INVESTIGACIÓN SOBRE TOBILLERAS ELECTRÓNICAS EN PARAGUAY

Tecnología & Derechos Humanos

TEDIC

INVESTIGACIÓN SOBRE TOBILLERAS ELECTRÓNICAS EN PARAGUAY

Tecnología & Derechos Humanos

La presente publicación ha sido financiada por la Unión Europea.
Su contenido es responsabilidad exclusiva de TEDIC y no refleja necesariamente los puntos de vista de la Unión Europea.

Este material forma parte del proyecto **Informadas y Resilientes**, que busca reducir desigualdades y promover los derechos humanos en Paraguay, combatiendo la desinformación y la violencia digital.

Financiado por la Unión Europea

CON EL APOYO DE

La gente cambia el mundo Diakonia

Tecnología & Derechos Humanos TEDIC

TEDIC es una Organización No Gubernamental fundada en el año 2012, cuya misión es la defensa y promoción de los derechos humanos en el entorno digital. Entre sus principales temas de interés están la libertad de expresión, la privacidad, el acceso al conocimiento y género en Internet.

INVESTIGACIÓN SOBRE TOBILLERAS ELECTRÓNICAS EN PARAGUAY

ABRIL 2026

COORDINACIÓN Y EDICIÓN
Maricarmen Sequera

INVESTIGACIÓN
Antonia Bogado
Araceli Ramírez

ASISTENCIA
Maricel Achucarro

COMUNICACIÓN
Camila Rolón

DISEÑO Y DIAGRAMACIÓN
Horacio Oteiza

Esta obra está disponible bajo licencia Creative Commons Attribution 4.0 Internacional (CC BY SA 4.0)
https://creativecommons.org/licenses/by-sa/4.0/deed.es

ISBN 978-99989-999-1-6

TABLA DE CONTENIDO

1. PRESENTACIÓN DEL PROBLEMA 6

2. OBJETIVO DE LA INVESTIGACIÓN 7

2.1. Objetivo general 7

2.2. Objetivos específicos 7

2.3. Preguntas de investigación 8

3. METODOLOGÍA 9

4. INTRODUCCIÓN 11

5. ENTRE LA PROMESA TECNOLÓGICA Y LA REALIDAD ESTRUCTURAL 12

5.1. La violencia de género como fenómeno estructural 13

6. TOBILLERAS ELECTRÓNICAS: GENEALOGÍA DE UNA TECNOLOGÍA AMBIVALENTE 14

6.1. De experimento conductual a política penal masiva 14

6.2. La llegada a América Latina: entre la modernización y la precariedad 14

6.3. El giro hacia la violencia de género: ¿protección o expansión del control? 15

6.4. Tecnologías para víctimas: riesgo de revictimización y responsabilización tecnológica 15

6.5. Tecnología, vigilancia y efectividad: por qué el dispositivo no garantiza seguridad 16
¿Qué es una tobillera electrónica y cómo funciona en Paraguay? 17
La tobillera como parte de un entramado institucional 18
El inicio del circuito: decisión judicial y factibilidad técnica 20
La instalación: activación del dispositivo y configuración de zonas 20
El monitoreo permanente: avisos, advertencias y alarmas 21
¿Qué pasa si el agresor se acerca o viola la restricción? 22
La respuesta en calle: Policía, 911 y apoyo táctico 22
El "dispositivo para la víctima" dentro del protocolo SIMDEC 23
Nendive: una herramienta distinta, pero parte del mismo ecosistema 23

6.6. Un sistema que produce datos, responsabilidades y zonas grises 24
Ecosistema tecnológico de respuesta a violencia de género en Paraguay 25

7. HACIA UN ANÁLISIS LEGAL 26

7.1. Marco normativo paraguayo: qué habilita el Estado y qué exige el derecho 26
Marco internacional de derechos humanos: obligaciones vinculantes del Estado paraguayo 26

7.2. Base constitucional del SIMDEC 29

7.3. Arquitectura legal del SIMDEC: del diseño normativo a los protocolos de operación 30

7.4. Leyes sustantivas de violencia de género 33

7.5. El régimen de datos personales: la privacidad como derecho subordinado al discurso de la seguridad 34

7.6. Hallazgos empíricos: implementación, transparencia y tensiones institucionales 40
La implementación real del sistema está fuertemente condicionada por la infraestructura material 41
Una implementación gradual atravesada por límites materiales y económicos 42
La prevención como posible circuito de vigilancia 44
La incorporación de las víctimas dentro del circuito de vigilancia 45
La desigualdad en la transparencia estatal 46
La debilidad del debate sobre privacidad, tratamiento de datos y auditoría 47
El sistema está diseñado para registrar pero no para rendir cuentas con el mismo nivel de intensidad 48

7.7. Del diagnóstico local a la perspectiva comparada: por qué mirar otras experiencias antes de recomendar 49
Análisis comparado internacional: lecciones, fallas y tensiones en perspectiva comparada. 50
Argentina: dispositivos duales, adquisiciones y desafíos de coordinación 51
Brasil: expansión acelerada y fragilidades estructurales 52
Uruguay: modelo orientado a víctimas y coordinación interinstitucional 55
España: fallas sistémicas, gobernanza y límites del enfoque tecnosolucionista 57
Lecciones transversales para Paraguay: crear condiciones para un sistema con enfoque de derechos 59

8. RECOMENDACIONES 61

9. NOTA FINAL 64

10. BIBLIOGRAFÍA 65

1. PRESENTACIÓN DEL PROBLEMA

En Paraguay, el crecimiento del debate público sobre la violencia de género convive con una respuesta estatal que, cada vez más, incorpora soluciones tecnológicas como parte de sus herramientas de prevención o protección. Entre ellas, las tobilleras electrónicas aplicadas a personas agresoras y distintas formas de soporte tecnológico dirigido a víctimas, incluyendo apps, botones de pánico, líneas de emergencia, sistemas de alerta.

Estas medidas suelen presentarse como herramientas "neutras" y "modernizadoras", asociadas a la idea de mejor control y mayor seguridad. Sin embargo, desde una perspectiva de derechos humanos, y especialmente desde una mirada feminista, es fundamental discutir la pregunta que frecuentemente queda fuera del diseño institucional: ¿qué tipo de seguridad se está construyendo y a costa de qué derechos?

El problema no es la existencia de herramientas tecnológicas en sí, sino el modo en que se insertan en el sistema de justicia y de seguridad pública. La tecnología puede convertirse en un sustituto de la política pública integral, una respuesta visible frente a la presión pública, o incluso una forma de expandir el control estatal sin rendición de cuentas suficiente. La tensión más delicada aparece cuando la "prevención" se apoya en mecanismos de vigilancia y rastreo, por ejemplo, geolocalización, que implican tratamiento de datos altamente sensibles, y que pueden amplificar riesgos de exposición, filtración, abuso, error operativo o revictimización.

Este estudio parte de una hipótesis central: las tecnologías de prevención de violencia de género no deben evaluarse solo por su promesa de seguridad, sino por su funcionamiento real, sus condiciones materiales de implementación, su gobernanza, el rol de las instituciones involucradas y sus efectos diferenciados sobre mujeres y cuerpos disidentes. Dicho de otro modo: la pregunta no es únicamente "funciona o no funciona", sino "qué produce, para quién, con qué costos y quién lo controla".

2. OBJETIVO DE LA INVESTIGACIÓN

2.1. Objetivo general

Analizar críticamente el uso de tobilleras electrónicas y otras tecnologías aplicadas a la prevención de la violencia de género en Paraguay, describiendo su marco normativo, su implementación práctica, su gobernanza institucional, las adquisiciones públicas asociadas y sus implicancias en la tensión entre seguridad, privacidad y derechos humanos, con énfasis en los derechos de mujeres y cuerpos disidentes.

2.2. Objetivos específicos

- Reconstruir el marco legal vigente que habilita y regula el uso de tobilleras electrónicas (SIMDEC) y tecnologías asociadas para la prevención de violencia de género, identificando obligaciones estatales, vacíos normativos y contradicciones internas.
- Describir el proceso institucional real de implementación: cómo se solicita, ordena, instala, monitorea, responde y registra una medida tecnológica (tobillera, app, botón o alerta).
- Sistematizar adquisiciones y contrataciones públicas vinculadas a tobilleras electrónicas y servicios de monitoreo, identificando modelo de contratación, costos, proveedores, capacidad instalada y reglas de operación.
- Relevar y analizar información pública disponible (Portal AIP) y evaluar el nivel de transparencia estatal, detectando patrones de respuesta, opacidad o ausencia de datos.
- Producir evidencia cualitativa mediante entrevistas con al menos 3 autoridades clave, para comprender criterios de decisión, capacidades operativas, fallas y tensiones interinstitucionales.
- Incorporar análisis comparado internacional, para anticipar escenarios de expansión de vigilancia, riesgos, condiciones mínimas de eficacia y oportunidades de incidencia.
- Elaborar recomendaciones concretas para incidencia estatal, orientadas a garantizar derechos, límites, transparencia, enfoque de género e institucionalidad efectiva de respuesta y cuidado.

2.3. Preguntas de investigación

Para que la investigación sea útil a la incidencia pública la organizamos alrededor de preguntas que vayan más allá del "sí/no" de la eficacia:

- ¿Qué se entiende por "prevención" dentro del Estado paraguayo cuando se adopta una tecnología? ¿Es prevención, es control, es gestión de riesgo, es respuesta?
- ¿Qué datos se recolectan y procesan con tobilleras, apps o sistemas de alerta? ¿Quién accede a esa información y bajo qué reglas?
- ¿Qué garantías existen para evitar usos secundarios, filtraciones o accesos indebidos?
- ¿Cómo se implementa en la práctica: qué pasa cuando hay una alerta, qué institución responde, con qué tiempos, con qué recursos, y qué ocurre si falla el sistema.
- ¿Cómo se reparte la carga del cuidado? ¿Estas tecnologías protegen o desplazan la responsabilidad hacia las víctimas (tener celular, cargar batería, estar conectadas, reportar, etc.)?
- ¿Qué modelo de compras/servicio se adoptó y qué dependencia tecnológica genera (proveedores, licencias, mantenimiento, monitoreo 24/7, infraestructura)?
- ¿Qué impactos diferenciados se producen sobre mujeres, personas LGBTIQ+, población rural, personas sin conectividad o sin alfabetización digital?
- ¿Qué aprendemos de experiencias internacionales (España, Australia, Estados Unidos, Argentina) sobre límites, fallas y condiciones de efectividad?

Estas preguntas buscan sostener un análisis que no se quede en la novedad tecnológica, sino que discuta el núcleo político: la vigilancia como forma de producir seguridad.

3. METODOLOGÍA

Esta investigación se inscribe en un enfoque cualitativo de carácter exploratorio, con orientación crítico-interpretativa y perspectiva de derechos humanos, privacidad y género. El interés no estuvo puesto en medir estadísticamente la eficacia del monitoreo electrónico, sino en comprender cómo se configura en la práctica una política tecnológica de prevención y respuesta frente a la violencia de género, qué racionalidades institucionales la sostienen, qué condiciones materiales requiere para operar y qué tensiones produce en la intersección entre seguridad, vigilancia y protección de derechos.

Desde esa perspectiva, el estudio se organizó como un estudio de caso ampliado sobre el ecosistema institucional y tecnológico desplegado en Paraguay en torno al Sistema de Monitoreo por Dispositivos Electrónicos de Control (SIMDEC) y otras herramientas asociadas, como aplicaciones, sistemas de alerta y canales de activación institucional. La elección de este diseño respondió a la necesidad de analizar no solo un dispositivo aislado, sino el entramado normativo, operativo y político que lo vuelve posible: las reglas que lo habilitan, las instituciones que lo implementan, las infraestructuras de las que depende, los actores que toman decisiones y las formas concretas en que se distribuyen responsabilidades, riesgos y cargas de cuidado.

El análisis combinó distintas estrategias de producción y contraste de información. En primer lugar, se realizó una revisión documental y normativa orientada a reconstruir el marco jurídico y operativo del sistema. Esto incluyó leyes, decretos, acordadas, protocolos, formularios, documentos técnicos y materiales institucionales vinculados tanto al funcionamiento del SIMDEC como a otras tecnologías estatales de respuesta frente a la violencia de género. Esta revisión permitió identificar qué prescribe formalmente el sistema, cuáles son sus fundamentos legales, qué obligaciones atribuye a cada actor y qué vacíos o zonas grises persisten en materia de implementación, coordinación y garantías.

En segundo lugar, se trabajó con solicitudes de acceso a la información pública como herramienta central para aproximarse al funcionamiento real del sistema. A través de estas solicitudes se buscaron datos sobre capacidades institucionales, procesos de monitoreo, criterios de factibilidad técnica, cobertura territorial, compras públicas, contratos, reglas de operación, métricas disponibles, tratamiento de datos y mecanismos de respuesta. Esta dimensión fue clave para contrastar el diseño formal con la práctica efectiva, así como para identificar opacidades, ausencias de información y dependencias institucionales o proveedoras que no siempre aparecen explicitadas en la normativa.

En tercer lugar, se realizaron entrevistas semiestructuradas a autoridades e informantes clave vinculados con el diseño, la implementación o la operación del sistema. Estas entrevistas permitieron reconstruir criterios de decisión, dificultades cotidianas, tensiones interinstitucionales y modos concretos de interpretar la idea de “prevención” dentro del Estado. Más que relevar opiniones aisladas, el objetivo fue acceder a las racionalidades institucionales que organizan la política tecnológica: cómo se justifican ciertas decisiones, qué problemas se consideran prioritarios, qué límites se reconocen y cómo se distribuyen en la práctica las funciones de control, respuesta y cuidado.

Como complemento, el estudio incorporó una dimensión de análisis comparado internacional. Esta comparación no tuvo por objeto equiparar mecánicamente experiencias nacionales diferentes, sino situar el caso paraguayo dentro de una discusión más amplia sobre monitoreo electrónico, vigilancia y violencia de género. La revisión de antecedentes de otros países permitió identificar patrones recurrentes, riesgos ya documentados, condiciones mínimas de funcionamiento y debates normativos relevantes para interpretar el caso local con mayor densidad analítica.

La estrategia metodológica fue, por tanto, de triangulación. El análisis se construyó a partir del cruce entre lo normativamente prescripto, lo administrativamente documentable y lo institucionalmente narrado por los propios actores involucrados. Esta triangulación permitió no limitar la investigación a la letra de las normas ni a la promesa tecnológica del dispositivo, sino examinar el ensamblaje concreto que sostiene la política pública. En otras palabras, el estudio buscó observar simultáneamente qué dice el sistema que hace, qué información pública permite verificar y cómo describen su funcionamiento quienes participan de él.

4. INTRODUCCIÓN

En diciembre de 2024, Paraguay dio un paso significativo en su política de seguridad pública con la implementación efectiva del Sistema de Monitoreo por Dispositivos Electrónicos de Control (SIMDEC)[1]. Las primeras tobilleras electrónicas[2] comenzaron a colocarse[3] en agresores denunciados por violencia doméstica, marcando el inicio de lo que las autoridades presentaron como una modernización del sistema de justicia y una respuesta "innovadora" a la crisis de violencia de género que atraviesa el país. Sin embargo, desde TEDIC se considera fundamental interrogar esta narrativa de progreso tecnológico y examinar críticamente qué tipo de seguridad se está construyendo, para quién, y a qué costo en términos de derechos humanos.

La urgencia del problema es innegable. Según datos del Ministerio de la Mujer, Paraguay registró 36 feminicidios en 2023[4], mientras que el Poder Judicial reportó más de 31.000 denuncias por violencia doméstica en el mismo período. Estas cifras, que apenas logran captar la superficie de un fenómeno profundamente arraigado en problemas estructurales más profundos, generan una presión social y política comprensible por respuestas efectivas. Es en este contexto de crisis donde emerge la tobillera electrónica y otras medidas tecnológicas como soluciones aparentemente rápidas y visibles, alimentando lo que Evgeny Morozov (2013) denomina "solucionismo tecnológico": la creencia de que los problemas sociales complejos pueden resolverse mediante la aplicación de tecnología, sin abordar sus causas estructurales.

Esta investigación se propone explorar el despliegue de tobilleras electrónicas y otras alternativas tecnológicas en Paraguay y a nivel internacional, no desde una posición tecnofóbica, sino desde una perspectiva de derechos digitales que reconoce tanto el potencial como los riesgos de estas tecnologías cuando se insertan en sistemas de justicia y seguridad. Partimos de la premisa de que la tecnología nunca es neutral: está situada en redes de poder, que reproducen las lógicas del sistema que la implementa y puede tanto proteger como vulnerar derechos, dependiendo de su diseño, gobernanza y condiciones de implementación.

