terms of territorial expansion and equipment availability. In the interview with the representative of the Judiciary to SIMDEC, it was explained that when the law began to be effectively enforced in January 2025, "we only had 20 devices", so its use was initially limited to cases of domestic violence. The interviewee added that between January and August 2025, expansion was gradual "due to a shortage of equipment", and that it was not until August of that same year that the system was made available "nationwide and to all criminal judges". At the time of the interview, the same source stated that the system had "3,000 ankle monitors available" and "156 ankle monitors in use throughout the country".

However, when this information is compared with the official response from the Ministry of the Interior, obtained through the access to public information mechanism, a more nuanced picture emerges. The management report submitted by the operating authority indicates that in 2025, 74 installations and 28 uninstallations were carried out, while as of the end of January 2026 there were 86 active beneficiaries, increasing to 94 by the end of February 2026. It also reported that the areas with the greatest presence of the system were Central, Alto Paraná, and Asunción. In other words, even though the institutional narrative refers to nationwide expansion and growing availability, the available data show that implementation remains limited and geographically uneven.

The response provided by the TRACK Consortium to the National Police also reveals how this gradual implementation affected the volume and type of alerts generated by the system. The quarterly statistics provided show exponential growth that coincides with the system's nationwide rollout: during the first quarter of 2025, only 2 alarms were recorded (all for "Inclusion Zone Violation"); in the second quarter, 12 alarms (critical battery, escalated critical battery, and 9 exclusion zone violations); in the third quarter—coinciding with the August 2025 expansion—the number of events jumped to over 9,000, including 6,260 "Inclusion Zone Violations", 2,555 "Victim Proximity Violation", and 314 "Exclusion Zone Violations"; in the fourth quarter of 2025, inclusion zone violations reached 57,234 events; and in the first quarter of 2026, there were 48,099 inclusion zone violations, 162 victim proximity violations, 47 exclusion zone violations, as well as 159 critical battery alerts, 5 strap tampering alerts, and 2 corrected tampering alerts. This growth cannot be interpreted simply as an increase in violence or violations: the Consortium itself clarifies that, out of the total alarms recorded in that last quarter, "only 5 represented a violation of the control measure applied". In other words, out of the tens of thousands of events generated by the system, only a minimal fraction corresponded to actual violations. This data is, in itself, one of the most revealing findings of the investigation: the expansion of the system produced a massive volume of alerts whose correlation with actual risk situations is marginal, which forces us to rethink what is being measured when SIMDEC's "coverage" is celebrated.

Another aspect must be added to this, one that is less visible in the narrative of "modernization" but central to understanding some of the system's potential limitations: the economic cost of the measure. In the interview with the same Judiciary representative, it is explicitly stated that "there is a fee that perpetrators must pay if they have private attorneys" while those represented by public attorneys due to insolvency are exempt. The interviewee added that the device "has a cost" and that, in her personal assessment, that amount "is quite high; it is not a small sum", which makes the payment of the fee a potential obstacle to its implementation. She also specified that the victim does not pay for the complementary device, although we have no information on whether or not the victim pays for the mobile data required for the effective operation of the mobile phone. The response received was that "the victim never pays anything; the State provides the mobile phone".

This point is particularly relevant because it shows that the expansion of the system depends not only on infrastructure and judicial will, but also on an access model shaped by criteria of financial solvency, public defense, and budgetary availability. The interviewee herself suggested that, in the future, the government would need to have "a budget allocated by law for this purpose", so as not to rely exclusively on fee payments by users. This interpretation is reinforced by the interview with Osvaldo Prates Grassi, a representative of the Ministry of Public Defense, who stated that "currently, the use of the ankle monitor is subject to a fee, and free access is exceptional", and that this "represents a barrier". From this perspective, the implementation of the system faces not only technical or territorial obstacles but also concrete economic constraints that can limit effective access to the measure, especially in contexts of vulnerability.

Taken together, these elements show that the expansion of SIMDEC should not be interpreted solely as an increase in devices or territorial coverage. It must also be analyzed in relation to the social, budgetary, and economic conditions that enable—or limit—its effective implementation. In other words, the system's growth does not eliminate the structural inequalities in access that are characteristic of Paraguay.

Prevention as a potential circuit of surveillance

The interviews and institutional responses allow us to reconstruct with considerable clarity how the concept of "prevention" operates within SIMDEC. In the interview with the representative of the Judiciary to SIMDEC, the ankle monitor is presented as "a vital tool for the protection of victims and for the real and effective enforcement of judicial rulings", in a context where previously "the judge had no way to truly verify compliance". The same interviewee added that, prior to the system, random monitoring of house arrest was highly precarious and lacked structured mechanisms, because the police did not have sufficient institutional capacity to carry out the verifications. In this context, technology appears not only as a tool for protection, but also as a mechanism to make judicial decisions enforceable and verifiable, decisions that previously depended on far more uncertain compliance.

The operational response from the monitoring authority (OMDEC) reinforces this approach. It explains that the system operates through 24/7 monitoring conducted by OMDEC, incident classification, and a tiered response activation process. Events are categorized into technical notifications, deterrent warnings, and immediate-response alarms. Upon receiving a warning, the operator issues up to three persuasive messages; if there is no compliance, the police intervention protocol is activated, involving georeferenced verification, dispatch of resources through the local police station, the 911 system, or the LINCE unit, and simultaneous contact with the victim to provide self-protection guidance. All activity is recorded in the system, including movements, communications, and event closure.

The information provided by the TRACK Consortium supports this approach from the perspective of the technology provider. The report describes a protocol for verifying false alarms that includes analyzing the movement patterns recorded by the system, verification via video call, and direct consultation with the beneficiary regarding their real-time location, using the personal phone number provided at the time the device was installed. This detail shows that, in practice, "prevention" operates through a technical verification process that combines GPS, video calls, and telephone communication with the person being monitored, that is, an additional layer of surveillance that is activated every time the system generates an unconfirmed alert.

What emerges from this reconstruction is a very specific form of prevention: not a comprehensive policy of care, support, and redress, but rather a circuit of geolocation, risk classification, warning, traceability, and operational response. In other words, in practice, prevention is organized less as a structural transformation of the conditions that produce violence and more as the anticipation of events through remote surveillance and police response. This finding does not imply denying that the system may offer some degree of protection and control; rather, it implies clarifying that the technological prevention currently implemented in Paraguay follows a predominantly security- and operations-based logic, rather than a comprehensive logic of rights and care.

The incorporation of victims into the surveillance circuit

One of the most significant findings of the empirical analysis is that the system is not directed solely at the perpetrator. It also incorporates the victim into the technical and operational framework. In the interview with the Judiciary representative, it was explained that the system includes "an ankle monitor for the accused and an electronic device (mobile phone) for the victim to communicate directly with the police". The same source clarified that this use is voluntary and that "90% agree", but that if the victim does not accept the mobile phone, then the police are limited to monitoring the aggressor's ankle monitor. It was also mentioned that the State provides the mobile phone and data for this purpose.

The operational response provided by the authority in charge of the system matches that description and clarifies it further: the victim's device is called MMA (Mobile Monitoring Unit) and works with an app called Empower. The perpetrator's device is a ReliAlert XC transmitter. The victim's device includes a panic button and direct communication with the monitoring center (OMDEC). In turn, the response protocol indicates that, upon an alarm or after all attempts at persuasion have been exhausted, the operator must contact the victim to warn her of the aggressor's proximity and provide self-protection guidance. In other words, the victim is not left out of the technological circuit: she is also located, alerted, and incorporated into the system's response flow.

The statistics provided by the TRACK Consortium allow for a more accurate assessment of the proportion of victim-centered surveillance within the total volume of alerts. In the third quarter of 2025 alone, 2,555 alerts were recorded for "Victim Proximity Violation", and in the first quarter of 2026, this type of alert accounted for 162 incidents. Each of these records implies, by definition, effective monitoring of the victim's movement relative to the aggressor, and therefore sustained tracking of the victim's own location. In other words, technological protection is not limited to monitoring the aggressor: it necessarily generates data on the victim, her movements, and her relative proximity.

This issue becomes even more critical when considering the perspective of the Ministry of Public Defense (MDP). In that interview, Osvaldo Prates Grassi, a representative of the MDP, stated that "the victim must have an active internet or mobile data connection at all times for the defense system to function", and it is emphasized that this constitutes "an economic barrier". It is also noted that the software linked to the system requires permissions that compel constant data sharing and that, in technical meetings, "no one addresses how the exposure of the victim's movements to third parties violates her privacy".

Taken together, these sources support the argument that technological protection not only expands the State's monitoring capacities, but could also shift technical burdens onto victims. Although the State formally provides the phone and data in some cases, the system's daily use requires battery power, connectivity, device availability, basic proficiency with the tool, and sustained exposure to a localization and alert regime. From a feminist and human rights perspective, this compels us to ask to what extent the promise of technological protection ultimately shifts part of the burden of ensuring safety onto those who are already in vulnerable situations.

Inequality in government transparency

Requests for access to public information revealed a clear pattern of institutional asymmetry. The most comprehensive response came from the Ministry of the Interior, the institution responsible for the system's operations, which provided detailed data on technical feasibility, facilities, number of active users, event classification, minimum records, data access, and operational continuity. Thanks to that response, it was possible to reconstruct with considerable precision the practical logic of SIMDEC and some of its main limitations.

In contrast, the response from the Ministry of Women was much more basic and general. The institution identified the "SOS Mujer" 137 emergency hotline and the WhatsApp assistance channel as its primary technological tools, and stated that both are supported by "protocols, operational manuals, intervention guidelines, and ministerial resolutions". However, they then indicated that these documents "are for internal use only and cannot be shared, ensuring confidentiality and data protection". They also mention general categories of collected data and mention initiatives related to accessibility and digital literacy, but without providing sufficient technical or regulatory documentation to allow for an external audit of the governance of these tools. The response regarding barriers and revictimization was equally revealing. The Ministry of Women acknowledged that "technological, economic, and territorial barriers constitute structural factors that limit equitable access to services", and maintained that digital contexts can generate "situations of permanent exposure, control, or pressure on victims", with potential effects of revictimization. However, these statements were not accompanied by specific assessments, metrics, diagnostic reports, or substantive documentation on how these risks are specifically addressed in the technological tools under its purview. In that regard, the response acknowledges the problem but does not provide sufficient public evidence of how the institution is addressing it.

The case of the National Police deserves special consideration. Unlike the Ministry of the Interior, which responded directly with institutional information, the National Police channeled its response through the private contractor (Consorcio TRACK), which is in itself a significant fact: the entity ultimately producing the operational information that feeds into public analysis is not a government institution, but a contracted company. Furthermore, the response arrived after the deadlines established by public information access regulations. Paradoxically, and despite this delay, it was one of the most detailed responses regarding quarterly statistics, specific training dates, and specific technical incidents. This dual condition—delayed response and informational density—reveals a structural tension: granular information exists and is available in the provider's systems, but its dissemination to the public is not organized under proactive publication standards; instead, it depends on specific requests answered after the deadline and mediated by a private actor.

From a transparency perspective, this is relevant because an administrative response does not automatically equate to an auditable public policy. The quality of the information provided, its level of detail, and the availability of specific documents remain highly uneven across institutions, which hinders public scrutiny of the system as a whole.

The weakness of the debate on privacy, data processing, and auditing

Another of the most concerning findings of the analysis is the fragility of the institutional debate on privacy, data protection, and access controls. The Ministry of Public Defense explicitly stated that "there is no formal recommendation" on these issues and that, in practice, "privacy seems to be treated as a secondary matter, both for the victim and the perpetrator", although it is acknowledged that the violation of privacy can be "worse than the illness". This statement carries particular weight because it does not come from an external critic, but from within an institution that is directly involved in implementing and managing these measures.

The same interview adds that technical working groups discuss GPS accuracy issues or operational security concerns, but "no one addresses how the disclosure of the victim's movements to third parties violates her privacy". It is also noted that the software audit, data retention and deletion, or the need to control who accesses the information and on what grounds were never substantively addressed. There is even a mention of a kind of "blind trust" that the ankle monitor is the "magic solution", and it is suggested that the technology functions as a "double-edged sword".

However, this weakness in the institutional discussion coexists with a more established narrative regarding technical security. The operational response indicates that access to the data is "strictly hierarchical and limited to authorized OMDEC and Monitoring Center personnel", that the data is encrypted "both at rest and in transit", and that the information is stored for the duration of the contract, after which it is deleted from the provider's systems and handed over to OMDEC.

The response from the TRACK Consortium adds important details and raises new questions. According to the provider, access to geolocation data and reports "is restricted to users in the Control and Monitoring Center, in accordance with the profiles and privileges assigned within the platform", while a "Support Team" operates on the same platform with "differentiated privileges that allow users and profiles administration, without interfering in the operational monitoring tasks". The creation of new user profiles is restricted exclusively to those with administrator roles. When an operator is reassigned, the outsourced company is formally notified to deactivate the profile; and, for new hires, the account activation is processed via a formal request. Additionally, "operational controls are carried out through daily verification of the roster of officers assigned to each shift". Finally, it is reported that the platform records users' activities "through access and operation logs", which "enables the traceability of actions performed within the system" and facilitates "subsequent verification of accesses and the detection of any misuse".

This level of technical detail, however, reinforces the critical finding rather than dispelling it. What TRACK Consortium describes is an internal audit system managed by the provider itself and by law enforcement authorities, not an independent, external, or citizen-led audit mechanism. The logs exist, but there is no public information on who reviews them, how often, based on what criteria, or what the consequences are if unauthorized access is detected. In other words, the system documents its own use, but that documentation does not translate into public accountability.

The finding, then, is not that the system completely lacks technical safeguards, but that there is a gap between technological security and democratic governance of the data. There are access controls, encryption, storage, and activity logs, but what does not appear with equal clarity is a sufficiently developed public framework for independent auditing, verifiable traceability of access, material limits on data processing, or accountability mechanisms toward the affected individuals.

The system is designed to record data but not to provide accountability with the same level of detail

Finally, empirical evidence supports another important finding: SIMDEC is designed to generate and store a large amount of information, but this recording capacity does not correspond to the level of public oversight available. The operational response indicates that the system stores data on the perpetrator, real-time geolocation, movement history, type of event or alert, date and time, and the police unit involved. It is also reported that all activity is logged in the software, including operator communications and the closure of the event by police units.

The information provided by TRACK Consortium confirms and clarifies this assessment. On the one hand, it provides data that does allow for a certain level of evaluation: quarterly series disaggregated by type of alert, specific training dates with the number of staff trained per session (for example, 37 operators on 01/09/2025, 38 on 01/10/2025, and so on until 02/21/2025, totaling several hundred training sessions), training program content (general system operation, alarm management, beneficiary administration, geofence configuration, MMA device assignment, execution of remote commands, report generation), and a description of improvements implemented after the first year of operation, such as the "reduction of response times through the application of prioritization criteria and immediate attention".

On the other hand, that same information highlights the gaps: while it is reported that there was an "optimization of alarm management" and a "reduction in response times", no specific average times, before-and-after comparison tables, or standardized performance indicators are provided. The protocol stipulates that, upon receiving an alarm, the operator must act "as quickly as possible", but it does not define a numerical standard for response time. Nor does it include, for example, consolidated reports on specific police dispatch times, the percentage of alerts confirmed as true out of the total number received, or comparable indicators across quarters. The mention of "ongoing" training is specified for 2025, but there are no details on what occurred in 2026 or how its impact is assessed.

The case of alarms classified as "false" is particularly illustrative of this asymmetry. The Consortium explains that these arise "primarily as a result of the inherent limitations of geolocation technologies", and that the manufacturer recommends a minimum radius of 40 meters to define the coverage zones. However, under current procedures, the zones are configured "in accordance with the provisions of the relevant judicial orders", even when these may differ from the manufacturer's technical recommendations. This mismatch between recommended technical parameters and judicial parameters actually applied is not publicly discussed in any other institutional document, and helps explain why, out of tens of thousands of recorded alerts, only 5 were considered actual violations of the order during the first quarter of 2026. In other words: the vast majority of the system's alerts are technical noise produced by the very design of the judicial order, and that noise is not publicly reported under comparable indicators, but rather remains as a footnote in a belated response from a private provider.

This gap between surveillance capacity and accountability mechanisms is one of the most significant findings of the research. The system appears to be better equipped to track monitored individuals, movements, and events than to provide robust public indicators regarding its own effectiveness, limitations, and shortcomings. From a critical perspective, this asymmetry is particularly relevant because it shows that the expansion of infrastructure was not accompanied—at least as far as could be ascertained—by a corresponding expansion of democratic transparency.

7.7. From local diagnosis to a comparative perspective: why look at other experiences before making recommendations

The findings presented so far allow us to assess, using our own data and the voices of Paraguayan institutions, how SIMDEC actually operates in its first year of consolidated operation. A consistent picture emerges: a system whose implementation is constrained by physical infrastructure, which generates massive volumes of information without corresponding accountability frameworks, which incorporates victims into the surveillance circuit under the guise of "protection", which relies on a private service provider, and which operates within a landscape of territorial, economic, and digital inequalities that the system itself cannot correct. This empirical evidence, read alongside the previous normative analysis, raises substantive questions about the institutional, material, and human rights governance conditions that the system has yet to resolve.

However, before moving on to specific recommendations, this research considers it necessary to include a section on international comparative analysis. This methodological decision is based on a specific argumentative premise. First, because the legislative background of SIMDEC itself drew on international experience to justify its implementation. If Paraguay invokes external models as a basis for adopting this technology, it makes sense to critically review some of these models in order to assess which promises they fulfilled, which ones failed, and what structural tensions they reproduced.

Second, because several of the issues identified as findings in Paraguay—dependence on electrical infrastructure and connectivity, the massive volume of false alarms, lack of transparency in data governance, the shifting of technical burdens onto victims, reliance on private service providers, and expansion driven by contractual inertia—are local particularities. These are recurring patterns that other countries have already experienced, in some cases for more than a decade. Argentina, Brazil, Uruguay, and Spain offer trajectories with varying degrees of institutional maturity, more consolidated regulatory frameworks, and, even so, documented structural failures that include femicides involving perpetrators under active monitoring, loss of historical data during contractual transitions, judicial dismissals due to evidentiary failures of the tracking devices, and quantitative expansion without evaluation mechanisms. Analyzing these experiences makes it possible to anticipate risks that, in the case of Paraguay, have not yet materialized but are plausible under the same structural conditions.

Third, because making recommendations without this comparative perspective would risk turning into a voluntaristic or merely normative exercise. International evidence provides something that local analysis cannot provide on its own: a longitudinal perspective on how these systems evolve once implemented, which institutional responses have been insufficient, which legal reforms came too late, and what cross-cutting lessons emerge when different States face similar problems under diverse resources and institutional frameworks. To make recommendations without that background would be to recommend blindly. Fourth, because Paraguay is in an early and still malleable phase of implementation. That institutional opportunity is, paradoxically, an analytical advantage: it allows to identify the minimum conditions and safeguards before the system becomes entrenched with its existing fragilities, and to learn from mistakes that other countries have already made and documented. The comparison, then, does not seek to transplant models—a move that the evidence itself advises against—but rather to extract thresholds of institutional viability that allow us to assess how prepared the Paraguayan State is to uphold the technological promise it has adopted.