---

1 Protocolo de implementación disponible en la página web del Poder Judicial de Paraguay. Recuperado de: https://www.pj.gov.py/images/contenido/otp/Dispositivos-electronicos/4%20PROTOCOLO%20DEL%20SIMDEC%2030_12_2024.pdf

2 A lo largo de este trabajo se utilizan los términos SIMDEC (Sistema de Monitoreo por Dispositivos Electrónicos de Control), sistema de monitoreo electrónico y tobilleras electrónicas de manera indistinta, siguiendo el uso extendido en el debate público y en buena parte de los documentos institucionales relevados. Sin embargo, conviene precisar que, en sentido estricto, estos términos no son equivalentes. La tobillera electrónica designa el dispositivo de hardware —el brazalete físico que porta el imputado— mientras que el SIMDEC es el sistema integral en el que ese dispositivo opera: incluye la plataforma de monitoreo, las aplicaciones de interacción con la víctima, el centro de control y la infraestructura de comunicaciones. El propio Protocolo SIMDEC/OMDEC (2024) distingue ambos planos al definir el "dispositivo electrónico de control" como la "tecnología utilizada por el SIMDEC para el monitoreo e interacción con el usuario y la víctima en su caso" (art. 5, lit. b). El uso indistinto de los términos en este estudio responde a razones de legibilidad y no implica desconocer esa distinción conceptual.

3 Tobilleras electrónicas se usarán en casos de violencia familiar en Asunción. Noticia disponible en página web del diario ABC Color, Paraguay.

4 Leer más en: https://mujer.gov.py/el-ano-2023-cierra-con-45-feminicidios-en-paraguay/

5. ENTRE LA PROMESA TECNOLÓGICA Y LA REALIDAD ESTRUCTURAL

La incorporación de tobilleras electrónicas en Paraguay no puede leerse como la simple llegada de un dispositivo técnico al sistema judicial. Lo que está en juego es la instalación de una infraestructura estatal de vigilancia que se presenta, entre otras, como respuesta frente a la violencia de género, pero que al mismo tiempo reorganiza relaciones entre castigo, cuidado, control y gestión del riesgo. Por eso, en este estudio exploratorio no interesa solamente preguntar si "la tobillera y otros dispositivos tecnológicos funcionan", sino qué tipo de protección prometen, qué condiciones institucionales necesitan para operar y qué efectos producen sobre derechos, responsabilidades y formas de intervención estatal. El propio Protocolo del Sistema de Monitoreo por Dispositivos Electrónicos de Control (SIMDEC) confirma esta mirada: define el sistema no como un aparato aislado, sino como un "conjunto de recursos, procesos, procedimientos y acciones" que incluye factibilidad técnica, monitoreo, advertencias, alarmas, coordinación y respuesta policial. (CSJ, 2024)

En Paraguay, además, las tobilleras fueron justificadas públicamente a partir de un triple encuadre[5] político. Por un lado, como herramienta para prevenir hechos de violencia familiar y feminicidios; por otro, como parte de una agenda de modernización institucional del Poder Judicial, el Ministerio del Interior y el Ministerio de Justicia; y, al mismo tiempo, como mecanismo para descomprimir cárceles, abaratar costos y fortalecer el control de medidas alternativas al encierro. Ese triple discurso aparece tanto en la normativa como en la cobertura de medios como ABC Color[6] y Última Hora[7], donde el monitoreo electrónico es presentado de manera simultánea como protección, eficiencia, innovación y ahorro. Precisamente por eso, este estudio parte de una premisa crítica: cuando una misma tecnología se ofrece al mismo tiempo como solución humanitaria, herramienta de seguridad y medida de gestión penal, es necesario examinar con cuidado qué racionalidad estatal está organizando su uso y qué problemas quedan desplazados del debate público. (ABC Color, 2024; Última Hora, 2024; CSJ, 2025).

La trayectoria del SIMDEC muestra que no se trata de una medida repentina ni neutra. La Ley 5863, de 2017, creó la base legal del sistema; el Decreto 466, de 2023[8], reglamentó su implementación; la Ley 7270, de 2024[9], modificó y amplió ese régimen; y desde fines de 2024 y durante 2025 se aprobaron protocolos y acordadas[10] para su despliegue gradual, primero en Asunción y luego con ampliaciones posteriores. Esa secuencia revela algo más que una evolución técnica, muestra la consolidación progresiva de una política pública de vigilancia que pasó de una promesa normativa a una operación efectiva, aún con grandes procesos en definición. (Poder Judicial, 2017; Poder Judicial, 2023; Poder Judicial, 2024; CSJ, 2025).

A esto se suma una dimensión que no debería quedar fuera del marco introductorio: la economía política del monitoreo. La prensa paraguaya documentó que la implementación estuvo atravesada por debates

5 Corte Suprema aprueba la acordada número 1779 sobre tobilleras electrónicas. Noticia disponible en página web del Poder Judicial de Paraguay.

6 Tobilleras electrónicas se utilizarán en casos de violencia familiar en Asunción. Noticia disponible en página web de diario ABC Color, Paraguay.

7 Gobierno lanza el sistema de monitoreo para las tobilleras electrónicas. Noticia disponible en página web del diario Última Hora, Paraguay.

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

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

10 Ver acordadas y protocolos en: https://www.pj.gov.py/contenido/2695-observatorio-de-la-oficina-tecnica-penal-otp/3241

sobre costos[11], financiamiento, proveedor y contratación pública. ABC Color informó que la licitación para provisión y monitoreo de tobilleras alcanzó un monto máximo de más de G. 81.000 millones[12], y que el costo mensual por dispositivo rondaría los G. 2.000.000 o más, a cargo del beneficiario salvo declaración de insolvencia. No se trata de un detalle administrativo menor. En tecnologías de vigilancia, la infraestructura contractual también es parte de la infraestructura de poder: determina dependencias técnicas, posibles opacidades, márgenes de auditoría y condiciones reales de funcionamiento. En otras palabras, la protección tecnológica también se define en los pliegos, en los contratos y en las cajas negras proveedoras. (ABC Color, 2024).

5.1. La violencia de género como fenómeno estructural

Para comprender las implicaciones del uso de tobilleras electrónicas y otros dispositivos tecnológicos en casos de violencia de género, es necesario partir de una conceptualización que reconozca la naturaleza estructural y sistémica de esta violencia. Como establece la Convención de Belém do Pará (1994), ratificada por Paraguay, la violencia contra la mujer es "cualquier acción o conducta, basada en su género, que cause muerte, daño o sufrimiento físico, sexual o psicológico a la mujer, tanto en el ámbito público como en el privado"[13]. Esta definición, adoptada también en la Ley 5777/2016 de Protección Integral a las Mujeres contra toda forma de Violencia[14], reconoce que la violencia de género no es un conjunto de incidentes aislados, sino una manifestación de relaciones de poder históricamente desiguales entre hombres y mujeres. (OEA, 1994; Ministerio de la Mujer, 2016).

TEDIC ha venido documentando cómo esta violencia estructural se manifiesta y amplifica en el espacio digital[15] (TEDIC, 2022 y 2024). La violencia de género facilitada por la tecnología (VGFT) no es un fenómeno separado de la violencia "offline", sino parte de un continuo que atraviesa todos los espacios donde las mujeres desarrollan sus vidas. Como señaló en su investigación sobre violencia digital contra mujeres políticas en Paraguay (TEDIC, 2024), la VGFT incluye "todo acto cometido, asistido, agravado o amplificado por el uso de tecnologías de la información y comunicación u otros medios digitales, que cause o pueda causar daño físico, sexual, psicológico, social, político o económico, y que se base en el género" (TEDIC, 2024). Esta definición es clave para este estudio porque impide pensar la tecnología solo como un canal neutral de protección: las mismas capacidades técnicas que permiten alertar, rastrear o geolocalizar también pueden ser usadas para vigilar, controlar y violentar. (TEDIC, 2024; ONU, 2023).

Esta comprensión del continuo online/offline es central para analizar las tobilleras electrónicas y otras soluciones tecnológicas, porque estos dispositivos operan precisamente en la intersección entre lo digital y lo físico. Son objetos materiales que producen datos, dependen de redes de telecomunicaciones, sistemas informáticos, geolocalización, bases de datos, protocolos de respuesta y decisiones humanas. La vigilancia, en este marco, no existe solo en Internet: se despliega como una infraestructura híbrida que atraviesa la vivienda, la calle, el trabajo, el teléfono, la oficina judicial, el centro de monitoreo y la intervención policial. Evaluar estas tecnologías exige mirar a la vez el dispositivo y el ecosistema que lo sostiene. (TEDIC, 2024; CSJ, 2024).

---

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

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

13 Organización de Estados Americanos. (1994). *Convención Interamericana para Prevenir, Sancionar y Erradicar la Violencia contra la Mujer "Convención de Belém do Pará"*. Recuperado de https://www.oas.org/juridico/spanish/tratados/a-61.html

14 República del Paraguay. (2016). Ley N° 5777/2016 de Protección Integral a las Mujeres contra toda forma de Violencia.

15 Violencia de género facilitada por la tecnología contra mujeres políticas en Paraguay TEDIC. (2024).

6. TOBILLERAS ELECTRÓNICAS: GENEALOGÍA DE UNA TECNOLOGÍA AMBIVALENTE

6.1. De experimento conductual a política penal masiva

La historia del monitoreo electrónico revela las tensiones inherentes a esta tecnología. Los primeros experimentos datan de la década de 1960 en Estados Unidos, cuando los hermanos Ralph y Robert Schwitzgebel desarrollaron en Harvard dispositivos de radio-telemetría para monitorear a personas en libertad condicional[16]. Estos primeros prototipos estaban imbuidos del espíritu del conductismo de la época: la idea de que el comportamiento criminal podía ser modificado mediante intervenciones tecnológicas de supervisión y refuerzo.

Sin embargo, la adopción masiva del monitoreo electrónico no ocurrió hasta la década de 1980, en un contexto muy diferente. Como documenta Mike Nellis (2013) en su historia comprehensiva del monitoreo electrónico, la expansión de estas tecnologías coincidió con la crisis del sistema penitenciario estadounidense: sobrepoblación carcelaria, costos crecientes y presión política por alternativas[17]. El monitoreo electrónico se presentó entonces no tanto como herramienta de rehabilitación, sino como solución pragmática a problemas de gestión penal.

Esta genealogía importa porque permite ver la ambivalencia política de la tobillera. En la literatura internacional, el monitoreo electrónico suele aparecer asociado a medidas alternativas al encarcelamiento. La Oficina de las Naciones Unidas contra la Droga y el Delito (UNODC) lo ubica dentro del repertorio de alternativas a la privación de libertad; al mismo tiempo, la evidencia comparada y las recomendaciones del Consejo de Europa advierten que su uso puede derivar en *net-widening*, es decir, en la ampliación del control penal hacia personas y espacios que antes no estaban sometidos a esa supervisión. El propio Consejo de Europa recomienda especial cuidado en etapas previas al juicio para evitar esa expansión y exige proporcionalidad en duración e intrusividad. En otras palabras: una medida presentada como menos dañina[18] que la cárcel también puede funcionar como una extensión de la lógica carcelaria hacia el hogar, el territorio y la vida cotidiana. (UNODC, 2007; Consejo de Europa, 2014).

6.2. La llegada a América Latina: entre la modernización y la precariedad

En América Latina, la adopción del monitoreo electrónico comenzó en la década de 2000, impulsada por una combinación de factores: crisis penitenciarias endémicas, presión de organismos internacionales por "modernizar" los sistemas de justicia, y la disponibilidad de tecnología más accesible. Brasil fue pionero en la región, seguido por Argentina, Chile y Colombia. Sin embargo, como señala Paladines (2019) en su análisis regional, la implementación latinoamericana ha estado marcada por la improvisación, la falta de evaluación sistemática y la ausencia de debate público sobre sus implicaciones[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.

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 llegó relativamente tarde a esta tendencia. La Ley 5863 que crea el SIMDEC data de 2017[20], pero su implementación efectiva no comenzó hasta finales de 2024. Este retraso, lejos de ser una desventaja, ofrecía la oportunidad de aprender de las experiencias regionales y evitar sus errores. Sin embargo, la evidencia disponible a lo largo de este estudio exploratorio sugiere que el despliegue paraguayo está reproduciendo patrones problemáticos observados en otros países: énfasis en la adquisición tecnológica sobre la construcción de capacidades institucionales, falta de transparencia en las contrataciones, y ausencia de mecanismos de evaluación y rendición de cuentas.

6.3. El giro hacia la violencia de género: ¿protección o expansión del control?

La aplicación de tobilleras electrónicas específicamente en casos de violencia de género representa un giro importante en la historia de esta tecnología. Ya no se trata solo de controlar arrestos domiciliarios o de administrar medidas alternativas a la prisión, sino de prometer protección a víctimas mediante la vigilancia del agresor, la geolocalización y la activación temprana de alertas. La comparación internacional[21] muestra que este desplazamiento desde un monitoreo centrado en el infractor hacia esquemas orientados también a la víctima no es neutro: reordena el sentido político del dispositivo y amplía su legitimidad social. Experiencias comparadas en Argentina, España e Inglaterra muestran justamente esa transición hacia modelos de *"victim-oriented monitoring"*, en los que la protección pasa a depender de infraestructuras de rastreo, exclusión territorial y respuesta institucional. (Paterson, 2015; Ministerio de Igualdad de España, s/f).

En el contexto paraguayo, este giro se inscribe en un ecosistema más amplio de soluciones tecnológicas para víctimas. Ya existían herramientas como la app Nendive del Poder Judicial, lanzada en 2021 para denuncias de violencia doméstica en Central, con georreferenciación y botón de pánico, y la línea 137 "SOS Mujer", que funciona con cobertura nacional y articulación interinstitucional. La llegada de las tobilleras no inaugura, por tanto, la relación entre género, seguridad y tecnología, sino que profundiza una tendencia estatal previa: responder a una problemática estructural mediante dispositivos de alerta, registro y reacción. El problema no es que existan herramientas técnicas, sino que estas terminen sustituyendo el debate sobre políticas integrales de prevención, acompañamiento y reparación. (Poder Judicial, 2021; Ministerio de la Mujer, s/f).

6.4. Tecnologías para víctimas: riesgo de revictimización y responsabilización tecnológica

Este punto se vuelve aún más delicado cuando la protección depende materialmente de la víctima o del entorno doméstico. La cobertura sobre el SIMDEC en Paraguay indicó que, en casos de violencia familiar, la víctima puede recibir un celular o una aplicación vinculada al sistema[22], mientras que el dispositivo del agresor tiene una batería de 48 a 72 horas cuya carga queda bajo responsabilidad del portador. A esto se suma que la factibilidad técnica[23] depende de condiciones concretas como dirección georreferenciada, señal y suministro regular de energía eléctrica. Desde una perspectiva feminista y de derechos humanos, estas condiciones no son detalles operativos: muestran cómo la política de protección puede

20 República del Paraguay. (2017). *Ley N° 5863/2017 que establece la implementación de dispositivos electrónicos de control de personas procesadas o condenadas*. 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

22 Gobierno lanza el sistema de monitoreo para las tobilleras electrónicas: ¿Cuánto cuestan y cómo funcionarán?. Noticia accedida a través de la página web del diario Última Hora.

23 Las tobilleras electrónicas ya se usarán en casos de violencia familiar: ¿Cómo funcionarán?. Noticia accedida a través de la página web del diario Última Hora.

derivar en una forma de responsabilización tecnológica, en la que la seguridad se vuelve dependiente de la conectividad, la batería, la infraestructura del domicilio y la capacidad de activar alertas. Si algo falla, el riesgo es que la carga vuelva a recaer sobre quienes ya estaban expuestas a la violencia. (Última Hora, 2024; CSJ, 2024; ABC Color, 2024).

La literatura sobre violencia facilitada por la tecnología en relaciones íntimas[24] ayuda a profundizar esta preocupación. Las revisiones recientes[25] muestran que la violencia interpersonal hoy incluye formas de rastreo, acoso, vigilancia y control mediante dispositivos digitales, redes y sistemas de localización. Esto obliga a desconfiar de cualquier respuesta que suponga que más tecnología equivale automáticamente a más protección. Una política tecnológica orientada a víctimas debe evitar reproducir, por otros medios, las mismas lógicas de vigilancia y control que caracterizan muchas situaciones de violencia. Dicho de otro modo: la protección tecnológica no puede convertirse en una extensión tecnificada del mismo problema que dice atender. (Rogers et al., 2022; TEDIC, 2024).

6.5. Tecnología, vigilancia y efectividad: por qué el dispositivo no garantiza seguridad

La evidencia comparada sobre monitoreo electrónico coincide en el siguiente punto: la tecnología no garantiza resultados por sí sola. La revisión sistemática de Belur y colegas (Belur et al., 2020)[26] muestra efectos heterogéneos sobre reincidencia y subraya que los resultados dependen de mecanismos, contextos y condiciones institucionales específicas. A este respecto, en Estados Unidos, el Instituto Nacional de Justicia (NIJ) evaluó programas de monitoreo GPS en violencia doméstica y encontró resultados mixtos: la reducción de reincidencia solo se observó cuando el dispositivo se combinó con supervisión activa y protocolos de respuesta rápida (Padgett et al., 2006; NIJ, 2012). Carter y Grommon (2016) documentaron que los agentes policiales frecuentemente no tenían claridad sobre sus roles ante una alerta y que existía confusión sobre si el sistema operaba como prevención o como control, un indicador de que la tecnología fue incorporada sin rediseño institucional previo.