Finally, the decision to prioritize comparative analysis over recommendations also reflects a methodological choice in this research: to prevent suggestions from appearing as isolated proposals, disconnected from international evidence, or vulnerable to the objection that "it works in other countries". By placing Paraguayan empirical findings in dialogue with comparative experiences, the recommendations formulated in the following section can be grounded both in what is actually happening within Paraguay and in what regional and European evidence has already documented regarding the minimum conditions without which electronic monitoring in contexts of gender-based violence tends to produce inconsistent or even counterproductive results.

With this objective in mind, the following section examines four selected cases: Argentina, Brazil, Uruguay, and Spain, in order to identify conditions for effectiveness, recurrent patterns of failure, and foreseeable structural tensions. The aim is not to present an ideal model, but rather to reconstruct a map of experiences from which to critically assess the possibilities and limitations of Paraguay's SIMDEC.

International comparative analysis: lessons, failures and tensions in comparative perspective

According to the legislative background itself, which drew on international comparisons to justify the need to implement the monitoring system, this comparative analysis aims to identify conditions for effectiveness, recurrent patterns of failure, and structural tensions that are foreseeable when electronic monitoring is introduced into judicial and security systems.

The countries selected for the comparative analysis—Argentina, Brazil, and Uruguay in the regional context, and Spain in the European context—have diverse trajectories in the implementation of electronic monitoring: some with more than a decade of accumulated experience, others with recent deployments and evaluations still in progress[67]. In all cases, the available evidence highlights the gap between the technological promise and the actual institutional capacity to sustain it.

As discussed earlier, both the literature and the available empirical evidence suggest that electronic monitoring does not, in itself, constitute a protective measure. Its effectiveness—in the sense of effectively reducing risk for victims—depends on factors external to the device: the State's operational response, inter-institutional coordination, trained human resources, clear protocols for handling alerts, and governance frameworks for the collected data. Without these conditions, at least as evidenced by international case studies, technology can create a false sense of security rather than providing effective material protection (Erez et al., 2012).

67 The selection of these four countries is based on a combination of methodological criteria. In the case of Argentina, Brazil, and Uruguay, their legal and institutional proximity to Paraguay—that is, their common civil law systems, shared regional frameworks such as the Belém do Pará Convention, and similar structural challenges in terms of State capacity, the digital divide, and gender-based violence—makes their experiences relevant for identifying transferable factors. Uruguay deserves special attention for having served as an explicit reference in the institutional design of SIMDEC, as revealed by the interviews conducted as part of this research. Brazil was also included due to the scale and regulatory density of its system, which allows for a more detailed examination of the effects of rapid expansion. Spain was included because it is the European system that has made the most progress in integrating electronic monitoring and risk assessment for gender-based violence, and because it operates within a framework for data governance. Countries such as Australia and the United Kingdom—which are relevant in the specialized literature—were deliberately excluded because their institutional conditions, legal traditions, and levels of infrastructure development are difficult to compare with Paraguay at this stage of the research. The United States, although a pioneer in the use of GPS in domestic violence, was not included as a comparative case due to its marked decentralization and punitive tradition, although findings from its academic literature are used as theoretical supporting evidence within the conceptual framework.

Argentina: dual devices, procurement and coordination challenges

In Argentina, the electronic monitoring system for cases of gender-based violence was implemented relatively early, with pilot programs in the Autonomous City of Buenos Aires followed by expansion to the provinces. The adopted model prioritizes the so-called "dual device" (Government of Argentina, 2021), which involves the simultaneous use of one device by the perpetrator and another for the victim, allowing for real-time calculation of the distance between the two parties and triggering alerts when the exclusion zone is violated (UNFPA Argentina, 2023).

However, implementation is characterized by a fragmented institutional framework. While the national government is involved in the initial procurement and distribution of the devices, operational management, monitoring, and response protocols fall under provincial jurisdiction. This structure results in a heterogeneous implementation, with significant differences in availability, monitoring capacity, and technical standards across jurisdictions, which hinders both the comparative evaluation of the system and the guarantee of uniform minimum protection standards (UNFPA Argentina, 2023).

At the operational level, the national survey on protection mechanisms identifies structural limitations that affect the system's effectiveness: connectivity issues, signal failures, uneven territorial coverage, and weaknesses in inter-institutional coordination—particularly among law enforcement institutions, the judiciary, and agencies specializing in gender-based violence (UNFPA Argentina, 2023). These conditions directly impact the ability to respond to alerts, particularly in contexts with limited technological infrastructure. The system's effectiveness has also been the subject of public debate. Cases of system breaches have been documented[68], including femicides where the perpetrator was wearing an active monitoring device[69], which prompted protocol revisions[70]. Beyond extreme cases, empirical evidence shows that the use of dual devices does not eliminate the sense of insecurity nor the restrictions on users' daily lives; who continue to bear significant operational and emotional burdens associated with their use (Paz-Ruíz, 2025). The predominant response in public debate has tended to focus on technical improvements and expanded coverage (Sohr, 2019; Carbajal, 2021), while critical perspectives have pointed out that these responses overemphasize the technological dimension at the expense of a comprehensive approach to protection: electronic monitoring can amplify the visibility of risk without guaranteeing its effective reduction.

With regard to the contractual dimension, the decentralization nature of the Argentine system has led to a variety of procurement and management models across jurisdictions, making it difficult to establish uniform standards of control over critical aspects such as interoperability, service continuity, and information security. Public controversies have been documented regarding costs, award conditions, and transparency in the selection of providers (Dolabjian, 2025), demonstrating that the contractual dimension is not neutral: it directly impacts service quality, technological dependence, and the system's sustainability. This dimension is not foreign to the Paraguayan case, where contract awards have also been the subject of public scrutiny, albeit with less visibility (ABC Color, 2024).

---

68 Cadena 3. (2026, March 24). Rauch: A man broke his ankle monitor and kidnapped his former partner. Retrieved April 14, 2026, from https://www.cadena3.com/noticia/sociedad/rauch-un-hombre-rompio-su-tobillera-y-secuestro-a-su-ex-pareja_532837

69 Fahsbender, F. (2025, July 28). Femicide in Berisso: the victim and the perpetrator were both wearing electronic ankle monitors. Infobae. Retrieved April 14, 2026, from https://www.infobae.com/sociedad/policiales/2025/07/27/femicidio-en-berisso-la-victima-y-el-asesino-tenian-tobilleras-electronicas/

70 A prime example is that of Carla Soggiu, who, despite having a panic button as a safety measure, did not receive timely assistance due to failures in the geolocation system, which prevented it from activating properly and contributed to her subsequent murder by her ex-partner. Observatorio Lucía Pérez. (s. f.). Carla Soggiu. Retrieved April 14, 2026, from https://observatorioluciaperez.org/femicidios/carla-soggiu/

Finally, the system generates continuous flows of real-time geolocation data that can accumulate over time and may reveal behavioral patterns (UNFPA Argentina, 2023). Although specific public privacy breaches linked to these systems have not been systematically documented in Argentina, current regulatory standards[71] recognize that this type of information constitutes a highly sensitive category of data, the processing of which requires enhanced safeguards in terms of access, security, and purpose (AAIP, 2021). Institutional fragmentation and the involvement of private providers in the system's operation amplify these risks by hindering the traceability of data use and weakening oversight mechanisms—a risk that increases in the absence of effective auditing regarding who accesses the information, under what conditions, and for what purpose. The Argentine case thus illustrates that the challenges of electronic monitoring are not limited to the effectiveness of the system itself, but extend to the governance of the data it produces.

Brazil: rapid expansion and structural weaknesses

Another relevant regional case to consider is that of Brazil, which has one of the most extensive electronic monitoring systems in the region, covering both the prison system and domestic violence. The scale of the Brazilian system places hundreds of thousands of people under various forms of electronic monitoring (CNJ, 2022). However, this scale coexists with institutional weaknesses that raise questions about the model's actual effectiveness, and the Brazilian government has responded with a regulatory reform process that deserves specific attention.

The Brazilian legal framework, anchored in Law No. 11,340/2006 (known as the Maria da Penha Law[72]), establishes a robust set of protective measures for victims of domestic violence. The reforms introduced by Law No. 13,871/2019 explicitly incorporated electronic monitoring as a precautionary measure applicable to aggressors (Art. 1) but on an optional basis: the judge could order it, but was not required to do so. This approach was progressively modified by two recent reforms that represent a qualitative shift in the Brazilian model.

First, Law No. 5,125/2025 expressly authorized the use of electronic monitoring of the aggressor and the provision of an alert device to the victim in case of improper approach, thereby enhancing the effectiveness of emergency protective measures. Second, the most recent law, Law No. 15,383/2026[73], which establishes electronic monitoring of aggressors as an autonomous protective measure, sets priority criteria for its application, creates a criminal aggravating circumstance for non-compliance with protective measures, and makes the monitoring program permanent (Arts. 1–4). This latest law also introduces a provision of practical relevance for contexts of low judicial institutionality: police officers may order the use of an ankle monitor in localities without a courthouse, with the obligation to notify the judge within 24 hours to confirm or revoke the measure. The decision to use the monitor is immediate when there is a risk to the life or physical or psychological integrity of the woman or her dependents.