En la misma línea, el Consejo de Europa[27] advierte no solo sobre el riesgo de *net-widening*, sino también sobre la necesidad de que el monitoreo, cuando forme parte de una supervisión, se combine con otras intervenciones y no se convierta en una medida autónoma desligada de apoyos institucionales. Esta advertencia es especialmente importante para el caso paraguayo: en un contexto de violencia de género, la vigilancia del agresor no reemplaza refugios, atención psicosocial, patrocinio jurídico, medidas de reparación, redes comunitarias ni capacidad estatal efectiva de respuesta. (Consejo de Europa, 2014).

En Paraguay, además, la efectividad del sistema está atravesada por desigualdades materiales y territoriales. El propio protocolo exige estudios de factibilidad técnica[28] y formularios con geolocalización precisa, número de casa, datos de la víctima y confirmación de suministro regular de energía eléctrica. Al mismo tiempo, el Instituto Nacional de Estadísticas (INE) reportó[29] que en 2024 el uso de internet alcanzó 81,6 % de la población de 10 años y más, con una brecha importante entre áreas urbanas (86,2 %)

---

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 *Violencia de género facilitada por la tecnología* (TEDIC;2023). Accedido el 20 de marzo de 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

27 Consejo de Europa. (2014). *Recomendación CM/Rec (2014/4) del Comité de Ministros a los Estados miembros sobre monitoreo electrónico.* Consejo de Europa.

28 Formulario de Factibilidad SIMDEC: Poder Judicial Paraguay. (2024). *Formulario de factibilidad técnica - Sistema de Monitoreo por Dispositivos Electrónicos de Control (SIMDEC)*. Oficina Técnica Penal. Disponible en la página web del Poder Judicial de Paraguay.

29 Noticia disponible en el portal del Instituto Nacional de Estadística (INE) sobre uso de internet: Instituto Nacional de Estadística (INE). (2024, marzo). *8 de cada 10 personas utiliza internet en Paraguay.*

y rurales (73,7 %), además de limitaciones de cobertura en ciertos territorios y poblaciones[30]. Aunque la tobillera no dependa siempre del smartphone de la víctima, el ecosistema de alertas, contacto, respuesta y monitoreo sí presupone infraestructura material y conectividad. Por eso, la vigilancia tecnológica tampoco opera sobre una superficie homogénea: produce segmentaciones y exclusiones que deben ser analizadas desde el inicio. (CSJ, 2024; INE, 2025). Esta advertencia no es novedosa: las evaluaciones del Instituto Nacional de Justicia (NIJ; 2012) en Estados Unidos documentaron patrones similares: comunidades rurales con conectividad deficiente, víctimas sin información sobre el funcionamiento del sistema, poblaciones en situación de vulnerabilidad estructural para quienes el modelo de protección tecnológica opera de forma deficiente. Esto sugiere que estas brechas no son contingencias locales sino condicionantes estructurales recurrentes de los sistemas de monitoreo electrónico.

Con este marco conceptual, la pregunta que abre esta investigación puede formularse con mayor precisión: cuando el Estado paraguayo adopta tobilleras electrónicas[31] y otras soluciones tecnológicas como respuesta frente a la violencia de género, ¿qué entiende por prevención y qué régimen de vigilancia, cuidado y responsabilidad está construyendo en la práctica? Nuestra hipótesis es que el tecnosolucionismo (Morozov, 2013)[32] puede operar como un atajo institucional[33]: ofrece una respuesta rápida y visible en un contexto de urgencia, pero corre el riesgo de omitir análisis de impacto, consulta a personas expertas en tecnología y derechos humanos, evaluación pública, transparencia contractual y fortalecimiento de políticas integrales[34]. Por eso, el análisis que sigue en esta investigación no se detendrá en la promesa del dispositivo, sino en el ensamblaje normativo, institucional y material que lo sostiene: primero, desde la lectura legal y de derechos humanos; luego, desde las entrevistas y la reconstrucción de su funcionamiento real. (TEDIC, 2023; OHCHR, s/f; Morozov, 2013).

¿Qué es una tobillera electrónica y cómo funciona en Paraguay?

Antes de profundizar en sus implicancias jurídicas, políticas y sociales, es importante detenernos en una pregunta básica: ¿qué es exactamente una tobillera electrónica? En términos generales, se trata de un dispositivo de monitoreo corporal que se coloca en el tobillo —o, en ciertos diseños, en el brazo— de una persona y que forma parte de un sistema más amplio de vigilancia remota. No es solamente un brazalete físico. Su funcionamiento depende de una combinación de hardware, software, geolocalización, transmisión continua de datos, conectividad móvil, soporte técnico y una central de monitoreo encargada de interpretar eventos y activar respuestas. La literatura y los modelos de gestión regional[35] sobre monitoreo electrónico describen estas tecnologías como ensamblajes sociotécnicos que combinan un dispositivo en el cuerpo, una plataforma de seguimiento y reglas institucionales para definir áreas permitidas, áreas prohibidas y respuestas frente a incumplimientos. (CNJ-PNUD, 2017; CNJ, 2020).

---

30 Informe TICs 2024: Instituto Nacional de Estadística (INE). (2024). Encuesta Permanente de Hogares Continua 2023: Tecnologías de la Información y Comunicación (TIC).

31 Tobilleras electrónicas: ¿más seguridad o una herramienta para la vigilancia?, artículo de TEDIC sobre tobilleras electrónicas: (TEDIC; 2023).

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

33 Un ejemplo paradigmático es la extensión del GPS pre-trial en Estados Unidos como medida de liberación anticipada, que se expandió sin evaluar previamente la capacidad operativa de respuesta, convirtiendo al dispositivo en un sustituto de la decisión cautelar en lugar de un complemento de la protección (Gies et al., 2013).

34 Pacto Internacional de Derechos Civiles y Políticos: Naciones Unidas. (1966). *Pacto Internacional de Derechos Civiles y Políticos.* Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos.

35 MJSP. (2017). *A implementação da política de monitoração eletrônica de pessoas no Brasil.* Departamento Penitenciário Nacional. Consultado el 14 de marzo de 2026.

En el caso paraguayo, además, el pliego de bases y condiciones[36] confirma que el Estado no contrató un "aparato" aislado, sino un servicio integral bajo demanda que incluye dispositivos, software de gestión y monitoreo, infraestructura para la Oficina de Monitoreo de Dispositivos Electrónicos de Control (OMDEC), adecuación edilicia, personal de apoyo permanente, soporte técnico y mantenimiento del sistema en su conjunto. (PBC, 2024; CSJ, 2024).

Dicho de otro modo, una tobillera electrónica no protege por sí sola. Lo que hace es producir información sobre ubicación, trayectorias, proximidades y transgresiones, y traducir esa información en eventos que deben ser procesados por instituciones humanas. Por eso, más que hablar de un aparato aislado, conviene hablar de una infraestructura de monitoreo. Esta precisión es especialmente relevante para Paraguay, donde tanto el Protocolo del Sistema de Monitoreo por Dispositivos Electrónicos de Control (SIMDEC) como el pliego técnico[37] muestran que el sistema fue pensado como un ensamblaje de monitoreo, reacción e infraestructura. El propio pliego establece que los componentes mínimos del dispositivo electrónico de control son el Transmisor —la tobillera o brazalete colocada sobre el cuerpo—, la Unidad de Base Residencial (UBR) —instalada de forma fija en el domicilio de la persona portadora de la tobillera cuando la señal GPS del transmisor resulte insuficiente— y la Unidad de Monitoreo Ambulatorio (UMA), diseñada para recibir alertas por cercanía entre víctima y agresor y transmitir datos al software de monitoreo mediante red celular 3G o superior. (PBC, 2024; CSJ, 2024). El propio Protocolo define al Sistema de Monitoreo por Dispositivos Electrónicos de Control (SIMDEC) como un "conjunto de recursos, procesos, procedimientos y acciones" orientados al monitoreo efectivo de los regímenes de control previstos por la ley. Desde el inicio, entonces, la normativa paraguaya reconoce que no está regulando solo un objeto técnico, sino una red institucional y operativa más amplia. (CSJ, 2024).

La tobillera como parte de un entramado institucional

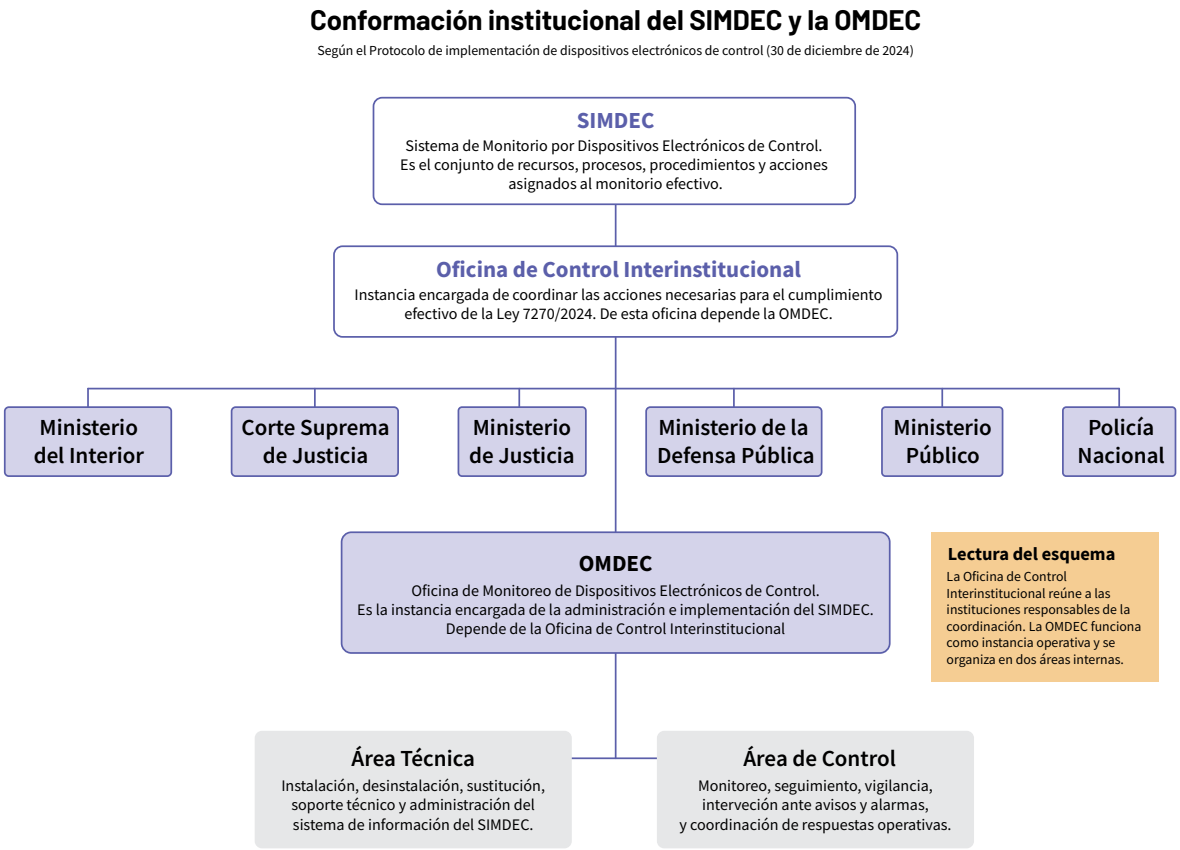
En Paraguay, el funcionamiento de las tobilleras no recae únicamente en el Poder Judicial. El reglamento orgánico del SIMDEC[38] distribuye funciones entre varias instituciones. La Oficina de Control Interinstitucional está integrada, entre otras, por la Corte Suprema de Justicia, el Ministerio Público, el Ministerio del Interior, el Ministerio de Justicia, y la Policía Nacional. Dentro de este esquema, la Oficina de Monitoreo de Dispositivos Electrónicos de Control (OMDEC) aparece como la instancia del Ministerio del Interior encargada de la administración e implementación del SIMDEC. A su vez, la OMDEC depende de la Oficina de Control Interinstitucional y cuenta con un Área Técnica y un Área de Control. El reglamento también establece que la jefatura de coordinación de la OMDEC está representada por el jefe del Departamento de Dispositivos Electrónicos de Control de la Dirección General del Sistema 911 del Ministerio del Interior. (Ministerio del Interior et al., 2024).

36 Pliego de bases y condiciones de adquisición de dispositivos de monitoreo electrónico. Recuperado del portal de contratacionesl del Gobierno paraguayo.

37 Ibidem.

38 Poder Judicial Paraguay. (2024). *Reglamento del Sistema de Monitoreo por Dispositivos Electrónicos de Control (SIMDEC)*. Oficina Técnica Penal. Consultado el 14 de marzo de 2026.

Conformación institucional del SIMDEC y la OMDEC



Fuente: elaboración propia a partir del Protocolo de Implementación de Dispositivos Electrónicos de Control, arts. 1, 2, 5, 6, 8, 11 y 12.

Este punto importa porque muestra que el uso de tobilleras en Paraguay no debe pensarse únicamente como una decisión judicial[39], sino como un circuito interinstitucional de vigilancia, registro, comunicación y reacción. El juzgado solicita o dispone la medida, pero la implementación efectiva involucra a OMDEC, al Sistema 911, a la Policía Nacional, a comisarías jurisdiccionales y, en determinados casos, a la Dirección de Operaciones Tácticas Motorizadas LINCE. La "eficacia" del sistema, por tanto, no depende exclusivamente de que el dispositivo funcione, sino de que toda esa red institucional funcione de manera coordinada y sostenida. (Ministerio del Interior et al., 2024; CSJ, 2024).

39 Ibidem.

- **Actores del sistema y sus roles principales**

PODER JUDICIAL	OMDEC / SIMDEC	EMPRESA PROVEEDORA	POLICÍA / 911 / LINCE	PERSONAS VÍCTIMA Y USUARIAS
▪ Juzgado ordena la medida ▪ Evaluación de presupuestos legales previa ▪ Autoriza o deniega ▪ Comunica cese de la medida	▪ Recibe oficio ▪ Evalúa factibilidad ▪ Instala y monitorea ▪ Opera alertas	▪ Provee hardware ▪ Mantiene software ▪ Almacena datos ▪ Soporte técnico	▪ Recibe activación ▪ Despacha móviles ▪ Intervención en terreno ▪ Registro del cierre	▪ Acepta/rechaza UMA ▪ Cumple condiciones tanto legales como de infraestructura ▪ Porta dispositivo ▪ Carga batería/ datos

Fuente: Elaboración propia con base en Protocolo SIMDEC/OMDEC (CSJ, 2024); Decreto N.º 466/2023.

El inicio del circuito: decisión judicial y factibilidad técnica

Según el Protocolo SIMDEC/OMDEC, la tobillera no se instala automáticamente. Antes, el juzgado debe solicitar a la OMDEC un informe de factibilidad técnica. Esa solicitud debe incluir, entre otros elementos, la identificación de la persona a monitorear, la individualización de la causa y los datos necesarios para ubicar el área de inclusión —es decir, el espacio geográfico en el que la persona debe permanecer— y/o el área de exclusión —el espacio al que tiene prohibido ingresar—. El protocolo agrega un dato particularmente relevante para los casos de alejamiento: cuando la medida legal se trate de una orden de alejamiento, el área de exclusión "será aquella que indique la víctima". (CSJ, 2024).

El formulario oficial de factibilidad permite ver con más detalle qué información requiere el sistema para funcionar. Allí se piden dirección, número de casa, ciudad, barrio, geolocalización en latitud, longitud y altitud, foto de fachada de la vivienda, número de celular del dueño de casa, número de celular de la víctima, radio de alejamiento delimitado en metros y confirmación de suministro regular de energía eléctrica. Incluso aparece la categoría de "canon" y la distinción entre gratuidad, onerosidad o insolvencia. Esto muestra que el dispositivo no se monta sobre un vacío: exige una serie de condiciones técnicas, habitacionales y administrativas previas. (OMDEC, 2024). El protocolo también prevé un punto de decisión que no es menor: si en el momento de la solicitud no existen dispositivos disponibles, la OMDEC debe informar esa situación al juez solicitante, sin necesidad de realizar el estudio de factibilidad. Es decir, la disponibilidad material de equipos condiciona desde el inicio el acceso a la medida. (CSJ, 2024).

La instalación: activación del dispositivo y configuración de zonas

Si existe factibilidad técnica y el juzgado ordena la instalación, el oficio judicial es remitido dentro de la OMDEC al Área de Control y al Área Técnica, que deben coordinar la instalación efectiva del dispositivo. El personal técnico instala y activa la tobillera, mientras que el Área de Control determina y configura en el sistema informático las áreas de inclusión y exclusión correspondientes. Luego, ya en el lugar definido judicialmente, ambas áreas coordinan el geoposicionamiento y la visualización en pantalla del sistema de monitoreo para constatar la ubicación del dispositivo "en tiempo real". Una vez realizados esos ajustes, el rastreo y control permanente quedan a cargo del Área de Control. (CSJ, 2024).

Este punto permite comprender por qué la tobillera no puede reducirse a un grillete digital. Su funcionamiento depende de la traducción de una decisión judicial en parámetros técnicos concretos: metros de alejamiento, zonas cargadas en el sistema, coordenadas, mapas, visualización en tiempo real y criterios operativos de monitoreo. La medida judicial se vuelve técnicamente operativa solo cuando ingresa a ese sistema de configuración y control. (CSJ, 2024; CNJ, 2020).