---

71 Argentina has Law No. 25,326 on the Protection of Personal Data and, more recently, legislative debates aimed at bringing that framework into line with the standards of the European Union's General Data Protection Regulation (GDPR). This means that, in the context of electronic monitoring, the regulations apply by establishing that geolocation data is sensitive data and that its processing requires specific purposes, a defined retention period, and safeguards against secondary uses (Law 25,326/2000, Articles 2 and 7; AAIP, 2021).

72 This law takes its name from the case of Maria da Penha Maia Fernandes, a victim of domestic violence for more than two decades, which included two attempted murders by her then-husband, leaving her paraplegic. In the absence of an effective response from the Brazilian judicial system, the case was brought before the IACHR, which held the State responsible for omission and tolerance in the face of gender-based violence. This process generated international pressure that led to the adoption of the law in 2006, considered one of the most advanced in the region (Wikipedia. (n.d.). Lei Maria da Penha (Brazil). Retrieved April 14, 2026, from https://es.wikipedia.org/wiki/Ley_Maria_da_Penha_(Brasil)).

73 To access the text of the law, see: Brasil. (2026, abril 9). Lei N.º 15.383, de 9 de abril de 2026. Retrieved April 14, 2026, from https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2026/Lei/L15383.htm

These reforms also include initiatives such as the Projeto Alerta Mulher Segura, promoted by the Ministry of Justice and Public Security (MJSP), and the Pacto Nacional Brasil contra o Feminicídio[74]. In particular, it is worth noting that the Projeto Alerta Mulher Segura reflects a trend toward expanding the use of monitoring technologies, incorporating devices for victims as well—for example, smartwatches capable of issuing real-time alerts when the aggressor is nearby[75]—integrated with electronic ankle monitors and security response systems (Ministério da Justiça e Segurança Pública, 2026). In general terms, these policies suggest that the institutional response has tended to focus on expanding the technological surveillance infrastructure, which raises questions about the balance between technological innovation and the development of comprehensive protection mechanisms.

This updated regulatory framework is clearer than Paraguay's in terms of the protective purpose of the mechanism, its integration with the justice system, and the definition of priority criteria. However, the gap between regulation and practice is an issue that cannot be ignored (Valadão & Freitas Lima, 2025). In this context, the documented failures in the Brazilian system operate on three levels (CNJ, 2023). First, at the technical level: devices with poor battery performance, signal failures in areas with limited coverage, and a lack of adequate maintenance; the report itself notes that many violations recorded as breaches are actually due to technical issues with the device, and that monitoring cannot be implemented throughout the entire territory due to GPS signal limitations (CNJ, 2023, p. 109). Second, at the operational level: monitoring centers with insufficient staff to manage the volume of active cases; at the time of the International Conference, Brazil had 91,362 people under monitoring, and SENAPPEN estimated that more than 1,500 additional professionals were needed for adequate support, while 11 states still lacked multidisciplinary teams (CNJ, 2023, p. 77). Third, at the institutional level: a lack of uniform protocols regarding which entity responds to an alert and within what timeframe; the report documents that each state classifies the same incident in different ways—ranging from approaches that prioritize human rights to more police-oriented approaches—which the system itself identifies as one of its main remaining challenges (CNJ, 2023, p. 77).

However, with regard to this last level, while the literature has identified structural shortcomings in inter-institutional coordination and in the management of alerts, more recent regulatory developments in Brazil have sought to address these shortcomings by strengthening response protocols and more precisely defining the respective responsibilities of the authorities involved, with an emphasis on immediate response to high-risk situations and coordination among judicial, police, and criminal prosecution bodies (Brazil, 2026). However, available evidence suggests that challenges persist in the effective implementation of these mechanisms, especially in contexts of operational limitations and infrastructure inequalities. These shortcomings are also exposed by cases of femicide where the perpetrator was under active monitoring—a documented reality in Brazil that has prompted parliamentary investigations, which invariably conclude that the system is useless without an efficient response mechanism (Brazilian Federal Senate, 2021).

74 These measures must be viewed in light of the scale of the problem, given that, according to data from the Painel de Estatística do Conselho Nacional de Justiça (CNJ), more than 600,000 protective orders were issued in the country in 2025 alone—an average of approximately 70 per hour (MJSP, 2026). However, the high number of orders issued does not automatically translate into effective protection, as high levels of femicide persist—including cases in which the victims had previously been granted protective orders (12.7%)—which highlights limitations in their implementation and enforcement.

75 According to official reports, this project integrates the aggressor's electronic ankle monitor with a digital device—similar to a smartwatch—assigned to the victim. This system enables real-time monitoring and triggers automatic alerts in the event of unauthorized proximity, thereby providing continuous geolocation tracking of the victim. The initiative demonstrates the expansion of the technological surveillance model toward dual-device systems with continuous monitoring.

In this context, the evidence confirms that an ankle monitor alone is not a solution; rather, it requires an efficient and expeditious monitoring and response system. Furthermore, when accompanied by psychological support, legal counseling, follow-up visits, and preventive surveillance, protection becomes substantially more effective. Law No. 15,383/2026 itself implicitly acknowledges this tension by establishing that monitoring should not be considered a standalone or isolated solution, but rather part of a structured protection network that includes legal, psychological, social, and institutional support.

Regarding data governance, Brazil has the Lei Geral de Proteção de Dados (LGPD, Law No. 13,709/2018), a functional equivalent to the European GDPR. The law classifies geolocation data as personal data subject to enhanced protection when it reveals behavioral patterns or allows inferences about private life (LGPD, Art. 5, subsections I and II; Art. 11). In the context of electronic monitoring, the data generated is highly sensitive: it reveals routines, frequented locations, and relational networks, and can be used—in the absence of adequate safeguards—for extrajudicial surveillance, revictimization, or stigmatization of the accused. The LGPD establishes specific legal grounds for data processing by the State, including public interest and security, but requires proportionality and purpose limitation (LGPD, Art. 23).

In this regard, the National Council of Justice, in its Resolution CNJ No. 412/2021[76], further establishes that the data collected through monitoring has a specific purpose and restricted access (Art. 13); furthermore, the systems must preserve the confidentiality of the person being monitored[77], of the woman in situation of violence, and of third parties. The same resolution provides that the sharing of data with public security agencies is subject to judicial authorization (Art. 13, §2), except in exceptional cases involving imminent risk, in which case a formal record of access must be kept for monitoring and potential auditing purposes. It also establishes a data retention period of six months following the termination of the measure, as well as the data subject's right of access to the information generated during the monitoring process (Art. 13). Thus, rather than a regulatory gap in data protection, the challenge in Brazil lies in the effective translation of these rules into uniform institutional practices, particularly in terms of traceability, oversight, and accountability.

Brazil's successive regulatory responses underscore a lesson that cannot be ignored: legislation alone is not enough. Electronic monitoring requires continuous critical evaluation, including systematic data collection and periodic review of its actual impact on the individuals involved. Furthermore, regarding data protection, the Brazilian model is instructive in that data derived from electronic monitoring—particularly real-time geolocation—constitutes particularly sensitive data that requires strict confidentiality safeguards, judicial authorization for access, and traceability of every instance of consultation. This point is particularly relevant, especially when considering implementation schemes involving private providers, the integration of databases among multiple state actors, and contractual arrangements in which personnel from external companies can access the system—thereby increasing the risk of overexposure, technological dependence, and the weakening of public control over information. Paraguay, for example, faces this same scenario under even more precarious institutional conditions.

76 To access the text of the resolution, see: Conselho Nacional de Justiça (Brasil). (2021, August 25). Resolução N.º 412/2021, que dispõe sobre o monitoramento eletrônico de pessoas. Retrieved April 14, 2026, from https://atos.cnj.jus.br/files/original00474820210825612593334b9264.pdf

77 These types of prevention and security considerations address the structural risk of overexposure arising from the circulation of sensitive data among multiple parties. Our research does not indicate that Paraguay has uniform mechanisms in place, such as formal data processing and protection terms, for all operators, which underscores the need for confidentiality and control over access to the information being processed.

Uruguay: a victim-centered model and inter-institutional coordination

Uruguay represents one of the earliest and most systematic examples in Latin America of the implementation of electronic monitoring in cases of gender-based violence. Unlike other countries where these technologies were adapted from the general criminal justice system, the Uruguayan system was developed progressively in coordination with specific public policies on domestic violence, within the framework of the National Plan to Combat Domestic Violence (MIDES, 2010). This approach directly influenced the Paraguayan institutional design. Key actors in the Judiciary have acknowledged that SIMDEC took the Uruguayan model as a reference in its initial conception, although its subsequent regulatory development resulted in a broader framework that was less focused on victim protection (Luraghi Sarubbi, interview, 2026). In this regard, the Uruguayan case is relevant both as a declared reference model and as a mirror in which to observe the gap between the original design and actual implementation.

In operational terms, the Uruguayan system relies on dual devices; that is, an electronic ankle monitor for the aggressor and a GPS device assigned to the victim, allowing for real-time calculation of the distance between the two parties and triggering alerts in the event of violations of the exclusion zone. Admission to the program requires a risk assessment and a prior court order. The Electronic Monitoring Directorate (DIMOE) is responsible for installation, removal, and 24-hour monitoring, in coordination with the Ministry of the Interior's Unified Command Center (CCU) for the management of operational coordination (Ministry of the Interior, Uruguay, 2020). Upon entering the program, both parties sign a contractual agreement regarding the use of the devices and are interviewed about their situation (Ministry of the Interior [Uruguay], n.d.). In effect, this dual model means that the number of people monitored exceeds the number of devices installed, since each case necessarily involves two parties: the aggressor and the victim.