El monitoreo permanente: avisos, advertencias y alarmas

Una vez activado el dispositivo, el Área de Control de la OMDEC asume la tarea de monitoreo[40], seguimiento y vigilancia permanente a través del software del sistema. El Protocolo[41] clasifica los eventos que pueden producirse en tres grandes categorías. La primera son los avisos, vinculados a incidencias técnicas que afectan el funcionamiento del dispositivo o la pérdida de cobertura del sistema de localización. La segunda son las advertencias disuasivas, que se activan cuando la persona monitoreada se aproxima a un área de exclusión o sale del área de inclusión. La tercera son las alarmas de reacción inmediata, que obligan a ejecutar acciones preventivas urgentes y a comunicar el hecho a la autoridad competente. (CSJ, 2024).

La distinción entre estas categorías no es meramente técnica. Organiza distintos niveles de intervención estatal. Un aviso supone, en principio, una incidencia que puede requerir contacto con la persona usuaria y restauración del servicio; una advertencia disuasiva supone que ya existe un desplazamiento problemático en relación con la medida judicial; y una alarma de reacción inmediata indica una situación que debe activar mecanismos operativos más severos. En ese pasaje se ve con claridad cómo una variación de ubicación se transforma en una cadena de decisiones institucionales. (CSJ, 2024).

- **Flujo de respuesta ante eventos y alertas del sistema**

AVISO	ADVERTENCIA DISUASIVA	ALARMA DE ACTIVACIÓN INMEDIATA
Incidencia técnica que puede afectar el funcionamiento o la localización ■ Batería crítica del dispositivo ■ Pérdida de señal GPS o cobertura ■ Falla de comunicación con la central ■ → Operador contacta al usuario para restaurar el servicio ■ → Si no se resuelve, se escala a supervisión técnica	*La persona usuaria se aproxima a zona prohibida o abandona zona permitida* ■ Sistema detecta acercamiento al área de exclusión ■ Operador realiza advertencia imperativa a la persona usuaria ■ Se realizan hasta 3 persuasiones sucesivas ■ SIMULTÁNEO en casos de VG: operador llama a la víctima para alertarla y conocer su ubicación ■ Si no acata → escala a Alarma de Reacción Inmediata	*Violación de perímetro o manipulación del dispositivo* ■ Violación del área de exclusión consumada ■ Salida del área de inclusión sin acatamiento ■ Manipulación o daño del dispositivo ■ Operador verifica posición georreferencial en tiempo real ■ Activa respuesta policial por canal de radio operativo ■ Contacta a la víctima (UMA) para orientaciones de autoprotección

Fuente: Elaboración propia - Art 8, Decreto N.° 466/2023

40 Poder Judicial Paraguay. (2024). *Reglamento del Sistema de Monitoreo por Dispositivos Electrónicos de Control (SIMDEC).* Oficina Técnica Penal. Consultado el 14 de marzo del 2026.

41 Ibidem.

¿Qué pasa si el agresor se acerca o viola la restricción?

Cuando se activa una advertencia disuasiva, el operador del Área de Control debe verificar la situación y realizar una advertencia imperativa al usuario, indicándole que se encuentra próximo a un área de exclusión o fuera del área de inclusión y que debe desistir de la acción y retornar al perímetro correspondiente. El protocolo[42] dispone expresamente la realización de tres persuasiones seguidas. Si el usuario no acata, el operador comunica de inmediato el hecho a la División de Dispositivos Electrónicos de Control de la Dirección del Centro de Seguridad y Emergencias de la Policía Nacional. (CSJ, 2024).

En casos de violencia doméstica o de protección integral a mujeres contra toda forma de violencia, el protocolo agrega una acción simultánea: el operador debe llamar a la víctima para su resguardo, conocer su ubicación y brindarle orientaciones de autoprotección. Este punto es clave porque muestra que, incluso cuando el sistema se presenta como vigilancia del agresor, también incorpora un componente directo de gestión sobre la víctima: contacto, localización, orientación y eventual articulación para resguardo. No se trata, por tanto, de una tecnología que solo "controle al agresor", sino de una infraestructura que también incorpora a la víctima en su cadena operativa. (CSJ, 2024). Si se agotan las tres advertencias disuasivas o si se activa directamente una alarma de reacción inmediata, el operador debe verificar el posicionamiento georreferencial en tiempo real y comunicar con celeridad la salida del área de inclusión o la violación del área de exclusión. A partir de allí se activa la respuesta policial. (CSJ, 2024).

La respuesta en calle: Policía, 911 y apoyo táctico

El protocolo[43] no se limita a prever alertas en pantalla. También regula una respuesta territorial. Una vez recibida la activación de la alarma, el operador debe convocar, por canal operativo de radiocomunicación, al personal de la comisaría más cercana o al personal de la Dirección de Operaciones Tácticas Motorizadas LINCE. Simultáneamente, debe convocar otro móvil de la comisaría jurisdiccional para acudir al resguardo de la víctima. Además, puede requerir la intervención de otros organismos integrantes del Sistema 911 según la magnitud del incidente. (CSJ, 2024; Ministerio del Interior et al., 2024).

- **Respuesta policial ante alarma**

RESPUESTA POLICIAL — activada por Alarma de reacción inmediata		
Despacho: ■ Comisaría más cercana al lugar del agresor ■ Grupo LINCE (Dirección de Operaciones Tácticas Motorizadas) ■ Otros recursos del Sistema 911 según magnitud	**Resguardo de la víctima:** ■ Móvil adicional de la comisaría jurisdiccional ■ Contacto simultáneo con la víctima (UMA/Empower) ■ Orientaciones de autoprotección en tiempo real	**Registro:** ■ Toda la intervención queda registrada en el software ■ El operador documenta el cierre del evento ■ Trazabilidad de comunicaciones y unidades despachadas

Fuente: Elaboración propia según reporte de acceso a la información pública proveído por el Ministerio del Interior.

Esto permite ver con claridad cuál es la lógica de mitigación que organiza el SIMDEC: delimitación espacial, monitoreo permanente, advertencia, llamada simultánea a la víctima y despacho policial. El sistema busca actuar antes de que el acercamiento se traduzca en una agresión consumada, pero lo hace mediante

42 Ibidem.

43 Ibidem.

una cadena de detección y reacción, no mediante una neutralización física automática del riesgo. Por eso, su funcionamiento real depende de cuestiones tan concretas como disponibilidad de móviles, cobertura comunicacional, tiempos de despacho y capacidad de coordinación en terreno. (CSJ, 2024).

El "dispositivo para la víctima" dentro del protocolo SIMDEC

Un elemento poco discutido públicamente es que el propio protocolo del SIMDEC incorpora, en un anexo, un dispositivo específico para la víctima. Allí se describe una unidad compuesta por un teléfono celular y una aplicación llamada *Empower*[44], diseñada para su seguridad. Según el anexo, esta aplicación permite enviar mensajes al Área de Control, muestra señal y nivel de batería, y cuenta con un botón de "Pánico Área de Control Principal" que genera una alarma SOS. También contempla un botón para llamar al Área de Control en caso de consultas o problemas con el dispositivo. El mismo anexo insiste en que la usuaria debe portar el teléfono en todo momento y cargar la batería al menos una vez al día. Cabe destacar que la aplicación solo se encuentra disponible para dispositivos con sistema operativo Android. (CSJ, 2024).

Este elemento es importante por dos razones. La primera es descriptiva: muestra que, dentro del propio diseño del SIMDEC, la víctima no queda completamente fuera del circuito tecnológico, sino que puede convertirse también en portadora de un dispositivo conectado al sistema. La segunda es analítica: evidencia que la protección prometida por el sistema depende parcialmente de prácticas materiales cotidianas —llevar el teléfono, mantener batería, conservar señal— que recaen sobre la persona que se busca proteger. Más adelante, en el análisis crítico, esto nos obligará a preguntarnos por los riesgos de revictimización y de responsabilización tecnológica. (CSJ, 2024).

Nendive: una herramienta distinta, pero parte del mismo ecosistema

Es importante no confundir SIMDEC con Nendive[45]. Aunque ambos forman parte del ecosistema institucional paraguayo de respuesta tecnológica frente a la violencia doméstica, cumplen funciones distintas. Nendive fue presentada por el Poder Judicial como una aplicación móvil para facilitar denuncias o solicitudes de asistencia en casos de violencia doméstica, inicialmente para el Departamento Central, a través de la Oficina de Atención Permanente y los Juzgados de Paz. Según la descripción oficial, la aplicación está solo disponible para Android, permite el registro de usuarios con georreferencia de la vivienda e incorpora un botón de pánico que genera automáticamente un caso urgente y envía una alerta a la Oficina de Atención Permanente. A partir de esa alerta, funcionarios judiciales se comunican con la víctima y, según la denuncia, podría activarse un protocolo de asistencia por medio de la fuerza pública y comunicación al juzgado de turno. (Poder Judicial, 2021).

La nota oficial también indica que Nendive incluye botones para llamar al 137 del Ministerio de la Mujer y al 911 de la Policía Nacional, que permite a funcionarios cargar información para seguimiento de casos y que contempla la posibilidad de incorporar evidencias —audios, videos e imágenes— enviadas por la víctima a través de otros medios como WhatsApp o Telegram. En este sentido, Nendive no funciona como una herramienta de restricción espacial del agresor, sino como un canal de denuncia, georreferencia, alerta y seguimiento institucional. (Poder Judicial, 2021).

Leídas en conjunto, estas dos herramientas muestran dos modalidades distintas de mitigación. La tobillera, según el protocolo SIMDEC, busca actuar mediante restricción espacial, monitoreo y respuesta policial ante la violación de perímetros. Nendive, en cambio, funciona como canal remoto de denuncia

---

44 Aplicación solo disponible para dispositivos con sistema operativo Android.

45 Poder Judicial Paraguay. (2021). *Aplicación para ayudar a víctimas de violencia doméstica*. Consultado el 14 de marzo del 2026.

y activación institucional a partir de la intervención de la víctima. Ambas tecnologías operan sobre el cruce entre vigilancia, datos y seguridad, pero lo hacen desde puntos diferentes del circuito. (CSJ, 2024; Poder Judicial, 2021).

6.6. Un sistema que produce datos, responsabilidades y zonas grises

La reconstrucción de este circuito operativo también permite advertir qué cosas sí quedan claras en los documentos públicos y cuáles no. A partir del protocolo[46] y de la documentación oficial puede afirmarse que el SIMDEC implica geolocalización en tiempo real, configuración de áreas de inclusión y exclusión, clasificación de eventos, comunicaciones con la víctima en determinados supuestos y coordinación con Policía y 911. También puede afirmarse que Nendive implica registro de usuarios, georreferencia del domicilio, generación de casos urgentes y eventual incorporación de evidencias. Pero esos documentos no detallan públicamente, al menos en lo relevado para esta investigación, aspectos fundamentales como plazos de retención de datos, estándares de auditoría independiente, arquitectura de almacenamiento, controles de acceso, *logs* de uso o métricas públicas de desempeño. Esta ausencia de detalle no es un dato menor: señala precisamente el terreno sobre el que deberá avanzar el análisis legal y de transparencia. (CSJ, 2024; Poder Judicial, 2021).

46 Poder Judicial Paraguay. (2024). *Reglamento del Sistema de Monitoreo por Dispositivos Electrónicos de Control (SIMDEC).* Oficina Técnica Penal. https://www.pj.gov.py/images/contenido/otp/Dispositivos-electronicos/5%20Reglamento%20SIMDEC%2030_12_2024.pdf

Ecosistema tecnológico de respuesta a violencia de género en Paraguay

SIMDEC / Tobillera	EMPOWER (App)	NENDIVE (App / Poder Judicial)	Linea SOS MUJER 137
Función: ■ Monitoreo del agresor + alerta a víctima ante acercamiento ■ Requiere orden judicial previa	**Función:** ■ Dispositivo entregado a la víctima (celular UMA) ■ Botón de pánico → comunicación directa con OMDEC ■ Alertas de proximidad del agresor en tiempo real ■ Ampliar denuncia sin concurrir a dependencia policial	**Función:** ■ Denuncia remota de violencia doméstica ■ Botón de pánico → caso urgente ■ Activación de Oficina de Atención Permanente	**Función:** ■ Atención telefónica 24 horas ■ Orientación y derivación a servicios ■ No requiere smartphone ni datos móviles
Cobertura: ■ Nacional (desde agosto 2025) ■ Requiere energía eléctrica y cobertura de red	**Cobertura:** ■ Nacional (vinculada al SIMDEC) ■ Solo Android · requiere datos móviles activos ■ Uso voluntario — no puede imponerse a la víctima	**Cobertura:** ■ Departamento Central ■ Solo Android · requiere datos móviles activos	**Cobertura:** ■ Nacional ■ Sin requisito de conectividad digital
Institución responsable: ■ Ministerio del Interior — OMDEC ■ Proveedor: Consorcio Track (Contrato 13/2024)	**Institución responsable:** ■ Ministerio del Interior — OMDEC ■ Mismo proveedor que la tobillera (Consorcio Track)	**Institución responsable:** ■ Poder Judicial ■ Oficina de Atención Permanente	**Institución responsable:** ■ Ministerio de la Mujer
Limitaciones clave: ■ Carga de cuidado sobre víctima (batería, datos, portabilidad) ■ Sin marco de protección de datos específico ■ Acceso del proveedor privado a datos sensibles	**Limitaciones clave:** ■ La víctima debe portar el dispositivo en todo momento ■ Debe mantener batería cargada al menos una vez al día ■ Debe tener datos móviles activos permanentemente ■ Si rechaza el dispositivo, el sistema solo monitorea al agresor ■ El Estado provee el celular, pero la carga operativa cotidiana recae en la víctima	**Limitaciones clave:** ■ Disponible solo para Android ■ Georreferenciación del domicilio de la víctima almacenada ■ Sin política pública de protección de datos documentada	**Limitaciones clave:** ■ Sin integración formal documentada con el SIMDEC ■ Depende de capacidad de respuesta institucional ■ Sin datos públicos de efectividad disponibles

Fuente: Elaboración propia según documentos proveídos vía Portal de acceso a la información pública por el Ministerio del Interior y la Policía Nacional.

7. HACIA UN ANÁLISIS LEGAL

Comprender cómo funciona la tobillera u otros dispositivos tecnológicos en la práctica es indispensable para evaluar su marco normativo. No alcanza con saber que existe una ley o un protocolo: hay que observar qué datos circulan, qué instituciones intervienen, quién toma decisiones en cada etapa, qué obligaciones materiales recaen sobre las personas involucradas y qué zonas grises aparecen entre la promesa de protección y la operación concreta del sistema. Por eso, una vez reconstruido este entramado técnico e institucional, el paso siguiente es examinar si el régimen jurídico paraguayo regula de manera suficiente cuestiones centrales como legalidad, necesidad, proporcionalidad, debido proceso, protección de datos, transparencia, acceso a información y rendición de cuentas. Es allí donde el análisis legal se vuelve clave: no para repetir cómo debería funcionar el sistema, sino para preguntar si las reglas vigentes son capaces de controlar los riesgos que este mismo funcionamiento produce.

7.1. Marco normativo paraguayo: qué habilita el Estado y qué exige el derecho

Para realizar una investigación documental en Paraguay necesitamos además reconstruir el entramado legal que sostiene la implementación del Sistema de Monitoreo por Dispositivos Electrónicos de Control (SIMDEC). Este análisis jurídico será abordado desde una perspectiva crítica. El interés no es solo establecer qué habilita el derecho, sino qué exige, qué tensiones genera y, especialmente, qué queda pendiente.

Para ello, el análisis está construido en capas jerárquicas, tal como lo impone el artículo 137 de la Constitución de la República del Paraguay (en adelante, la Constitución), que establece la supremacía constitucional y la incorporación de los tratados internacionales de derechos humanos como parte del bloque normativo aplicable. Esa jerarquía define, además, cuáles son las obligaciones vinculantes del Estado y cuál es la vara con la que debe evaluarse cualquier política pública, incluida, en este caso, la implementación del SIMDEC.

El capítulo avanza en cuatro bloques: el marco internacional de derechos humanos ratificado por Paraguay; el marco constitucional y la arquitectura legal específica del SIMDEC; el marco sustantivo de violencia de género en el que opera el sistema; y el régimen de datos personales aplicable. La pregunta que guía a este apartado no es si el SIMDEC tiene base legal —la tiene—, sino si esa base legal es suficiente para garantizar que el sistema funcione con enfoque de derechos: protegiendo efectivamente a las víctimas, respetando las garantías del imputado, salvaguardando los datos de ambas partes y habilitando la rendición de cuentas pública.

Marco internacional de derechos humanos: obligaciones vinculantes del Estado paraguayo

Así, partiendo del marco internacional de derechos humanos, debemos recordar que Paraguay ha ratificado los principales instrumentos internacionales de derechos humanos, lo que le genera al país obligaciones jurídicas concretas. En ese sentido, la Declaración Universal de Derechos Humanos (Naciones Unidas, 1948) constituye la matriz de la que derivan los demás instrumentos. Para este estudio, interesan especialmente el derecho a la vida, la libertad y la seguridad de las personas (artículo 3), el principio de igualdad ante la ley (artículo 7) y el derecho a la privacidad (artículo 12), que protege a las personas contra injerencias arbitrarias en su vida privada.

El Pacto Internacional de Derechos Civiles y Políticos (PIDCP) (Naciones Unidas, 1966.a), ratificado mediante Ley Nº 5/1992, y el Pacto Internacional de Derechos Económicos, Sociales y Culturales (PIDESC) (Naciones Unidas, 1966.b), ratificado mediante Ley Nº 4/1992, completan el piso normativo universal. El PIDCP es el más directamente relevante para este estudio, ya que protege el derecho a la vida (artículo 6), la libertad y seguridad personal (artículo 9), la privacidad frente a injerencias ilegítimas (artículo 17) y la igualdad ante la ley (artículo 26). El PIDESC complementa ese marco desde la perspectiva de los derechos que hacen posible una vida libre de violencia: acceso a la salud, a la educación y a condiciones materiales mínimas de bienestar.

Por su parte, la Convención Americana sobre Derechos Humanos (CADH), conocida como Pacto de San José de Costa Rica (1969), fue el primer tratado internacional de derechos humanos ratificado por Paraguay tras el advenimiento de la democracia. Este tratado protege derechos que el SIMDEC pretende garantizar, pero también derechos que el sistema debe respetar, y esa doble función genera la primera tensión jurídica fundamental del sistema.

Desde la perspectiva de la víctima, la CADH garantiza el derecho a la vida (artículo 4), la integridad personal (artículo 5), la protección judicial (artículo 25), la igualdad ante la ley (artículo 24), y el derecho a la intimidad y protección de la Honra y de la Dignidad (artículo 11). Estos derechos fundamentan la obligación del Estado de adoptar medidas activas para proteger a las mujeres en situación de violencia. Desde la perspectiva del imputado, la misma Convención garantiza la presunción de inocencia (artículo 8.2), las garantías del debido proceso (artículo 8) y también, el derecho a la privacidad. Precisamente porque el SIMDEC afecta derechos protegidos por la CADH, tanto los del imputado como los de la víctima, su implementación debe superar el test de legalidad, necesidad y proporcionalidad que la propia Convención y la jurisprudencia de la Corte Interamericana exigen para cualquier restricción de derechos.

Igualmente, el Protocolo Adicional a la Convención Americana sobre Derechos Humanos en materia de Derechos Económicos, Sociales y Culturales (Protocolo de San Salvador, 1999), ratificado por Paraguay mediante Ley N.º 1.040/1997, complementa este marco reconociendo derechos que inciden en las condiciones materiales de protección de las víctimas.

Cabe señalar que la Comisión Interamericana de Derechos Humanos (CIDH), en su informe sobre el uso de la prisión preventiva, ha recomendado la adopción de medidas alternativas a esta, criterio que posteriormente fue retomado por la Organización de los Estados Americanos (OEA) en su informe de 2017. En particular, se destaca la recomendación de implementar mecanismos menos restrictivos, incluyendo expresamente "la vigilancia del imputado mediante algún dispositivo electrónico de rastreo o posicionamiento de su ubicación física" (OEA, 2017, párr. 122). Esta recomendación respalda formalmente el marco jurídico del SIMDEC como medida compatible con los estándares interamericanos. Sin embargo, es importante notar que ambos informes refieren a la cuestión en términos generales, considerando la reducción del hacinamiento carcelario y salvaguarda de derechos de personas privadas de libertad, sin abordar específicamente el uso de estas tecnologías en contextos de violencia de género[47]. Esa ausencia de orientaciones específicas para el contexto de género constituye un vacío interpretativo relevante que el marco normativo nacional debe llenar.

47 En Paraguay, sin embargo, el sistema ha sido presentado públicamente con un encuadre distinto al de medida cautelar alternativa al encarcelamiento. Las declaraciones del Ministro del Interior a la prensa lo posicionaron como una herramienta de respuesta directa a la violencia de género —en particular la violencia física— y de prevención de sus consecuencias más graves (Ministerio de justicia, s.f.; ABC Color, 2023). Este encuadre discursivo no es menor: desplaza la lógica garantista del monitoreo electrónico hacia una lógica de control del riesgo, en la que la tecnología se presenta como respuesta visible a una demanda social urgente. Esa reconfiguración del sentido político del sistema tiene consecuencias sobre las expectativas que genera, los criterios con que se evalúa su eficacia y la presión institucional para expandirlo, independientemente de la evidencia disponible sobre su funcionamiento real.

Para complementar el marco internacional, se tiene el instrumento jurídico más directamente relevante para este estudio, la Convención Interamericana para Prevenir, Sancionar y Erradicar la Violencia contra la Mujer, conocida como Convención de Belém do Pará (1994), ratificada por Paraguay mediante Ley N.º 605/1995. Es frecuentemente citada como modelo de tratado vinculante en la materia, lo que refleja su carácter paradigmático en el sistema interamericano. Esta convención consagra el derecho de toda mujer a una vida libre de violencia, tanto en el ámbito público como privado (artículo 3), y establece que los Estados deben garantizar el pleno ejercicio de los derechos civiles, políticos, económicos y sociales de las mujeres, incluyendo el derecho a un recurso sencillo y rápido ante los tribunales que la ampare contra actos que violen sus derechos (artículo 4, literal g). A este respecto, el SIMDEC puede entenderse como una materialización de este derecho a la protección efectiva.

En segundo lugar, el artículo 7 establece la obligación estatal de adoptar, "por todos los medios apropiados y sin dilaciones, políticas orientadas a prevenir, sancionar y erradicar dicha violencia". Ese mandato de adoptar todos los medios apropiados es la base jurídica internacional más sólida para la implementación del SIMDEC en casos de violencia de género. La Convención también obliga al Estado a actuar con la debida diligencia para prevenir, investigar y sancionar la violencia (artículo 7, literal b). El estándar de diligencia debida no exige solo que las medidas existan normativamente, sino que sean efectivas en la práctica. Un sistema de monitoreo electrónico que funcione deficientemente ya sea por falta de infraestructura, tiempos de respuesta inadecuados o errores operativos, no satisface este estándar, aunque cuente con respaldo legal formal.

En tercer lugar, la Convención establece mecanismos concretos de responsabilidad internacional, es decir, las personas y grupos tienen derecho a presentar peticiones ante la CIDH cuando los Estados han fallado en adoptar las medidas necesarias para prevenir, sancionar y erradicar la violencia contra la mujer. Esto significa que el incumplimiento de las obligaciones derivadas de la Convención implica una fuente de responsabilidad internacional del Estado.

Otro instrumento internacional fundamental para este análisis es la Convención sobre la Eliminación de Todas las Formas de Discriminación contra la Mujer (CEDAW), ratificada por Paraguay mediante Ley N.º 1.215/1986, que impone a los Estados la obligación de adecuar su legislación y políticas públicas para garantizar la igualdad y no discriminación de las mujeres en todas las esferas de la vida. Su Protocolo Facultativo, ratificado mediante Ley N.º 1.683/2001, reconoce la competencia del Comité CEDAW para recibir comunicaciones individuales de víctimas de violaciones una vez agotados los recursos internos, ampliando así el mecanismo de exigibilidad.

Para este análisis, dos Recomendaciones Generales del Comité CEDAW son de especial relevancia. La Recomendación General N.º 19 (Comité para la Eliminación de la Discriminación contra la Mujer [CEDAW], 1992) establece que los Estados pueden ser responsables de actos privados si no adoptan medidas con la diligencia debida para impedir la violación de los derechos, investigar y castigar los actos de violencia e indemnizar a las víctimas. Esto posiciona al Estado como actor activo en la prevención, y fundamenta la legitimidad de medidas de monitoreo electrónico orientadas a esa finalidad. La Recomendación General N.º 35, que actualiza y profundiza la N.º 19 (CEDAW, 2017), avanza en la misma dirección e insta a los Estados a adoptar medidas tecnológicas efectivas de protección y monitoreo. Estas recomendaciones tienen carácter obligatorio y deben ser implementadas por los poderes del Estado, aspecto que suele ser subestimado en el diseño institucional paraguayo y que constituye en sí mismo, un problema de cumplimiento.

La CEDAW también resulta importante al momento de considerar la participación de las mujeres en el diseño de las políticas que las afectan, arista frecuentemente subvalorada cuando se considerar políticas públicas que conciernen al colectivo[48]. Un sistema como el SIMDEC, diseñado sin consulta a organizaciones de mujeres y sin evaluación diferenciada de sus impactos, presenta una deuda con estos estándares internacionales.

En suma, el marco internacional ratificado por Paraguay respalda sin ambigüedades la implementación del SIMDEC como herramienta legítima de política pública orientada a la protección de las mujeres. Pero ese mismo marco no admite cualquier implementación. Exige efectividad real y no solo existencia normativa. Es por ello por lo que, la tensión entre legitimidad formal e impacto práctico es el hilo conductor del resto del análisis.

7.2. Base constitucional del SIMDEC

La Constitución contiene los elementos normativos necesarios para fundamentar y, al mismo tiempo, limitar la implementación de políticas como el SIMDEC. A raíz de ello, es necesario evaluar si las tensiones resultantes están suficientemente resueltas en el diseño normativo.

Desde el punto de vista de los derechos que justifican el sistema, la Constitución protege la vida e integridad física de las personas (artículo 4), la libertad y la seguridad individual (artículo 9) y, de forma más específica, la protección contra la violencia en el ámbito familiar. El artículo 60 establece explícitamente que "el Estado promoverá y garantizará la protección de la familia" y prohíbe la violencia en las relaciones familiares, imponiendo una obligación positiva de actuación estatal. Esta disposición, junto con los principios de igualdad formal consagrados en los artículos 46 a 48, constituyen la base constitucional del mandato de protección a las mujeres víctimas de violencia.

Ahora bien, el mismo texto constitucional que fundamenta el SIMDEC también genera tensiones que deben resolverse para su efectiva implementación. El derecho a la intimidad —protegido en los artículos 33 y 36 de la Constitución— resulta directamente afectado por el sistema de geolocalización en tiempo real que caracteriza al monitoreo electrónico. Esta afectación no es necesariamente ilegítima: el propio texto constitucional admite restricciones de derechos cuando estas son necesarias, proporcionales y están fundadas en ley. Pero esa habilitación condicional exige que el marco normativo del SIMDEC justifique, con precisión, qué datos se recogen, con qué finalidades, por cuánto tiempo y bajo qué controles[49].

Las garantías procesales consagradas en los artículos 16 y 17 de la Constitución —la presunción de inocencia y el derecho al debido proceso— también entran en el análisis, en particular a partir de las modificaciones introducidas por la Ley N.º 7270/2024 (que abordaremos más adelante) que eliminó la prohibición de aplicar el sistema a personas imputadas por crímenes y suprimió el requisito de no

48 La participación de las mujeres en el diseño de medidas como el SIMDEC no es una exigencia procedimental menor. Un sistema pensado sin considerar las condiciones materiales y digitales de sus destinatarias puede reproducir, bajo apariencia protectora, las mismas desigualdades que pretende corregir. La activación del botón de pánico, por ejemplo, presupone que la víctima cuenta con un teléfono inteligente operativo, plan de datos activo, cobertura de red y alfabetización digital suficiente para usar la aplicación bajo presión, condiciones que no pueden darse por garantizadas para mujeres en situación de vulnerabilidad económica, residentes en zonas rurales o con acceso limitado a la conectividad. Una mirada interseccional sobre el diseño del sistema es la única forma de identificar estas brechas antes de que se conviertan en riesgos reales.

49 La geolocalización constituye un dato personal cuya recolección y procesamiento en tiempo real involucra, en el marco del SIMDEC, no solo al imputado sino también a la víctima. Mientras que sobre el imputado recae la lógica explícita del control, la víctima queda igualmente expuesta a una vigilancia constante: su ubicación, sus movimientos y sus datos de contacto son accesibles, en tiempo real, a todos los actores institucionales que operan el SIMDEC. Esta asimetría no está tematizada en ningún instrumento normativo vigente. El marco legal justifica la vigilancia del imputado, pero no examina, ni limita, el grado de exposición de la víctima como condición de funcionamiento del sistema. La víctima no elige ser vigilada; lo es como consecuencia necesaria de ser protegida.

reincidencia. Esos cambios no son necesariamente inconstitucionales, pero requieren una justificación normativa sólida sobre los criterios de proporcionalidad que rigen la decisión judicial de imponer una tobillera electrónica como medida cautelar.

Desde un criterio formal, la Constitución habilita el SIMDEC como mecanismo compatible con sus valores y mandatos. Sin embargo, esa compatibilidad depende de que el diseño normativo e institucional resuelva activamente las tensiones que el mismo texto constitucional genera. Una política pública que invoca la protección de las mujeres sin resolver esas tensiones puede crear un sistema que ampare formalmente pero no proteja de manera integral en la práctica.

7.3. Arquitectura legal del SIMDEC: del diseño normativo a los protocolos de operación

El SIMDEC es regulado por un conjunto articulado de normas que van desde la ley formal hasta los protocolos de operación cotidiana. Entender ese ensamble legal es indispensable para evaluar su funcionamiento real y sus implicancias para los derechos de las personas involucradas.

Este parte de la Ley N° 5863/2017 que creó el SIMDEC con el objetivo de implementar su uso en el marco de procesos judiciales. En su formulación original, el sistema fue concebido fundamentalmente como una medida alternativa a la privación de libertad, en otras palabras, una herramienta para reducir el uso de la prisión preventiva y humanizar la respuesta penal. El enfoque específico en la violencia de género no estaba en el centro de ese diseño inicial. La primera modificación, introducida por la Ley N° 6345/2019, fue posteriormente derogada por la Ley N° 7270/2024, que constituye el cambio normativo más significativo del sistema hasta la fecha. Esta última ley amplió los artículos 2, 3, 4, 5, 6, 7, 8, 10 y 11 de la norma original, introduciendo modificaciones que merecen un análisis cuidadoso.

En el artículo 2, que define el ámbito de aplicación, la Ley N° 7270/2024 incorpora expresamente la Ley N° 5777/2016 de Protección Integral a las Mujeres contra toda Forma de Violencia. Este cambio tiene una relevancia jurídica y política fundamental dado que formaliza la conexión entre el SIMDEC y el marco normativo de violencia de género, lo que hasta ese momento era solo una posibilidad interpretativa. A partir de 2024, el sistema de monitoreo electrónico está explícitamente diseñado para operar en casos de violencia contra las mujeres.

Por su parte, el artículo 3, que regula las condiciones de aplicabilidad, fue modificado de dos maneras. La ley anterior prohibía la aplicación del SIMDEC a personas imputadas por crímenes; la nueva norma elimina esa prohibición. Asimismo, suprime el requisito de no reincidencia para acceder a la medida. Ambos cambios amplían el espectro de personas sobre las que puede operar el sistema como alternativa a la prisión.

Finalmente, la Ley N.º 7270/2024 previó su reglamentación en un plazo de sesenta días a partir de su promulgación. Sin embargo, esa ley no cuenta con un decreto reglamentario propio y exclusivo; en cambio, la implementación se rige por el conjunto normativo conformado por la Ley N° 5863/2017, su modificatoria Ley N° 7270/2024 y el Decreto N° 466/2023, que había sido dictado antes de la modificación legislativa. Esta situación genera atención ya que las disposiciones reglamentarias que operativizan el sistema fueron diseñadas para la ley anterior, y no necesariamente incorporan los estándares exigidos por la ampliación de 2024, en especial en lo referente a los casos de violencia de género.

En efecto, el Decreto N° 466/2023 es la norma que operativiza el mandato legal. Es también, en muchos aspectos, la norma más reveladora del análisis jurídico, porque es aquí donde el sistema muestra su arquitectura institucional concreta, define a sus actores, establece sus características técnicas y regula el tratamiento de la información generada.

En cuanto al mapa de actores, el Decreto distingue entre varios componentes institucionales, tanto desde la empresa proveedora, responsable de la prestación de servicios de apoyo al monitoreo (artículo 1, literal e); los operadores del SIMDEC (artículo 8, literal f), encargados del monitoreo continuo de los dispositivos; hasta la Oficina de Control Interinstitucional, que articula la acción entre los diferentes organismos involucrados. Esta última, conforme al artículo 4 del Decreto, puede solicitar la contratación de servicios de acuerdo con lo establecido en la Ley N° 7021/2023 de Suministros y Contrataciones Públicas[50]. Para nuestro análisis, es importante tener en cuenta esta remisión jurídicamente significativa, que es la que vincula la operatividad del SIMDEC al régimen de contrataciones públicas y, por tanto, a las obligaciones de transparencia y rendición de cuentas que ese régimen impone.