One of its most notable features is the level of inter-institutional coordination[78], with protocols that establish clear responsibilities and information flows between the Judiciary, the Ministry of the Interior, and agencies specializing in gender issues (MIDES, 2019). The protocol of the CCU's Gender-Based Violence Unit also establishes explicit confidentiality obligations: all staff must sign an affidavit regarding the information collected, under express responsibility and with notification of applicable sanctions (Ministry of the Interior [Uruguay], n.d.). Compared to other regional contexts, this structure reduces ambiguity regarding who must act in response to an alert and under what responsibility.

Furthermore, from a formal standpoint, the protocols analyzed and the actions of institutions such as the Ministry of Social Development (MIDES) and the National Institute for Women (Inmujeres) suggest the existence of an approach aimed at integrating electronic monitoring with comprehensive support services. However, the available evidence indicates that the system continues to face structural challenges typical of this type of technology in the region. In particular, while complementary assistance

78 Ministerial Resolution B-1956 (2010) of the Uruguayan Ministry of the Interior established an Inter-institutional Working Commission tasked with studying and advising on the implementation of protection mechanisms for victims of domestic violence, including the evaluation of the use of presence and location verification technologies (electronic ankle monitors). This commission, composed of representatives from the Judiciary, the Bicameral Women's Caucus, the National Institute for Women (Inmujeres/MIDES), and the Uruguayan Network Against Domestic and Sexual Violence, defined the initial framework for the incorporation of electronic monitoring devices and delineated institutional responsibilities.

mechanisms are provided for—such as shelters, psychosocial care, and legal support[79]—this research identified limitations in access to systematized information on how they function in practice, especially regarding response times and outcomes in specific cases, which makes it difficult to assess the extent to which electronic monitoring is effectively integrated with these services.

That said, this entire system, considered a protective measure, has expanded significantly since its initial implementation in 2010. According to indicators presented by the Ministry of the Interior in November 2025, the ankle monitor program—operational nationwide since 2017—recorded an increase of over 1,000% in the number of cases handled, rising from 691 to 3,739 cases. Women account for 9 out of every 10 victims, and the aggressors are 9 out of every 10 men. Between January and October 2025, 817 complaints were filed regarding the removal or destruction of devices, out of which 111 resulted in formal charges or convictions for contempt (Ministry of the Interior, Uruguay, 2025). In other words, this expansion has not been free of tensions.

In fact, on this point, a survey conducted by the Ministry of the Interior itself found that approximately 250 of the 2,100 ankle monitors available for domestic violence cases were being used in a "questionable" manner: cases of people who left the country, others who have been wearing the device for more than two years when the recommendation is not to extend the measure beyond six months, and even people who simultaneously wear two ankle monitors—one as an aggressor and another as a victim, in two separate relationships—(Tapia, 2025). This finding illustrates a recurring problem in the comparative evidence: quantitative expansion is not necessarily accompanied by evaluation and review mechanisms that ensure the relevance of each active case. It should also be noted that this research has not identified, in the available sources, a specific public protocol establishing criteria for categorizing cases according to risk level—high, medium, or low. In practice, this determination appears to fall primarily within the domain of judicial assessment.

Furthermore, this case study also demonstrates that the response to the limitations of the current system is more technology. In late 2025, the Ministry of the Interior introduced Élida 360, a complementary device that operates on the mobile phones of female victims whose aggressors are subject to restraining orders, targeting cases classified as medium or low risk once ankle-monitoring has ended (Ministry of the Interior, Uruguay, 2025). The device, which began as a pilot program in Montevideo with 500 units starting December 22, 2025, requires a prior court order, operates using facial biometrics to ensure exclusive access for the victim, and includes an emergency button, 24-hour chat, and the ability to file a more detailed report without going to the police station (Ministry of the Interior, Uruguay, 2025). The five-year budget allocates an annual budget of 55 million Uruguayan pesos for the leasing of devices starting in 2027, with the intention of adding 1,000 additional units to the 2,300 active devices (Demirdjian, 2025).

79 In the case of Paraguay, the research failed to identify any such provisions in the institutional design of SIMDEC. The only component of the system specifically geared toward victims is the voluntary provision of the MMA device—a mobile phone equipped with the Empower app—which includes a panic button and direct communication with the OMDEC. While the representative of the Judiciary indicated that the State provides the device and data (Luraghi, interview, 2026), the representative of the Ministry of Public Defense noted that, in practice, the victim must maintain an active internet or mobile data connection at all times for the system to function, identifying this as a real economic barrier (Prates, interview, 2026). Upon an alarm, the system's only interaction with the victim consists of contacting her to alert her of the aggressor's proximity and provide "self-protection guidance" (SIMDEC Protocol, 2024). No provisions regarding shelter homes, psychosocial support, independent legal assistance, or economic reintegration linked to the system's operation were identified. The Ministry of Women, the institution with specific jurisdiction over these matters, responded to this research's request for public information with general and institutional information, without providing technical documentation on comprehensive support mechanisms linked to SIMDEC.

The model presented by Élida 360 is significant for comparative analysis, as it is not intended as a revision of the comprehensive protection model, but rather as an additional tool that expands surveillance and the data collected on the victim. The operator now has real-time access not only to the victim's location but also to their personal data, information on the aggressor, and trusted contacts (Ministry of the Interior, Uruguay, 2025). This raises the question of who controls that data and what safeguards remain in place, even within a system with a more robust regulatory framework than Paraguay's.

Finally, regarding data governance, Uruguay has a consolidated regulatory framework for the protection of personal data based on Law No. 18,331 of 2008, regulated by Decree No. 414 of 2009[80], and the activities of the Regulatory and Control Unit for Personal Data (URCDP). However, Article 3 of that law itself excludes from its scope of application databases related to public safety, criminal investigation, and law enforcement, which is directly relevant to electronic monitoring systems.

This exclusion does not imply a lack of regulation, but rather subjection to specific regimes and general principles of fundamental rights protection. In this context, judicial and institutional protocols reinforce the purpose limitation by stipulating that the information generated by the system may only be used in connection with the ordered precautionary measure. Likewise, the inter-institutional nature of the system—which involves not only security authorities but also victim assistance agencies and, potentially, private service providers—raises questions about the differentiated application of data protection standards within the same operational framework. In this regard, while no specific rulings by the URCDP on these systems have been identified, the Uruguayan framework offers robust conditions for institutional structuring that are superior to those observed in the Paraguayan case, where protection standards are still in the process of consolidation.

Spain: systemic failures, governance, and the limits of the technosolutionist approach

Spain is a key reference point in any comparative analysis of technology and gender-based violence, both due to the scale of its system and the tensions generated by its evolution toward predictive and algorithmic models. The Spanish system combines electronic monitoring with a risk assessment and management system called VioGén[81], administered by the Ministry of the Interior (Ministry of the Interior, Spain, 2019).

Electronic monitoring in Spain is implemented through the COMETA system (Control and Observation of Alternative Measures and Sentences), which includes GPS devices for aggressors who have been convicted or are subject to precautionary measures (General Secretariat of Penitentiary Institutions, 2018). Spain has one of the most extensive electronic monitoring systems for gender-based violence in Europe, with thousands of devices active simultaneously. The system operates under the coordination of the National Center for Telematic Monitoring Control (CNCST).

80 To see the text of the Law: Uruguay. (2008). Law No. 18,331 on Personal Data Protection and Habeas Data Action. Retrieved April 18, 2026. https://www.impo.com.uy/bases/leyes/18331-2008

81 VioGén is the Comprehensive Monitoring System for cases of gender-based violence implemented in Spain, which incorporates risk assessment tools—including algorithmic components—for the management and protection of victims. Although it is not directly linked to the electronic monitoring systems analyzed in this study, it constitutes a relevant example of the use of technologies in the prevention of gender-based violence, whose specific dimension regarding artificial intelligence would warrant a separate analysis. Nevertheless, the debate surrounding this technological application must be taken into account because it foreshadows tensions that Paraguay will face if it later incorporates algorithmic risk assessment components into its monitoring protocols.

However, recent evidence from Spain reveals that the problems with electronic monitoring in cases of gender-based violence are not limited to isolated technical failures, but rather reflect structural deficiencies in design, implementation, and governance. Journalistic reports and institutional documentation identify design flaws in the devices, loss of coverage, and a lack of resources, compounded by a poor transition between service providers (RTVE, 2025).

In fact, a particularly critical issue is data management during contractor transitions. The 2023 transition—from Telefónica (with Securitas Direct) to a joint venture between Vodafone and Securitas—resulted in data transfer failures that prevented access to historical geolocation data for several months. According to the Public Prosecutor's Office, this resulted in "potential vulnerability for victims", highlighting that the continuity and traceability of data are central to the system's effectiveness (El País, 2025a). Likewise, it has been documented that these failures have had a direct legal impact, including the dismissal of cases and acquittals of offenders due to the inability to prove violations of restraining orders, revealing a critical interdependence between technology and criminal evidence (El País, 2025b). This goes beyond the technical dimension and positions electronic monitoring as a fragile evidentiary device when data integrity is not guaranteed.

The Spanish institutional response has generally consisted of technical reinforcement and expansion of the system, without a structural review of the underlying logic of the response (Ministry of Equality, 2024; El País, 2025c). However, this approach reproduces a logic of incremental technological correction—that is, "more technology as a solution" (García Arenales, 2026)—without necessarily addressing in a comprehensive manner the underlying problems linked to public procurement (RTVE, 2025; Maldita.es, 2025; RTVE, 2026), interoperability between systems, and data governance. From a comparative perspective, these developments are particularly relevant for Paraguay. The design of the SIMDEC system and the incorporation of monitoring technologies must consider not only the functionality of the device, but also guarantees of data continuity, interoperability standards, and control mechanisms over private providers[82]. The Spanish experience demonstrates that even in contexts with robust regulatory frameworks—such as the GDPR—significant risks persist when the technological infrastructure depends on multiple actors and complex contractual processes.