En cuanto a las características técnicas con implicancias de derechos, el Decreto establece que el SIMDEC debe "reflejar el posicionamiento georreferencial de los usuarios en tiempo real, con indicación de la fecha y hora" (artículo 3, literal b), y "emitir alertas en casos del acercamiento entre el usuario y la víctima" (artículo 3, literal e), incluyendo la obligación de informar a la víctima de la proximidad del usuario a un área de exclusión (artículo 11, literal a). Estas funcionalidades no son técnicamente neutrales, porque implican la recolección y procesamiento en tiempo real de datos de geolocalización tanto del imputado como de la víctima, lo que constituye tratamiento de datos personales de ambas partes desde el momento en que el sistema se activa. Que estas funciones estén establecidas normativamente en el Decreto da base legal a la recopilación de datos; sin embargo, el Decreto no establece quién tiene acceso diferenciado a esa información, en qué condiciones puede ser consultada o compartida, ni qué ocurre con ella cuando el sistema detecta un error o una falsa alarma.

El tercer estrato normativo del SIMDEC está compuesto por las acordadas de la Corte Suprema de Justicia (CSJ) y el Protocolo SIMDEC/OMDEC. Estas normas de inferior jerarquía son, sin embargo, las que más directamente determinan la experiencia real del sistema dado que definen quién puede solicitar la medida, cómo se evalúa su factibilidad técnica, qué información se requiere a la víctima y cómo se gestiona una alerta.

La Acordada N.º 1779/2025 aprobó el "Protocolo de Aplicación de Tobilleras Electrónicas: Implementación Primera Fase". Su texto de fundamentos es revelador en sí mismo: el protocolo surge para brindar a los magistrados una herramienta procedimental adecuada que les permita garantizar la correcta aplicación del SIMDEC, "a fin de asegurar y optimizar el control, vigilancia, así como la ubicación y los movimientos de las personas y de las medidas cautelares aplicadas". El protocolo limita la primera fase al fuero penal ordinario, específicamente a los jueces penales de garantías de la capital, y establece que, en primer término, la medida corresponde a casos de violencia familiar. Asimismo, dispone que los jueces penales de garantías, al momento de aplicar la medida, deberán escuchar e informar a las víctimas de todas las actuaciones referentes a las tobilleras colocadas al imputado, y notificarlas de todas

50 Según información proporcionada por el Ministerio del Interior mediante Nota DGS911 N.º 53/2026, en respuesta a una solicitud de acceso a la información pública, la empresa adjudicada para la provisión y operación del sistema es el Consorcio Track, en el marco de la Licitación Pública Nacional N.º 02/2024 (ID 451113), formalizada mediante Contrato Abierto N.º 13/2024. (Portal Unificado de Información Pública. *Solicitud #100405*. (23 de febrero, 2026). https://informacionpublica.paraguay.gov.py/#!/ciudadano/solicitud/100405

las audiencias y resoluciones relacionadas[51]. Esta última disposición merece destacarse positivamente ya que incorpora a la víctima como sujeto activo del procedimiento, no como mera destinataria de las decisiones del sistema. No obstante, su alcance práctico depende de la capacidad operativa real de los juzgados para cumplirla, cuestión que la norma no aborda.

Por su parte, la Acordada N.º 1801/2025 amplió el protocolo en la misma línea, expandiendo gradualmente el alcance del sistema. El Protocolo SIMDEC/OMDEC, aprobado el 30 de diciembre de 2024 e implementado conforme al conjunto normativo, es el documento más operativo del sistema y cuenta con cuatro elementos que merecen atención específica.

Primero, el Protocolo limita explícitamente la primera etapa de implementación al ámbito territorial de la ciudad de Asunción. Esta delimitación geográfica no es solo una cuestión de capacidad: genera una desigualdad de protección entre las mujeres víctimas de violencia según su lugar de residencia, lo que plantea preguntas sobre el cumplimiento del mandato constitucional e internacional de protección igualitaria. Cabe señalar que la Nota DGS911 N.º 53/2026, obtenida mediante solicitud de acceso a la información pública[52], registra dispositivos activos fuera de la capital entre enero de 2025 y enero de 2026, lo que sugiere que la práctica habría superado el marco territorial del Protocolo.

Segundo, el artículo 5, literal b, del Protocolo define el "dispositivo electrónico de control o dispositivo" como la "tecnología utilizada por el SIMDEC, para el monitoreo e interacción con el usuario y la víctima en su caso". Esta definición es significativa porque reconoce explícitamente que el dispositivo no solo controla al imputado, sino que también interactúa con la víctima. Esa interacción implica, necesariamente, recolección de datos de la víctima.

Tercero, el artículo 7 regula el informe de factibilidad técnica, que es el procedimiento por el cual se evalúa si es técnicamente posible aplicar el SIMDEC en un caso concreto. Para realizar esa evaluación, cuando el área de exclusión se concibe como una orden de alejamiento, la víctima debe proporcionar su dirección, ubicación georreferenciada y otros datos de relevancia (literal e). Esto convierte a la víctima en fuente obligatoria de datos para la operación del sistema que la protege. El Protocolo no establece ningún mecanismo de consentimiento informado ni de protección específica de esa información.

Cuarto, el Protocolo establece que, en caso de alerta en contextos de violencia doméstica o de protección integral de las mujeres, el operador del Área de Control debe generar simultáneamente una llamada a la víctima "para su resguardo, así como para conocer su ubicación y brindar las orientaciones adecuadas" (artículo correspondiente, literal c). Asimismo, el artículo 15 regula el botón de pánico: "en los casos de activación del Botón de Pánico generados por Unidad de Monitoreo Ambulatorio (UMA) en el sistema, el operador del Área de Control deberá atender el llamado del usuario víctima, para cerciorarse de la situación que generó la alarma y actuar conforme a la información recibida". Estos mecanismos son positivos en términos de protección. Sin embargo, su efectividad real depende de condiciones

51 La obligación de escuchar e informar a la víctima que establece el Protocolo es un avance que no debe sobrevalorarse. En su formulación actual es una mención procedimental que no define el contenido mínimo de esa información, ni el momento en que debe brindarse, ni el formato accesible en que debe comunicarse. Informar efectivamente a una víctima sobre las implicancias del SIMDEC no es notificarle que se colocó una tobillera al imputado; es explicarle qué datos suyos serán recolectados, cómo funciona el sistema de alertas y qué se espera de ella, qué limitaciones técnicas tiene y qué hacer si falla, y a quién acudir si el sistema no responde. Esa información, para ser real y no meramente formal, debe además considerar las condiciones concretas de cada víctima, desde la alfabetización digital, acceso a conectividad y situación emocional al momento de recibirla. La obligación de informar debería estar regulada como requisito sustantivo de validez de la medida, no como un paso administrativo dentro del expediente.

52 Portal Unificado de Información Pública. Solicitud #100405. (23 de febrero, 2026). https://informacionpublica.paraguay.gov.py/#!/ciudadano/solicitud/100405

que a simple lectura del documento, no se garantiza. Esto es, que la víctima tenga teléfono celular, que ese teléfono esté cargado y con cobertura, que la víctima sepa usar la herramienta, y que el operador pueda responder en tiempo real. La transferencia de responsabilidades hacia la víctima, que debe tener dispositivo, estar conectada y activar el sistema, no está examinada críticamente en ningún punto del marco normativo.

En definitiva, el ensamble normativo del SIMDEC construye un sistema jurídicamente fundado, pero con brechas significativas en materia de protección de datos, cobertura territorial, efectividad operativa y distribución de responsabilidades. Esas brechas reflejan las limitaciones estructurales de una política pública diseñada bajo aparente urgencia y sin evaluación de impacto previa.

7.4. Leyes sustantivas de violencia de género

La Ley N.º 5777/2016 "de Protección Integral a las Mujeres contra toda forma de violencia" constituye el marco sustantivo central del sistema de protección a las mujeres en Paraguay. Su objeto es garantizar a las mujeres una vida libre de violencia, reconociendo el carácter estructural de la violencia de género y la obligación del Estado de actuar en todos los ámbitos, desde la prevención, atención, sanción y reparación, con enfoque diferenciado. La ley define en su artículo 3 los distintos tipos de violencia contra las mujeres, lo que implica que el sistema de monitoreo electrónico puede ser aplicable en un universo de situaciones bastante más amplio que la violencia física visible.

La incorporación expresa de la Ley N.º 5777/2016 al ámbito de aplicación del SIMDEC tiene una consecuencia interpretativa importante y es que el sistema de monitoreo electrónico queda sujeto a los principios de no revictimización, acceso a la justicia con enfoque de género, protección de la intimidad de las víctimas y transversalidad de género en todas las medidas adoptadas. Esos principios deberían ser considerados rectores de la implementación para evitar que el sistema transfiera cargas operativas a la víctima, exponga sus datos a riesgos innecesarios o funcione de manera que disuada la denuncia.

Por otro lado, la Ley N.º 1600/2000 es el instrumento procesal básico mediante el cual las víctimas de violencia doméstica acceden al sistema de medidas de protección en Paraguay. Establece el procedimiento de denuncia, la competencia de los Juzgados de Paz y las medidas que pueden disponerse, entre las cuales se incluyen, a partir de su articulación con el SIMDEC, las de monitoreo electrónico. La Ley N.º 6568/2020, que modificó la Ley N.º 1600/2000, amplió el alcance de las medidas de protección y la posibilidad de su cumplimiento mediante tecnología, creando así el nexo normativo entre el régimen de violencia doméstica y el SIMDEC.

En esta misma línea, el artículo 229 del Código Penal tipifica la violencia familiar como delito, castigado con pena privativa de libertad de uno a seis años al que, aprovechándose del ámbito familiar, ejerciera actos de violencia física o psicológica sobre el cónyuge, concubino, pareja sentimental, o la persona con quien se hubiese negado a restablecer una relación de pareja, así como sobre parientes hasta el cuarto grado de consanguinidad. La disposición aclara explícitamente que el vínculo incluye las relaciones vigentes o finalizadas, y que la convivencia no es un requisito. Esta última precisión es especialmente relevante para la aplicación del SIMDEC, considerando que la amenaza puede provenir de parejas o exparejas que no conviven con la víctima, haciendo que el monitoreo de la proximidad sea operativamente más complejo y requiera una definición precisa de las áreas de inclusión y exclusión.

La pena puede aumentarse hasta ocho años cuando el autor fuese reincidente, cuando el acto se realizare contra niños, niñas y adolescentes o en su presencia, cuando el autor utilizara un arma, o cuando los actos tengan lugar en el domicilio de la víctima. Estos agravantes son precisamente el tipo de situaciones que la Ley N.º 7270/2024 habilitó a monitorear mediante tobilleras, al eliminar la exclusión anterior de personas imputadas por crímenes y el requisito de no reincidencia. Aunque, aquí surgen cuestionamientos en cuanto a que esa extensión no estuvo acompañada de estándares de proporcionalidad ni de evaluación de impacto.

En definitiva, el marco sustantivo de violencia de género en el que opera el SIMDEC provee la base normativa que justifica su uso y define los principios con los que debe ser compatible. Pero ese marco también genera preguntas: cómo se garantiza la coordinación entre las distintas instancias competentes, cómo se protege a la víctima en el proceso de activación del sistema, y cómo se evita que la tecnología devenga en una carga adicional sobre quienes ya cargan con las consecuencias de la violencia. Asimismo, ¿la víctima que inicia un proceso recibe información adecuada sobre las implicancias de la aplicación de una tobillera electrónica al agresor? ¿Sabe que el sistema requerirá sus datos de geolocalización? ¿Está en condiciones de evaluar los beneficios y riesgos de esa medida frente a otras alternativas disponibles? El Protocolo SIMDEC/OMDEC establece que la víctima debe ser informada y escuchada, pero no define el contenido mínimo de esa información ni establece mecanismos para garantizar que sea comprensible y accesible para personas con distintos niveles de alfabetización digital.

7.5. El régimen de datos personales: la privacidad como derecho subordinado al discurso de la seguridad

El tratamiento de datos personales es quizás el aspecto menos visible del SIMDEC, opacado por el discurso prevalente de la seguridad y la urgencia de proteger la vida e integridad física de las víctimas. No obstante, esa circunstancia no está justificada plenamente a nivel jurídico. De la lectura articulada de la ley y los protocolos de implementación se desprende que, desde el momento en que el SIMDEC se activa, genera y procesa datos de al menos dos personas: el imputado, cuya geolocalización es monitoreada en tiempo real, y la víctima, cuyos datos de contacto, domicilio y ubicación son incorporados al sistema como condición de su funcionamiento. La privacidad no es aquí un valor abstracto en tensión con la seguridad sino una condición de la seguridad misma.

Al tratarse datos personales en la implementación del sistema, su inadecuada protección podría generar riesgos considerables, incluyendo la exposición de la víctima a la persona agresora, la filtración de información a terceros no autorizados o el uso secundario de los datos para fines distintos a los declarados. Considerando el riesgo, el SIMDEC tendría que incluir como arista fundamental, el marco legal de protección de datos personales.

En noviembre de 2025, quedó sancionada la ley N.º 7593/2025 de Protección de Datos Personales en Paraguay. La aprobación de esa norma es un avance institucional significativo en un país que, hasta ese momento, carecía de un marco general aplicable al tratamiento de datos por parte del Estado y de los particulares. Sin embargo, la propia ley establece un período de vacancia de veinticuatro meses antes de entrar en pleno vigor y condicionado a la reglamentación de esta. Durante ese intervalo, el régimen jurídico aplicable al tratamiento de datos generados por el sistema es sectorial y fragmentado.

En el caso de estudio, este período de vacancia implica que el Estado paraguayo puede seguir expandiendo un sistema de vigilancia sobre datos de personas en situación de vulnerabilidad sin contar con los principios, garantías y mecanismos de control que una ley general de protección de datos debería proveer: minimización de datos, finalidad específica, limitación de la retención, derechos de acceso y rectificación, autoridad de control independiente y régimen de sanciones administrativas[53]. La ausencia de ese marco no significa que el SIMDEC opere en el vacío absoluto; significa, que lo hace bajo un conjunto disperso de normas sectoriales que cubren aspectos parciales, pero no garantizan una protección integral.

A falta de una ley general, el tratamiento de datos en el marco del SIMDEC se rige por un conjunto de normas sectoriales que no fueron diseñadas específicamente para este sistema y que, en consecuencia, dejan sin regular aspectos críticos de su funcionamiento. El Decreto N.º 466/2023, artículos 17 a 19, es la norma más directamente aplicable al SIMDEC en materia de datos. El artículo 17 autoriza el uso de la información generada por el sistema para fines estadísticos o de política criminal, siempre que ello no violente las circunstancias particulares del tratamiento de datos personales. El artículo 18 establece un plazo de retención de cinco años contados desde la comunicación judicial del cese de la medida, transcurridos los cuales la información debe ser destruida[54]. El artículo 19 tipifica el uso o divulgación indebida de la información como indicio de comisión del hecho punible de revelación de un secreto de carácter privado, conforme al artículo 147 del Código Penal, sin perjuicio de otras sanciones administrativas. Estas disposiciones constituyen un punto de partida, pero presentan ciertas limitaciones, por ejemplo, al no regular el acceso diferenciado según el rol institucional de cada actor o definir quién está habilitado para auditar el cumplimiento de estas reglas[55].

La Ley N.º 6.534/2020 de Protección de Datos Personales Crediticios es una norma sectorial orientada al ecosistema financiero y crediticio. Sin embargo, en ausencia —hasta la entrada en vigor plena de la nueva normativa— de un régimen general de protección de datos personales[56], sus definiciones y principios son aplicables como referencia interpretativa por analogía al tratamiento de datos en otros contextos, incluido el tratamiento de datos en el SIMDEC. En este contexto, los datos tratados en el SIMDEC —en particular los datos de geolocalización del imputado y los datos de contacto y ubicación

53 Los principios mencionados forman parte de cualquier régimen moderno de protección de datos. La minimización exige que solo se recojan los datos estrictamente necesarios para el fin declarado. La finalidad específica prohíbe usar los datos para propósitos distintos a los que justificaron su recolección: datos recogidos para monitorear una medida cautelar no pueden utilizarse, por ejemplo, para construir perfiles de riesgo o alimentar bases policiales. La limitación de la retención impone que los datos se conserven solo durante el tiempo necesario y se eliminen una vez cumplida su finalidad. Los derechos de acceso y rectificación garantizan que las personas cuyos datos son tratados puedan saber qué información existe sobre ellas y corregirla si es inexacta. La autoridad de control independiente es el organismo estatal —ajeno a quienes operan el sistema— encargado de supervisar el cumplimiento de estas reglas y recibir denuncias. Finalmente, el régimen de sanciones administrativas establece consecuencias concretas ante incumplimientos.

54 Sobre el punto, resulta particular que el Decreto N.º 466/2023 establece que la información debe ser destruida a los cinco años del cese de la medida. El Pliego de Bases y Condiciones (PBC) de la Licitación Pública Nacional N.º 02/2024 (ID 451113) por la que se adjudicó e implementó el SIMDEC, en cambio, dice que la información "será entregada al OMDEC" al finalizar el contrato, sin mencionar destrucción. No son necesariamente contradictorios, pero tampoco son coherentes. El pliego no prevé ningún protocolo de destrucción, lo que deja abierta la pregunta de qué ocurre con los datos una vez transferidos y si el plazo de retención del Decreto se aplica efectivamente.