In this regard, the challenge lies not only in adopting technology, but also in developing a legal and technical framework that ensures the system's reliability, data protection, and the effectiveness of the institutional response. In Paraguay, the SIMDEC system is still in the early stages of implementation, which presents a critical opportunity to discuss these potential risks. Unlike the Spanish case, where failures emerge in a consolidated system, Paraguay faces the challenge of designing, from the outset, mechanisms for data continuity and portability, clear criteria for liability in the event of failures (provider vs. State), minimum standards for infrastructure and coverage, and effective protocols for responding to alerts. If these issues are not addressed, there is a risk of replicating the structural failures observed in Spain, but in a context with fewer institutional capacities.

82 From a comparative perspective, international experience confirms the findings of this research: the effectiveness of electronic monitoring systems depends not only on the functionality of the device, but also on data governance—specifically, data continuity, interoperability between systems, and the existence of effective oversight mechanisms for technology providers.

Cross-cutting lessons for Paraguay: creating conditions for a rights-based system

One of the cross-cutting findings of the comparative analysis is that all the countries examined share a significant commonality: the implementation and effectiveness of the electronic monitoring system depend to a large extent on basic material infrastructure conditions. As in Paraguay, the imposition of the measure is contingent on the technical feasibility of its enforcement, which requires verifying that the user has continuous access to electricity, sufficient connectivity for data transmission, and minimum network coverage conditions. These limitations demonstrate that the implementation of the system is not merely a legal decision, but also an operational issue linked to territorial inequalities and unequal access to basic services.

Another significant point is that all the countries reviewed have regulatory provisions regarding the protection of personal data processed by electronic monitoring systems that are more advanced than Paraguay's. This is not a minor issue, but rather a structurally relevant factor in assessing the risks of the model Paraguay is implementing. The data generated by electronic ankle monitors, applications—such as Empower and Nendive—and alert systems includes real-time geolocation, movement history, contact information, and even potential inferences about behavior and risk levels, and therefore requires specific safeguards.

Without adequate safeguards or controls, they can be exploited to revictimize the protected person, stigmatize the accused before a final conviction, or enable unauthorized secondary uses (Citron & Pasquale, 2014; TEDIC, 2023; UNHCHR, 2021). The comparative analysis confirms that this discussion did not arise in any of the countries examined in advance, but always afterward and generally following incidents. Paraguay has the opportunity and the responsibility to act proactively by taking advantage of the early stage of SIMDEC's implementation.

From the review of the countries used as comparative cases, recurring patterns also emerge that help identify the minimum conditions without which electronic monitoring of gender-based violence produces inconsistent or counterproductive results (Renzema & Mayo-Wilson, 2005; Hucklesby, 2008). These are outlined below not as an ideal model, but as a threshold for institutional viability.

The first condition is the capacity for effective operational response. In all the cases analyzed, the determining factor was not the device itself, but the quality of the State's response to an alert, which requires sufficient staff available 24 hours a day, with clear protocols and genuine inter-institutional coordination (Carter & Grommon, 2016; CNJ, 2022; Ombudsman, Spain, 2019). For Paraguay, the critical question is not how many ankle monitors are installed, but what response capacity exists when an alert is triggered.

The second condition is that electronic monitoring cannot function as an isolated protective measure nor be considered a solution in itself. Comparative evidence consistently highlights the need for a comprehensive protection network: its effectiveness depends on being embedded within a broader institutional framework that includes, among other things, shelter services, psychosocial support, and legal assistance, functioning as a complement to these policies rather than as their substitute (Erez et al., 2012; ANROWS, 2020). Some international experiences have documented risks associated with the expansion of the system without a parallel development of these capacities, even in contexts where such support mechanisms were active at the time the harm occurred. In the case of Paraguay, this research has not yet identified any formally established mechanisms linking SIMDEC to this type of comprehensive support network, beyond the voluntary provision of a mobile phone to the victim in certain cases.

The third condition is data governance with an operational regulatory framework, which includes a general data protection law, an independent supervisory authority, prior impact assessments, purpose limitation, and defined retention periods. In the case of Paraguay, the adoption of Law No. 7593/2025 represents significant progress, but its 24-month transitional period and pending regulations mean that the system will continue to expand for a considerable time under the sectoral and fragmented regime discussed in the previous chapters.

The fourth condition is a mandatory impact assessment, using a publicly disclosed methodology and binding criteria for the renewal of the system. Related to this, the Argentine and Brazilian experiences warn of the risk of expansion driven solely by contractual inertia, whereby payment per active device model generates systemic pressure toward quantitative growth regardless of outcomes (UNFPA Argentina, 2020; CNJ, 2022). In our interviews, a similar tension was identified in the Paraguayan case, associated with the recent availability of 3,000 purchased devices, whose deployment act as an implicit incentive for expansion.

The fifth condition is that the victim should not be held technologically responsible. Spain has documented that when the system fails, the institutional narrative tends to place the burden on the very person who should be protected (Nancarrow & Modini, 2018; Maffei, 2021; Dragiewicz et al., 2018). The design of SIMDEC—which requires the victim to carry the device, maintain an active connection, and trigger alerts—could structurally reproduce this logic, as discussed in the section on empirical findings, if the necessary adjustments are not made.

Paraguay is in the early stages of effective implementation. Although the law dates back to 2017, the implementing decree was not enacted until 2023, the most significant legislative amendment in 2024, and the operational protocols in 2025, meaning that the system has been in operation for barely a year with a regulatory framework that is only minimally consolidated. This relative institutional youth represents a concrete opportunity to incorporate the conditions identified before the system expands with the weaknesses documented by comparative evidence. The question this analysis leaves open is whether the Paraguayan government has the political will and institutional capacity to avoid repeating the same mistakes.

8. RECOMMENDATIONS

The findings of this research suggest that the problem lies not only in the existence of monitoring technologies, but also in the institutional, material, and regulatory conditions under which they are deployed. In Paraguay, SIMDEC is presented as a policy aimed at improving security and reducing prison overcrowding, yet its actual effectiveness depends on a much broader network: police and judicial response capacity, electrical and connectivity infrastructure, coordination with support services, clear rules regarding personal data, public transparency, and mechanisms for democratic oversight. For this reason, the recommendations that follow are not based on an abstract and simplistic opposition to this technology, but rather on a more concrete and politically relevant question: under what conditions, with what limits, and with what safeguards can a tool of this kind operate without increasing the very risks it claims to mitigate.

RECOMENDACIÓN 1. The institutional response as a condition, not a complement

The effectiveness of electronic monitoring does not depend on the device itself, but rather on the actual capacity of the State and its institutions to respond when the device triggers an alert. Detecting that an aggressor has violated an exclusion zone does not protect the victim if there is no sufficient and coordinated police response capacity. Without this provision, the system would be limited to recording the violation without this translating into effective protection.

It is recommended that the expansion of SIMDEC be conditional upon prior verification that such response capacity exists in each jurisdiction where implementation is planned, the establishment of minimum standards for response time to alerts, and the precise definition of which institution assumes operational responsibility at each stage of the process. As long as certain ambiguities in coordination between the Judiciary, the Ministry of the Interior, and the National Police—as documented in this investigation—persist, incorporating more devices without resolving this gap merely expands the promise without increasing actual protection.

RECOMENDACIÓN 2. Integrating SIMDEC into a support network: the device does not resolve what caused the violence

Electronic monitoring is a tool for territorial control, not for relational transformation. On its own, it does not address the social, economic, and relational vulnerabilities underlying gender-based violence, nor does it guarantee that the aggressor disconnects from the dynamics that led to the conflict. For it to produce sustainable results, its use must be combined with complementary professional interventions: psychosocial support for the victim, legal assistance, access to shelters, and, where appropriate, accountability programs for the aggressor that go beyond formal compliance with the measure.

It is recommended that the expansion of SIMDEC be formally articulated with the services of the Ministry of Women and specialized organizations, establishing what kind of support the victim receives from the moment the measure is activated, and not only when an alert is triggered.

RECOMENDACIÓN 3. Continuing training with a rights-based approach for all system operators

The proper functioning of SIMDEC depends not only on the devices working correctly, but also on the people who operate the system—judges, prosecutors, public defenders, OMDEC staff, police officers, and multidisciplinary teams—understanding the multiple implications of the policy they are implementing and acting in accordance with uniform, proportionate criteria that respect the rights of all individuals involved. This research documented that staff training was identified as an area for improvement by the institutions themselves, without clear specification of the content or actual scope of such training.

Continuing training processes must explicitly address the electronic monitoring management policy from a human rights and gender perspective, the ethical handling of personal data generated by the system, criteria to avoid technological victim-blaming, and the understanding that violations recorded by the device do not always reflect voluntary conduct by the monitored person—sometimes they result from technical failures that the system must clearly distinguish before triggering criminal consequences. This is especially relevant for those who apply the measure in on-call hearings without specialization in domestic violence, and for those who operate the monitoring during night shifts or in areas with limited infrastructure.

RECOMENDACIÓN 4. Establish a specific policy on data protection, auditing, and system traceability

One of the most significant shortcomings identified by this research is the absence of sufficiently clear public rules regarding what data is collected, who has access to it, how long they are retained, under what protocols they are shared, and what external oversight mechanism exist over its processing. Opacity in this area is particularly significant because SIMDEC and its associated tools process highly sensitive data: real-time location, addresses, routines, movements, contacts, and critical events involving individuals in situations of violence.

It is recommended that a specific data governance policy be adopted for the system, with differentiated access rules, retention periods, traceability of queries, security protocols, and independent auditing mechanisms. This policy must apply not only to State institutions but also to the contractor involved in the system's operation. Without a clear data protection governance framework, the expansion of electronic monitoring risks consolidating an intensive surveillance infrastructure without equivalent rights-based safeguards.

RECOMENDACIÓN 5. Produce active transparency and comparable public indicators on performance, failures, and outcomes

The research showed that the system appears to be better equipped to track movements, events, and monitored individuals than to publicly account for its own effectiveness, errors, and limitations. It also showed that much of the more detailed information does not come from systematic government publications, but rather from partial, delayed responses—and in some cases, responses mediated by the private provider.

It is recommended to create an active transparency framework with periodic publication of aggregated and comparable data on: the number of active devices, allocation criteria, rejected feasibility reports, installation times, volume and types of alerts, false alarms, police interventions, technical failures, penalties for non-compliance, territorial coverage, and the outcomes of the measures. Publishing more data on installed devices does not equate to publishing better information. Accountability must allow for an assessment of whether the system provides effective protection, where it fails, and what material inequalities it operates upon.

RECOMENDACIÓN 6. Avoid shifting technological responsibilities onto victims and ensure alternatives that do not depend on connectivity

Empirical findings show that part of the promise of protection rests on conditions that fall on the victim themselves: carrying a device, keeping it charged, having connectivity, answering calls, or activating alerts. This distribution of burdens is especially problematic in contexts of territorial inequality, economic precariousness, or technological barriers, as it transforms protection into a daily obligation of technical maintenance.

It is recommended that no protection strategy rely exclusively on material availability, digital literacy, or the victim's immediate reaction. The State must ensure alternatives that do not depend solely on smartphones, mobile data, or a reliable electricity supply, and revise protocols so that any technical failure of the ecosystem does not result in a new burden on the victims already at risk. Technology can support protection, but it must not become a condition for accessing it.

9. FINAL NOTE

In its current state, SIMDEC should not be evaluated solely on the basis of its technological novelty or the number of devices acquired or installed, but rather on its actual ability to ensure comprehensive protection. The main warning that emerges from this research is that a public policy of this kind can quickly become expansive without having yet resolved its minimum conditions for democratic legitimacy: effective coordination, public oversight, clear limits on surveillance, data protection, impact assessment, and a network of care that does not shift the burden onto victims.

If the Paraguayan government decides to maintain and expand this system, it should do so under a basic premise: technology cannot replace comprehensive public policy, much less correct on its own the structural inequalities within which it operates. Only an approach that combines institutional capacity, transparency, care, and human rights will prevent a tool presented as protection from ultimately consolidating new forms of surveillance, opacity, and exclusion.

Statement on the use of Artificial Intelligence tools

In compliance with academic transparency standards, we hereby declare the use of artificial intelligence tools (Claude.AI, NotebookLM, ChatGPT) exclusively for the purposes of style unification, systematization, and bibliographic organization, as well as to assist in the identification of bibliographic sources during the literature review phase. All analytical content, argumentative development, and normative interpretation are the direct intellectual work of the authors.

10. BIBLIOGRAPHY

AAIP – Agencia de Acceso a la Información Pública. (2021). Guía para el tratamiento de datos de geolocalización. AAIP.

ABC Color. (2023, 6 de septiembre). Riera dice que quieren empezar con 100 tobilleras electrónicas antes de fin de año.

ABC Color. (2024, 30 de noviembre). Adjudican a empresa "mimada" la millonaria provisión de tobilleras. Retrieved April 13, 2026, de

ANROWS. (2018). Electronic monitoring in the context of domestic and family violence: Report for the Queensland Department of Justice and Attorney-General.

Belur, J., Thornton, A., Tompson, L., Manning, M., Sidebottom, A., & Bowers, K. (2020). A systematic review of the effectiveness of the electronic monitoring of offenders.

Brasil. (2025). Lei 15.125, de 2025. Autoriza expressamente o uso de monitoramento eletrônico do agressor e o fornecimento de dispositivo de alerta à vítima em caso de aproximação indevida.

Brasil. (2026). Lei 15.383, de 9 de abril de 2026. Estabelece a monitoração eletrônica de agressores como medida protetiva autônoma e os critérios de prioridade para a monitoração eletrônica de agressores.

Carbajal, M. (2021, 1 de marzo). Las tobilleras, una opción desaprovechada en casos de violencia de género. Página/12.

Carter, J. G., & Grommon, E. (2016). Police as alert responders? Lessons learned about perceived roles and responses from pretrial GPS supervision of domestic violence defendants. Policing: A Journal of Policy and Practice, 10(4), 361–377.

CEDAW. (2017). Recomendación general N.º 35 sobre la violencia por razón de género contra la mujer, por la que se actualiza la Recomendación general N.º 19. Naciones Unidas.

Citron, D. K., & Pasquale, F. (2014). The scored society: Due process for automated predictions. Washington Law Review, 89(1), 1–33.

CNN Español. (2019, 1 de marzo). Argentina: Con tobilleras electrónicas para víctimas y victimarios quieren prevenir reincidencia en violencia de género. Retrieved April 13, 2026.

Comisión Interamericana de Derechos Humanos. (2017). Informe sobre medidas dirigidas a reducir el uso de la prisión preventiva (OEA/Ser.L/V/II.163 Doc. 105).

Comisión Nacional de Telecomunicaciones. (2025). Resolución Directorio N.º 0700/2025 por la cual se modifica la Resolución Directorio N.º 2583/2024 sobre la conservación de registros de conexión. Retrieved April 14, 2026

Comité para la Eliminación de la Discriminación contra la Mujer. (1992). Recomendación general N.º 19: La violencia contra la mujer. Naciones Unidas.

Conselho Nacional de Justiça. (2020).Modelos de gestión y monitoreo electrónico. CNJ.

Conselho Nacional de Justiça. (2022). Condiciones institucionales del monitoreo electrónico. CNJ.

Conselho Nacional de Justiça. (2023). Relatório da Conferência Internacional sobre Monitoração Eletrônica: Tecnologia, ética e garantia de direitos. CNJ.

Conselho Nacional de Justiça. (2026, 3 de febrero). CGJ emite recomendação sobre monitoramento eletrônico em casos de violência doméstica. Retrieved April 13, 2026.

Conselho Nacional de Justiça, & Programa de las Naciones Unidas para el Desarrollo. (2017).

Conselho Nacional de Política Criminal e Penitenciária. (2024, 26 de marzo). Recomendação n.º 3, de 26 de março de 2024. Diário Oficial da União.

Consejo de Europa. (2014). Recommendation CM/Rec(2014)4 of the Committee of Ministers to member States on electronic monitoring.

Constitución de la República del Paraguay. (1992).

Corte Suprema de Justicia. (2024). Protocolo del Sistema de Monitoreo por Dispositivos Electrónicos de Control (SIMDEC/OMDEC).

Corte Suprema de Justicia. (2025, 22 de enero). Acordada N.º 1779 por la cual se aprueba el protocolo de aplicación de tobilleras electrónicas: implementación primera fase, propuesto por la Oficina Técnica Penal.

Demirdjian, S. (2025, 1 de septiembre). Presupuesto para violencia de género: creación de dos juzgados especializados, una fiscalía más y un nuevo delito en el Registro de Violadores. la diaria. Retrieved April 18, 2026.

Dolabjian, C. (2025, 27 de abril). Polémica y denuncias por el contrato de tobilleras electrónicas que se encamina a ganar Montoto, por un precio más alto de lo esperado. La Nación. Retrieved April 14 2026.

Dragiewicz, M., Harris, B., Woodlock, D., & Salter, M. (2018). Technology-facilitated coercive control. Feminist Media Studies, 18(4), 609–625.

El País. (2022, 10 de abril). Pascual, M. G., & Valdés, I. VioGén: Visita a las tripas del algoritmo que calcula el riesgo de que una mujer sufra violencia machista. Retrieved April 14, 2026.

El País. (2025a, 19 de septiembre). Los fallos en las pulseras antimaltrato exponen las grietas de un sistema vital para la protección de las víctimas de violencia machista. Retrieved April 14, 2026.

El País. (2025b, 17 de septiembre). Fallos en el sistema de las pulseras antimaltrato han provocado una gran cantidad de sobreseimientos y absoluciones de agresores. Retrieved April 14, 2026.

El País. (2025c, 17 de septiembre). Igualdad cambia las pulseras telemáticas por tobilleras para evitar su manipulación. Retrieved April 14, 2026.

Erez, E., Ibarra, P. R., & Lurie, N. A. (2012). GPS monitoring technologies and domestic violence: An evaluation study. National Institute of Justice.

Erez, E., & Ibarra, P. R. (2007). Making your home a shelter: Electronic monitoring and victim re-entry in domestic violence cases. British Journal of Criminology, 47(1), 100–120.

Eubanks, V. (2018). Automating inequality: How high-tech tools profile, police, and punish the poor. Picador.

García Arenales, M. (2026, 27 de enero). Igualdad cambia las pulseras telemáticas para agresores por tobilleras para evitar su manipulación. Infobae. Retrieved April 18, 2026.

Gies, S., Gainey, R., Cohen, M., Healy, E., Duplantier, D., Yeide, M., Bekelman, A., Bobnis, A., & Hopps, M. (2012). Monitoring high-risk sex offenders with GPS technology: An evaluation of the California Supervision Program, final report. National Institute of Justice.

Gobierno de Argentina. (2021). Dispositivos duales, una herramienta contra la violencia de género. Retrieved April 13, 2026.