55 El pliego de bases y condiciones de la Licitación N.º 451113/2024 establece que "el responsable de la base de datos, en tanto titular de ella, será el SIMDEC, y el encargado de su tratamiento, la Empresa Proveedora." Esta distinción entre titular y encargado es correcta en términos de protección de datos, pero el pliego no establece qué obligaciones concretas asume la empresa como encargada. Sin auditoría técnica independiente, sin estándares de seguridad exigibles contractualmente y sin acceso irrestricto del Estado a sus propios datos, la distinción es más formal que real.

56 La Ley N.º 7.593/2025 dispone la derogación expresa, a través de su artículo 59, de diversas disposiciones de la Ley N.º 6.534/2020, incluyendo las definiciones de datos personales y datos personales sensibles (art. 3, incisos a y b), así como la prohibición de difusión de datos sensibles (art. 4). No obstante, dado que la nueva ley aún no ha entrado plenamente en vigor, se configura un escenario de transición normativa en el que las definiciones previamente vigentes pierden sustento formal sin que el nuevo régimen resulte todavía plenamente aplicable. Esta situación exige recurrir a interpretaciones sistemáticas y a estándares internacionales para asegurar un nivel adecuado de protección de los datos personales.

de la víctima— deben ser considerados datos personales que requieren protección y garantías al momento de su procesamiento, incluso en ausencia de una regulación plenamente vigente, atendiendo a su carácter intrusivo y a los riesgos asociados a su tratamiento.

Por su parte, la Ley N.º 4.868/2013 de Comercio Electrónico, en su artículo 10, establece que los proveedores de servicios de intermediación y de alojamiento de datos[57] deben almacenar los datos de conexión y tráfico generados durante la prestación del servicio por un período mínimo de seis meses, únicamente a los efectos de facilitar la localización del equipo terminal empleado para la transmisión de la información. La norma prohíbe expresamente el uso de esos datos para fines distintos a los permitidos por la ley y exige la adopción de medidas de seguridad para evitar su pérdida, alteración o acceso no autorizado. Esta disposición es relevante para el SIMDEC porque la empresa proveedora del sistema opera, en la práctica, como un proveedor de servicios de intermediación que almacena y transmite datos de conexión y geolocalización en tiempo real. Su Decreto Reglamentario N.º 1.165/2014, en el artículo 11, añade el deber de informar al usuario sobre la finalidad y el tratamiento de sus datos personales, quién los recibirá y quién será responsable de su custodia, reforzando el principio de transparencia en el tratamiento. Si bien, podría decirse que estas normas conforman un régimen que, en conjunto, es parche ante la ausencia de una protección integral que comprometen la integridad del sistema y la protección efectiva de las personas que lo protagonizan.

En la misma línea, la Comisión Nacional de Telecomunicaciones (CONATEL) establece obligaciones de registro y conservación de datos de tráfico en el marco de la prestación de servicios de comunicaciones. Así, la Resolución Directorio N.º 0700/2025[58] —que modifica la Resolución N.º 2583/2024— impone a los prestadores de servicios de acceso a internet la obligación de conservar registros de conexión por un período mínimo de seis meses, incluyendo información como direcciones IP, puertos, fecha, hora e identificación del abonado (artículo 1). A su vez, la Ley N.º 7549/2025[59] refuerza este esquema al establecer un plazo mínimo de conservación de doce meses para datos de tráfico (art. 7), con una finalidad estrictamente delimitada a la identificación de usuarios en el marco de investigaciones penales específicas (artículos 1 y 2).

No obstante, estos regímenes responden a una lógica sectorial y finalista, centrada en datos de tráfico y conectividad, y no contemplan el tratamiento de datos de geolocalización en tiempo real ni otras categorías de información como las que procesa y almacena el SIMDEC. Siendo así, su aplicabilidad resulta, en el mejor de los casos, analógica y limitada. En este contexto, la fijación de un plazo único de conservación de cinco años para los datos del SIMDEC, previsto en el decreto reglamentario, excede los estándares sectoriales existentes y plantea interrogantes en términos de proporcionalidad, especialmente ante la falta de criterios diferenciados según el tipo de dato o de mecanismos claros de

57 Cabe precisar que los proveedores de sistemas de monitoreo electrónico, como los dispositivos de tobilleras utilizados en el SIMDEC, no encuadran estrictamente en la categoría de prestadores de servicios de intermediación o alojamiento de datos prevista en la Ley N.º 4.868/2013. No obstante, dado que estos sistemas implican la transmisión, almacenamiento y procesamiento continuo de datos de geolocalización mediante redes de telecomunicaciones —incluyendo tráfico de datos y señales asociadas a la conectividad—, las obligaciones de conservación, seguridad y finalidad establecidas en dicha normativa pueden ser consideradas como un marco de referencia analógico en materia de gobernanza de datos.

58 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. Recuperado el 14 de abril de 2026, de 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). 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. Recuperado el 14 de abril de 2026, de https://silpy.congreso.gov.py/web/descarga/ley-146014

almacenamiento, revisión y supresión verificable de la información. Nos encontramos entonces, por un lado, entre un modelo de retención mínima y finalista y por el otro, un régimen de almacenamiento prolongado planteado por el marco normativo del SIMDEC, sin una gobernanza equivalente que garantice su tratamiento adecuado[60].

El primer vacío es la ausencia de un protocolo de acceso diferenciado a los datos. El SIMDEC involucra a múltiples actores, desde jueces, fiscales, operadores del sistema, policía, empresa proveedora, hasta personal del Ministerio de la Mujer, que tienen roles distintos y que, lógicamente, deberían tener niveles de acceso diferenciados a la información generada. Sin embargo, ningún instrumento vigente establece quién puede ver qué, en qué condiciones, con qué registro de accesos y bajo qué responsabilidad. Esto no es un mero detalle técnico sino una condición que facilita el uso indebido de la información, consciente o inconscientemente, y que impide cualquier auditoría significativa sobre el manejo de los datos.

El segundo vacío es la falta de regulación sobre la interoperabilidad entre sistemas. El SIMDEC no opera de forma aislada, sino que interactúa, o debería interactuar, con el sistema 911, la Fiscalía y eventualmente el sistema de alerta policial. Cada uno de esos sistemas tiene sus propias bases de datos, sus propios protocolos de acceso y sus propias reglas de retención. La ausencia de un marco de interoperabilidad significa que no hay reglas claras sobre qué datos pueden circular entre estos sistemas, en qué formato[61], con qué garantías[62] y bajo qué controles. En la práctica, esto puede generar tanto duplicación innecesaria de información como falta de coordinación en situaciones de emergencia.

El tercer vacío es la inexistencia de auditoría técnica independiente. La empresa proveedora del SIMDEC opera la infraestructura del sistema, incluyendo los servidores donde se almacenan los datos de geolocalización e interacción[63]. Ningún instrumento vigente establece dónde deben estar ubicados esos servidores, si en Paraguay o en la nube de un proveedor extranjero, qué estándares técnicos y legales de seguridad deben cumplir, ni quién tiene la facultad y la capacidad técnica de auditar ese cumplimiento. La delegación de la infraestructura de datos en un proveedor privado, sin auditoría independiente, constituye una caja negra desde el punto de vista de la gobernanza pública.

---

60 Puede parecer que estas discusiones sobre cómo se guardan los datos son secundarias frente a un objetivo mucho más urgente, como prevenir la violencia y proteger la vida de las víctimas. Sin embargo, precisamente porque el sistema busca proteger, es fundamental que funcione bien y de forma segura. Si los datos se almacenan por demasiado tiempo, sin reglas claras sobre quién puede acceder a ellos o cómo se eliminan, el mismo sistema que pretende proteger puede terminar generando nuevos riesgos. Por eso, al diseñar una política pública como el SIMDEC, no basta con incorporar tecnología, también es necesario definir cómo se usan, se guardan y se protegen los datos que esa tecnología produce.

61 De hecho, llama la atención que el PBC de la Licitación Pública N.º 02/2024 (ID 451113) prevé que los datos del sistema —incluyendo ubicaciones almacenadas y geozonas— puedan ser entregados en un pendrive, disco externo o CD/DVD. Transferir datos de geolocalización de víctimas e imputados en medios físicos portátiles, sin que el pliego establezca ningún estándar de cifrado ni protocolo de cadena de custodia, es un riesgo de seguridad significativo. La mención del CD/DVD también revela un desfase tecnológico que no es menor cuando se habla de infraestructura de vigilancia crítica.

62 Aquí, cabe resaltar que, revisado el PBC de la Licitación Pública N.º 02/2024 (ID 451113) se exige el backup (resguardo) diario de la información del sistema, lo cual es positivo. Pero no establece ningún estándar técnico sobre cómo debe realizarse: cifrado, almacenamiento seguro, acceso restringido, verificación de integridad. Un backup diario sin estándares de seguridad definidos ofrece una garantía formal sin contenido técnico verificable.

63 La revisión del PBC de la Licitación Pública N.º 02/2024 (ID 451113) confirma que el documento no establece ningún requisito sobre la ubicación física de los servidores en los que se almacena la información generada por el SIMDEC. La única mención relevante exige que operen en “modalidad de alta disponibilidad” por tratarse de un sistema de misión crítica, pero no precisa si deben estar radicados en el territorio nacional, bajo qué legislación operan ni si el Estado tiene derecho de auditoría sobre ellos. La omisión no es menor ya que la localización de los servidores determina qué marco jurídico rige los datos almacenados, qué autoridades pueden acceder a ellos y qué ocurre con esa información si el contrato se rescinde o la empresa enfrenta contingencias legales en su país de origen.

El cuarto vacío concierne al régimen de responsabilidad ante brechas de seguridad. El artículo 19 del Decreto N.º 466/2023 tipifica el uso indebido de la información generada por el SIMDEC como indicio de comisión de un delito penal. Pero esa remisión al Código Penal es esencialmente reactiva: actúa una vez producido el daño. No existe un mecanismo administrativo de control preventivo, ni una obligación de notificar a las personas afectadas en caso de brecha de seguridad, ni un plazo definido para la respuesta institucional ante incidentes de este tipo. En el contexto del SIMDEC, donde una filtración de datos de ubicación de la víctima puede tener consecuencias directas sobre su seguridad física, la ausencia de un régimen preventivo y de notificación es particularmente grave.

El quinto vacío es la falta de justificación de proporcionalidad en el régimen de retención. El artículo 18 del Decreto N.º 466/2023 establece que la información generada por el SIMDEC debe ser destruida transcurridos cinco años desde el cese de la medida. Ese plazo no está acompañado de ninguna justificación de proporcionalidad, ni diferenciado según el tipo de dato (geolocalización, datos de contacto, registros de alertas), ni modulado según la gravedad del caso o el resultado del proceso judicial. Un plazo uniforme de cinco años para todos los datos, de todas las personas, en todos los casos, no satisface el principio de minimización que el derecho internacional de protección de datos exige como estándar.

En conjunto, estos vacíos no son excepciones al funcionamiento normal del sistema. El SIMDEC funciona hoy en un entorno de protección de datos jurídicamente insuficiente. Esta circunstancia afecta de manera diferenciada a las víctimas de violencia de género, que son quienes tienen más que perder si la información que proporcionan al sistema termina siendo accesible a quien precisamente debería estar lejos de ellas.

El recorrido por el marco jurídico del SIMDEC permite ahora formular un juicio de conjunto. No un inventario de normas, sino una evaluación crítica de la arquitectura normativa del sistema a la luz del estándar que el propio derecho constitucional e internacional exigen para cualquier medida que restrinja o interfiera con derechos fundamentales: el test de legalidad, necesidad y proporcionalidad[64]. Este test no es una herramienta externa que se aplica al sistema desde afuera; es la vara que el propio marco ratificado por Paraguay impone como condición de validez de cualquier intervención estatal que afecte derechos.

El primer umbral del test pregunta si la medida tiene base legal suficiente: si está prevista en norma accesible, precisa y previsible en sus efectos. La respuesta en este caso es afirmativa, en términos generales. Como se vio, el SIMDEC cuenta con base legal formal en la Ley N.º 5863/2017, su modificatoria Ley N.º 7270/2024, el Decreto Reglamentario N.º 466/2023 y los protocolos de implementación. Sin embargo, el mandato de legalidad no se satisface solo con la existencia de normas, ya que también exige que esas normas sean suficientemente precisas para que las personas destinatarias puedan prever las consecuencias de su aplicación. En ese sentido, las brechas identificadas en materia de datos personales, como la ausencia de reglas de acceso diferenciado, falta de auditoría independiente, indefinición sobre la ubicación de los servidores, debilitan la calidad de la legalidad del sistema. Una norma que habilita el procesamiento de datos personales sin definir quién accede a ellos ni en qué condiciones no cumple plenamente el estándar de precisión que el principio de legalidad exige.

---

64 Este test tiene raíces en la teoría constitucional alemana y fue sistematizado por el jurista Robert Alexy en su obra *Teoría de los Derechos Fundamentales* (1985). Su formulación original se conoce como el principio de proporcionalidad, del cual la legalidad, la necesidad y la proporcionalidad en sentido estricto son sub-mandatos; es decir, no tres pruebas independientes sino tres niveles de un mismo análisis. La Corte Interamericana de Derechos Humanos ha incorporado este estándar en su jurisprudencia, y en la práctica judicial y en la literatura jurídica latinoamericana sus elementos suelen presentarse como criterios autónomos, uso que este estudio sigue sin desconocer su origen común. Lo relevante, en cualquier caso, es la función que cumple el análisis, de obligar al Estado a justificar racionalmente por qué una restricción de derechos está habilitada, es necesaria y no genera más daño del que pretende evitar.

El segundo umbral pregunta si la medida persigue un objetivo compatible con los derechos humanos y declarado con suficiente claridad. Aquí la respuesta también es afirmativa. La protección de las mujeres víctimas de violencia de género y la alternativa al encarcelamiento preventivo son finalidades no solo compatibles con el marco de derechos humanos sino exigidas por él.

Ahora bien, el tercer umbral pregunta si la medida es necesaria: si el objetivo perseguido no puede alcanzarse con medidas menos intrusivas, o si al menos se justifica racionalmente su selección frente a alternativas disponibles. Aquí la respuesta es solo parcialmente afirmativa. La evidencia comparada internacional —que se examina en capítulos posteriores de este estudio— muestra que el monitoreo electrónico puede ser una herramienta útil en determinadas condiciones, pero que su eficacia depende de un conjunto de factores institucionales que el marco normativo paraguayo no garantiza, como son los tiempos de respuesta adecuados, capacidad operativa de monitoreo continuo, integración con servicios de asistencia a las víctimas. Más importante aún, el SIMDEC fue implementado sin una evaluación de impacto previa y sin una comparación sistemática con otras medidas de protección menos intrusivas. La necesidad de una medida no puede darse por supuesta, debe ser demostrada, y ese ejercicio está ausente del proceso de aplicación del SIMDEC.

El cuarto umbral es el más exigente y el que genera mayor tensión en el caso del SIMDEC. La proporcionalidad pregunta si los medios empleados son adecuados al fin perseguido, sin sacrificar derechos de manera desproporcionada. El SIMDEC presenta aquí un problema estructural que el marco normativo no ha resuelto: para funcionar, el sistema requiere que la víctima proporcione sus datos de contacto y geolocalización, que esté disponible para ser contactada en caso de alerta, que cuente con un dispositivo móvil operativo y que cargue con las responsabilidades operativas que el botón de pánico implica. Esa carga no está justificada proporcionalmente en ningún instrumento normativo, ni se ha evaluado si los beneficios del sistema para las víctimas compensan los riesgos que su participación en él genera. Un sistema de protección que convierte a la persona protegida en sujeto de recolección de datos personales, sin garantías claras de cómo esa información será protegida, plantea una pregunta de proporcionalidad que el actual entramado legal no responde.

Por último, se debe incorporar la rendición de cuentas como dimensión adicional del análisis, siguiendo el enfoque de los Principios Internacionales sobre la Aplicación de los Derechos Humanos a la Vigilancia de las Comunicaciones (Principios Necesarios y Proporcionales, 2013), que establecen explícitamente que la supervisión independiente y la rendición de cuentas son condiciones autónomas de legitimidad para cualquier sistema de vigilancia estatal[65], más allá del test clásico de proporcionalidad.

A este respecto, el régimen que sustenta al SIMDEC es predominantemente reactivo y penal. La sanción por uso indebido de datos existe, pero solo opera una vez producido el daño. No hay auditoría técnica independiente, no hay obligación de publicar estadísticas periódicas sobre el funcionamiento del sistema, no hay evaluación de impacto vinculada a la renovación de los contratos de servicio, y no

65 Sobre el punto, es importante recordar el informe del Alto Comisionado de Naciones Unidas para los Derechos Humanos El derecho a la privacidad en la era digital (A/HRC/48/31, 2021), el mismo subraya que los mecanismos de supervisión independiente y rendición de cuentas constituyen condiciones autónomas de legitimidad para los sistemas de vigilancia estatal, y no pueden considerarse satisfechos por el mero cumplimiento del test de proporcionalidad.

hay mecanismos de participación de las organizaciones de mujeres en el seguimiento del sistema[66]. La rendición de cuentas no puede ser solo un recurso judicial al que acudir después del daño, sino que debe ser una condición estructural de operación del sistema.