Gordo, Á., & Rubio-Martín, M. J. (2024). Incertidumbres algorítmicas en torno a las violencias de género. El caso del sistema VioGén y otros sistemas de predicción del riesgo. Revista Española de Sociología, 33(2).

Hucklesby, A. (2008). Vehicles of desistance? The impact of electronically monitored curfew orders. Criminology & Criminal Justice, 8(1), 51–71.

Ibarra, P. R., Gur, O. M., & Erez, E. (2023). Mismatches and criminal justice policy: The case of GPS for domestic violence. Criminology & Criminal Justice, 24(4).

La Nación. (2024, 12 de junio). Tobilleras electrónicas: Estado absorberá gastos en caso de insolvencia del procesado. Retrieved April 13, 2026.

Maldita.es. (2025, 23 de septiembre). Qué sabemos sobre los fallos de las pulseras telemáticas antimaltrato y la pérdida de datos de órdenes de alejamiento. Retrieved April 18, 2026.

Ministerio de Desarrollo Social (Uruguay). (2010, 25 de noviembre). Plan nacional de lucha contra la violencia doméstica. Retrieved April 18, 2026.

Ministerio de Desarrollo Social (Uruguay). (2019). Protocolo de actuación en situaciones de violencia basada en género. Retrieved April 18, 2026.

Ministerio de Igualdad (España). (2024). Protocolo de actuación en el sistema de seguimiento por medios telemáticos en casos de violencia de género. Retrieved April 14, 2026.

Ministerio de Justicia (Paraguay). (s. f.). Autoridades ponen en vigencia el uso de tobilleras electrónicas.

Ministerio de la Mujer (Paraguay). (2016). Ley N.º 5777/2016 de protección integral a las mujeres contra toda forma de violencia.

Ministerio del Interior (Paraguay), Corte Suprema de Justicia, Ministerio Público, Ministerio de Justicia, & Policía Nacional. (2024). Reglamento orgánico / protocolo de implementación de dispositivos electrónicos de control.

Ministerio del Interior (Uruguay). (s. f.). Protocolo área violencia de género: Centro de Comando Unificado. Retrieved April 18, 2026.

Ministerio del Interior (Uruguay). (2025, 21 de noviembre). El Ministerio del Interior presentó los principales indicadores de violencia doméstica y de género. Retrieved April 18, 2026.

Ministério da Justiça e Segurança Pública (Brasil). (2026, 9 de abril). Governo federal sanciona leis de enfrentamento à violência contra a mulher. Retrieved April 14, 2026.

Ministério da Justiça e Segurança Pública (Brasil). (2026, 17 de abril). [Publicación en Instagram sobre el Projeto Alerta Mulher Segura]. Instagram. Retrieved April 18, 2026.

Morozov, E. (2013). To save everything, click here: The folly of technological solutionism. PublicAffairs.

Naciones Unidas. (1948). Declaración Universal de Derechos Humanos.

Naciones Unidas. (1966a). Pacto Internacional de Derechos Civiles y Políticos.

Naciones Unidas. (1966b). Pacto Internacional de Derechos Económicos, Sociales.

Naciones Unidas. (2006). Estudio a fondo sobre todas las formas de violencia contra la mujer: Informe del Secretario General (A/61/122/Add.1).

Natarajan, M. (2016). Police response to domestic violence: A case study of TecSOS mobile phone use in the London Metropolitan Police Service. Policing, 10(4), 378–390.

National Institute of Justice. (2012). Monitoreo GPS en violencia doméstica y brechas de conectividad.

O'Neil, C. (2016). Weapons of math destruction: How big data increases inequality and threatens democracy. Crown.

OMDEC. (2024). Formulario de factibilidad técnica / documentación operativa del SIMDEC.

Organización de los Estados Americanos. (1994). Convención Interamericana para prevenir, sancionar y erradicar la violencia contra la mujer (Convención de Belém do Pará).

Organización de los Estados Americanos. (2017). Informe sobre medidas dirigidas a reducir el uso de la prisión preventiva. CIDH/OEA.

Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos. (2021).

Oficina de las Naciones Unidas contra la Droga y el Delito. (2007). Handbook of basic principles and promising practices on alternatives to imprisonment.

Padgett, K., Bales, W., & Blomberg, T. (2006). Under surveillance: An empirical test of the effectiveness and consequences of electronic monitoring. Criminology & Public Policy, 5, 61–91.

Paladines, J. (2019). Implementación latinoamericana del monitoreo electrónico.

Paraguay. (1992). Ley N.º 1/1992 por la cual se aprueba y ratifica la Convención Americana sobre Derechos Humanos (Pacto de San José de Costa Rica, 1969).

Paraguay. (2016). Ley N.º 5777/2016 de protección integral a las mujeres contra toda forma de violencia.

Paraguay. (2017). Ley N.º 5863/2017 que crea el Sistema de Monitoreo por Dispositivos Electrónicos de Control (SIMDEC).

Paraguay. (2020). Ley N.º 6568/2020 que modifica la Ley N.º 1600/2000 contra la violencia doméstica.

Paraguay. (2023). Decreto N.º 466/2023 por el cual se reglamenta el SIMDEC.

Paraguay. (2024). Ley N.º 7270/2024 que modifica y amplía el régimen del SIMDEC.

Paraguay. (2024). Pliego de bases y condiciones para la contratación del servicio integral de monitoreo electrónico(PBC, 2024).

Paraguay. (2025). Ley N.º 7549/2025 que dispone la obligatoriedad de la conservación de datos para combatir la pornografía relativa a niños y adolescentes y hechos punibles conexos. Retrieved April 14, 2026.

Pascual, M. G., & Valdés, I. (2022, 10 de abril). VioGén: Visita a las tripas del algoritmo que calcula el riesgo de que una mujer sufra violencia machista. El País. Retrieved April 14, 2026.

Paz-Ruiz, D. S. (2025). Protección y violencia de género: experiencia de un grupo de usuarias de dispositivos duales en Córdoba, Argentina. Prospectiva. Revista de Trabajo Social e Intervención Social, (40).

Poder Judicial (Paraguay). (2017). Fuente citada sobre la creación del SIMDEC; vinculada a la Ley 5863/2017.

Poder Judicial (Paraguay). (2025, 24 de enero). Corte Suprema aprueba Acordada N.º 1779 sobre tobillera electrónica.

Poder Judicial (Uruguay). (2012). Circular N.º 158/2012: Protocolo de actuación para la implementación de tecnología de verificación de presencia y localización de personas en caso de alto riesgo en violencia doméstica (Anexo Acordada N.º 7755). Retrieved April 18, 2026.

Presidencia de la República (Uruguay). (2025, 22 de octubre). Aplicación digital brindará respuesta a mujeres víctimas de violencia con medidas cautelares de no acercamiento. Retrieved April 18, 2026.

Presidencia de la República (Uruguay). (2025, 21 de noviembre). Dispositivo de seguridad que complementa tobilleras electrónicas estará operativo a fines de diciembre. Retrieved April 18, 2026.

Principios Internacionales sobre la Aplicación de los Derechos Humanos a la Vigilancia de las Comunicaciones. (2013). Principios necesarios y proporcionales.

Protocolo de San Salvador. (1999). Protocolo adicional a la Convención Americana sobre Derechos Humanos en materia de derechos económicos, sociales y culturales.

Reglamento General de Protección de Datos. (2016). Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016. Diario Oficial de la Unión Europea, L 119.

Renzema, M., & Mayo-Wilson, E. (2005). Can electronic monitoring reduce crime for moderate to high-risk offenders?Journal of Experimental Criminology, 1, 215–237.

Rolls, E., Youle, Y., & Hartwright, C. (2024). Electronic monitoring of domestic abuse perpetrators on licence: Process evaluation. Ministry of Justice. Retrieved April 14, 2026.

RTVE. (2025, 11 de noviembre). Igualdad revisa el protocolo de protección de víctimas de violencia machista tras incidentes en el sistema de pulseras. Retrieved April 14, 2026.

RTVE. (2026, 27 de enero). El Gobierno sustituye pulseras electrónicas por tobilleras tras fallos del año pasado. Retrieved April 14, 2026.

Secretaría General de Instituciones Penitenciarias (España). (2018). Sistema COMETA / seguimiento por medios telemáticos.

Sohr, O. (2019, 8 de marzo). Se usan menos de 500 tobilleras electrónicas de Nación en casos de violencia de género. Chequeado. Retrieved April 14, 2026.

Subrayado. (2025, 20 de septiembre). El control de la tobillera electrónica: relato de los miedos de una víctima y la incertidumbre del después.

Tapia, C. (2024, 26 de mayo). Interior alerta por mal uso de tobilleras electrónicas: indagados que se fueron del país y otros que tienen dos dispositivos. El País Uruguay. Retrieved April 18, 2026.

Sequera y García (2021) Explorando la violencia digital de género en Paraguay. TEDIC

TEDIC. (2023, 18 de octubre). Tobilleras electrónicas: ¿Más seguridad o una herramienta para la vigilancia?

Sequera y Cuevas (2024) Violencia de género facilitada por la tecnología a mujeres políticas en Paraguay. TEDIC

UNFPA Argentina. (2023). Relevamiento del funcionamiento de los dispositivos de protección ante emergencias por violencias de género.

UOL Notícias. (2026, 23 de marzo). Relógio alertará vítimas de violência doméstica de aproximação do agressor. Retrieved April 14, 2026.

Virtua Barcelona. (2025, 24 de noviembre). VioGén 2: La IA que decide quién vive o muere en violencia machista. Retrieved April 14, 2026.


Technology
& Human
Rights