Aquí, se debe aclarar que las debilidades identificadas no son una condena al sistema sino un diagnóstico jurídico. Queda claro que el SIMDEC cuenta con base legal y persigue finalidades legítimas, pero presenta ciertos déficits en cuanto a la legalidad de precisión, necesidad demostrada, proporcionalidad en el tratamiento de datos de las víctimas y rendición de cuentas estructural. Debilidades que son corregibles mediante ajustes normativos y decisiones institucionales concretas. Y, es precisamente, mediante su identificación que las recomendaciones de este estudio pueden ser jurídicamente fundadas y políticamente operativas.

Los capítulos que siguen examinan las dimensiones que el marco jurídico por sí solo no puede revelar: cómo funciona el sistema en la práctica, qué transparencia existe sobre las adquisiciones y contrataciones que lo sostienen, y qué enseñan otras experiencias internacionales sobre los límites y condiciones de efectividad del monitoreo electrónico en contextos de violencia de género.

7.6. Hallazgos empíricos: implementación, transparencia y tensiones institucionales

Para complementar el análisis normativo y reconstruir el funcionamiento real de estas tecnologías en Paraguay, esta investigación incorporó una estrategia empírica basada en dos vías. Por un lado, se realizaron tres pedidos de acceso a la información pública a través del Portal Unificado de Acceso a la Información Pública, dirigidos al Ministerio del Interior, al Ministerio de la Mujer y a la Policía Nacional, todos enviados el 23 de febrero de 2026. Por otro lado, se realizaron entrevistas semiestructuradas con dos actores clave vinculados directamente al funcionamiento o la activación del sistema: un representante del Ministerio de la Defensa Pública y la Secretaria Ejecutiva de la Técnica Penal de la Corte Suprema de Justicia y representante ante el SIMDEC. Además, se realizaron tres intentos de contacto con representantes del Ministerio de la Mujer, que no prosperaron. Sin embargo, respondieron a través del pedido de información pública.

Las respuestas obtenidas fueron desiguales. El Ministerio del Interior remitió una contestación ampliada que permitió reconstruir con mayor detalle el funcionamiento operativo del SIMDEC, sus estadísticas de uso, los criterios de factibilidad técnica y varios aspectos de la infraestructura contratada. En cambio, el Ministerio de la Mujer respondió de forma más general, con información básica sobre sus herramientas institucionales y sin remitir la documentación técnica solicitada.

66 La revisión del Pliego de Bases y Condiciones de la Licitación N.º 02/2024 permite precisar algunos de estos señalamientos. En cuanto a la auditoría técnica, el pliego exige que el software cuente con “auditoría y registro de eventos” (criterio 12 de seguridad del software), pero esa auditoría es interna al sistema y operada por la propia empresa proveedora, no por un organismo independiente. En cuanto a la supervisión del Estado sobre los datos, el acceso del organismo contratante a la base de datos de producción está condicionado a que sea “requerido por la Convocante” y limitado a una vista de solo lectura, lo que significa que el Estado no tiene acceso irrestricto ni permanente a la información que el sistema genera. En cuanto a las penalizaciones, el pliego prevé sanciones contractuales ante incumplimientos del nivel de servicio técnico, pero no contempla penalizaciones específicas ante brechas de seguridad de datos ni ante uso indebido de información sensible. Finalmente, no existe en el pliego ninguna obligación de producir informes periódicos públicos sobre el funcionamiento del sistema, ni mecanismo alguno de rendición de cuentas hacia la ciudadanía.

En el caso de la Policía Nacional, si bien el requerimiento se inició en tiempo y forma, la respuesta sustantiva no fue recibida dentro del plazo originalmente previsto para la investigación: la contestación, canalizada a través del Consorcio TRACK, empresa proveedora del sistema INTELLITRACK, llegó aproximadamente un mes y medio después de presentado el pedido, mediante la Nota D.T.A. N.º 56/2026, con fecha 31 de marzo de 2026, dirigida al Comisario. Gral. Insp. Rafael Candia, Director del CSE de la Policía Nacional y representante ante la Oficina de Control Interinstitucional del SIMDEC. Pese a su carácter tardío, se decidió incorporar estos datos al análisis porque aportan un nivel de detalle cuantitativo y operativo que ninguna de las otras fuentes había provisto, especialmente en relación con series trimestrales de alertas, incidentes técnicos puntuales, capacitación de personal y criterios de clasificación de falsas alarmas. Esta asimetría en la calidad, la oportunidad y la profundidad de las respuestas constituye, en sí misma, un hallazgo sobre el estado de la transparencia pública en torno a estas tecnologías.

La implementación real del sistema está fuertemente condicionada por la infraestructura material

Uno de los hallazgos más claros de esta investigación es que la implementación del SIMDEC no depende solamente de una decisión judicial, sino de una serie de condiciones materiales y técnicas sin las cuales la medida no puede volverse operativa. En la entrevista con el Poder Judicial, la representante ante el SIMDEC, la Dra. Silvana Luraghi, explicó que, antes de otorgar la medida, el juez libra un oficio para el estudio de factibilidad técnica, y que muchos informes iniciales fueron negativos porque las personas imputadas residían en zonas con conexiones eléctricas precarias o sin buena señal. En sus palabras, "muchos informes iniciales fueron negativos porque los imputados vivían en zonas vulnerables (bañados) con conexiones clandestinas o sin señal", mientras que al momento de la entrevista se contabilizaban "163 informes positivos".

Este diagnóstico se ve reforzado por la respuesta oficial del Ministerio del Interior, institución encargada de la operativa del sistema. Según la contestación remitida vía acceso a la información pública, durante 2025 se recibieron 196 pedidos de factibilidad técnica, de los cuales 161 fueron aprobados y 35 resultaron "no factibles". Entre las causas registradas aparecen la falta de infraestructura eléctrica regular, la ausencia de medidor de la ANDE, la insuficiencia de señal celular o satelital, la imposibilidad de ubicar correctamente el domicilio, la negativa de ingreso al lugar y la existencia de oficios judiciales con datos incompletos o direcciones no actualizadas. La propia respuesta subraya que la falta de electricidad regular y la baja cobertura de señal constituyen los factores críticos que limitan la implementación efectiva del SIMDEC en áreas rurales, periféricas o asentamientos urbanos informales.

La respuesta del Consorcio TRACK, en tanto operador técnico del sistema INTELLITRACK contratado por la Policía Nacional, aporta una capa adicional a este diagnóstico. El informe detalla una serie de incidencias técnicas posteriores a la instalación de los dispositivos que confirman la fragilidad material de la que depende el funcionamiento cotidiano del sistema: pérdida definitiva de comunicación en dispositivos que "dejaron de transmitir datos de manera permanente, imposibilitando su monitoreo remoto"; problemas de carga o ausencia de carga atribuidos, en su mayoría, a "uso inadecuado por parte del beneficiario, incluyendo la manipulación indebida o daño en el puerto de conexión durante el proceso de carga"; y ausencia de trazas de posicionamiento vinculadas a fallas en el módulo GPS del dispositivo que afectan la transmisión de datos de geolocalización. A esto se suma un incidente puntual documentado el 7 de febrero de 2026, consistente en la indisponibilidad temporal del módulo de gestión de alarmas entre las 11:30 y las 12:00 horas, que, si bien no interrumpió el monitoreo en tiempo real, impidió dar de alta nuevos dispositivos durante ese intervalo.

Este dato es central porque desplaza la imagen de la tobillera como una solución universal, inmediata y autosuficiente. En la práctica, el acceso a la medida está atravesado por infraestructura eléctrica, conectividad, georreferenciación correcta del domicilio, viabilidad técnica mínima y, además, por la continuidad operativa de una plataforma administrada por un proveedor privado. La promesa de monitoreo permanente reposa sobre una base material profundamente desigual y sobre una arquitectura tecnológica que también registra fallos puntuales. Esto confirma que la política de vigilancia tecnológica no opera sobre un territorio homogéneo, sino sobre un mapa de desigualdades preexistentes y sobre una infraestructura contratada que, como toda infraestructura, falla.

A ello se suma una barrera económica nada menor: las personas interesadas en acceder a la medida deben asumir su costo, y, según señaló el propio defensor público especializado, existe apenas un cupo limitado de dispositivos cubiertos gratuitamente para el área penal de la Defensa Pública. En ese escenario, la tobillera deja de presentarse únicamente como una medida de protección o de control y se revela también como una alternativa a la prisión diferencialmente accesible según la capacidad económica de quien la solicita o la necesita. Más aún, esto muestra que la capacidad estatal de "prevenir" mediante tecnología depende no solo de condiciones básicas de habitabilidad e infraestructura pública, sino también de la posibilidad material de costear el acceso a la propia medida.

Una implementación gradual atravesada por límites materiales y económicos

Otro hallazgo importante es que la implementación del SIMDEC no fue lineal ni homogénea, sino gradual, restrictiva en su etapa inicial y luego acelerada en términos de expansión territorial y disponibilidad de equipos. En la entrevista con la representante del Poder Judicial ante el SIMDEC se explica que, cuando la ley comenzó a aplicarse efectivamente en enero de 2025, "solo contábamos con 20 dispositivos", por lo que el uso se limitó en un primer momento a casos de violencia familiar. La entrevistada agregó que entre enero y agosto de 2025 la expansión fue progresiva "por la escasez de equipos", y que recién en agosto de ese mismo año el sistema se liberó "para todo el país y para todos los jueces penales". Al momento de la entrevista, la misma fuente sostuvo que el sistema contaba con "3.000 tobilleras disponibles" y "156 tobilleras en uso en todo el país".

Sin embargo, cuando esta información se pone en diálogo con la respuesta oficial del Ministerio del Interior, obtenida vía acceso a la información pública, aparece una imagen más matizada. El informe de gestión remitido por la autoridad operativa señala que durante 2025 se realizaron 74 instalaciones y 28 desinstalaciones, mientras que al cierre de enero de 2026 había 86 beneficiarios activos y esa cifra ascendía a 94 al finalizar febrero de 2026. También se informa que las zonas con mayor presencia del sistema eran Central, Alto Paraná y Asunción. Es decir, aun cuando el discurso institucional habla de ampliación nacional y disponibilidad creciente, los datos disponibles muestran una implementación todavía acotada y territorialmente desigual.

La respuesta remitida por el Consorcio TRACK a la Policía Nacional permite observar, además, cómo esa implementación gradual se tradujo en el volumen y tipo de alertas generadas por el sistema. Las estadísticas trimestrales entregadas muestran un crecimiento exponencial que coincide con la liberación del sistema a nivel nacional: durante el primer trimestre de 2025 solo se registraron 2 alarmas (todas por "Violación de Zona de Inclusión"); en el segundo trimestre, 12 alarmas (batería crítica, batería crítica escalada y 9 violaciones de zona de exclusión); en el tercer trimestre —coincidiendo con la ampliación de agosto de 2025— los registros saltaron a más de 9.000 eventos, entre ellos 6.260 "Violación de zona de inclusión", 2.555 "Violación de proximidad de la víctima" y 314 "Violación de zona de exclusión"; en

el cuarto trimestre de 2025 las violaciones de zona de inclusión alcanzaron 57.234 eventos; y en el primer trimestre de 2026 se contabilizaron 48.099 violaciones de zona de inclusión, 162 de proximidad de la víctima, 47 de zona de exclusión, además de 159 alertas de batería crítica, 5 de manipulación de la correa y 2 de manipulación corregida. Este crecimiento no puede leerse linealmente como aumento de violencia o de incumplimientos: el propio Consorcio aclara que, del total de alarmas registradas en ese último trimestre, "solo 5 representaron una violación a la medida de control aplicada". Es decir, de decenas de miles de eventos generados por el sistema, apenas una fracción mínima se correspondió con incumplimientos reales. Este dato es, en sí mismo, uno de los hallazgos más reveladores de la investigación: la expansión del sistema produjo un volumen masivo de alertas cuya correspondencia con situaciones efectivas de riesgo resulta marginal, lo que obliga a repensar qué se mide cuando se celebra la "cobertura" del SIMDEC.

A esta dimensión hay que agregarle otra, menos visible en la narrativa de "modernización", pero central para comprender algunos posibles límites del sistema: el costo económico de la medida. En la entrevista con la misma representante del Poder Judicial se señala expresamente que "existe una tasa que deben pagar los victimarios si tienen abogados particulares" y que quienes cuentan con defensores públicos por insolvencia están exonerados. La misma entrevistada añadió que el dispositivo "tiene un costo" y que, en su apreciación personal, ese monto "es bastante elevado, no es un monto menor", lo que vuelve el pago de la tasa un posible obstáculo para su aplicación. También precisó que la víctima no paga por el dispositivo complementario, aunque no tenemos información sobre si paga o no por los datos móviles para el funcionamiento efectivo del teléfono celular. La respuesta recibida fue que "la víctima nunca paga nada; el Estado provee el celular".

Este punto es especialmente relevante porque muestra que la expansión del sistema no depende solo de la infraestructura ni de la voluntad judicial, sino también de un modelo de acceso atravesado por criterios de solvencia, defensa pública y disponibilidad presupuestaria. La propia entrevistada sugirió que, a futuro, sería necesario que el Estado tenga "un presupuesto asignado por ley para eso", de modo a no depender exclusivamente del pago de tasas por parte de las personas usuarias. Esta lectura se ve reforzada por la entrevista con Osvaldo Prates Grassi, representante del Ministerio de Defensa Pública, donde se sostuvo que "actualmente, el uso de la tobillera es tarifado y la gratuidad es excepcional", y que eso "representa una barrera". Desde esa perspectiva, la aplicación del sistema no solo enfrenta obstáculos técnicos o territoriales, sino también limitaciones económicas concretas que pueden restringir el acceso efectivo a la medida, especialmente en contextos de vulnerabilidad.

En conjunto, estos elementos muestran que la expansión del SIMDEC no debe leerse únicamente como un aumento de dispositivos o cobertura territorial. También debe analizarse en relación con las condiciones sociales, presupuestarias y económicas que hacen posible, o limitan, su efectiva implementación. En otras palabras, el crecimiento del sistema no elimina las desigualdades estructurales de acceso características de Paraguay.

La prevención como posible circuito de vigilancia

Las entrevistas y las respuestas institucionales permiten reconstruir con bastante claridad cómo opera la noción de "prevención" dentro del SIMDEC. En la entrevista con la representante del Poder Judicial ante el SIMDEC, la tobillera es presentada como "una herramienta vital para la protección de las víctimas y para el control real y efectivo de las resoluciones judiciales", en un contexto donde antes "el juez no tenía cómo verificar realmente el cumplimiento". La misma entrevistada añadió que, antes del sistema el control aleatorio del arresto domiciliario era altamente precario y carente de mecanismos estructurados, porque la policía no contaba con capacidad institucional suficiente para realizar las verificaciones. En ese marco, la tecnología aparece no solo como una herramienta de protección, sino también como un mecanismo para hacer ejecutables y verificables decisiones judiciales que antes descansaban en un cumplimiento mucho más incierto.

La respuesta operativa de la autoridad encargada del monitoreo (OMDEC) refuerza esta lógica. Allí se explica que el sistema funciona mediante monitoreo 24/7 a cargo de la OMDEC, clasificación de incidencias y activación escalonada de respuestas. Los eventos se dividen en avisos técnicos, advertencias disuasivas y alarmas de reacción inmediata. Ante una advertencia, el operador realiza hasta tres persuasiones; si no hay acatamiento, se activa el protocolo de intervención policial con verificación georreferencial, despacho de recursos mediante comisaría, Sistema 911 o grupo LINCE, y contacto simultáneo con la víctima para brindarle orientaciones de autoprotección. Toda la actividad queda registrada en el sistema, incluyendo movimientos, comunicaciones y cierre del evento.

La información aportada por el Consorcio TRACK complementa esta lógica desde la perspectiva del proveedor tecnológico. El informe describe un protocolo de verificación de falsas alarmas que incluye el análisis de las trazas de desplazamiento registradas por el sistema, la verificación mediante videollamada y la consulta directa al beneficiado respecto de su ubicación en tiempo real, a través del número telefónico particular declarado al momento de la instalación del dispositivo. Este detalle muestra que, en la práctica, la "prevención" opera mediante un circuito técnico de contrastación que combina GPS, videollamada y comunicación telefónica con la persona monitoreada, es decir, una capa adicional de vigilancia que se activa cada vez que el sistema produce una alerta no confirmada.

Lo que emerge de esta reconstrucción es una forma muy específica de prevención: no una política integral de cuidado, acompañamiento y reparación, sino un circuito de geolocalización, clasificación de riesgos, advertencia, trazabilidad y reacción operativa. Dicho de otro modo, en la práctica la prevención se organiza menos como transformación estructural de las condiciones que producen violencia y más como anticipación de eventos a partir de vigilancia remota y respuesta policial. Este hallazgo no implica negar que el sistema pueda ofrecer cierto margen de protección y control; implica, más bien, precisar que la prevención tecnológica que hoy se implementa en Paraguay tiene una lógica predominantemente securitaria y operativa, antes que una lógica integral de derechos y cuidados.

La incorporación de las víctimas dentro del circuito de vigilancia

Uno de los hallazgos más relevantes del trabajo de análisis empírico es que el sistema no se dirige únicamente a la persona agresora. También incorpora a la víctima dentro del ensamblaje técnico y operativo. En la entrevista con la representante del Poder Judicial se explicó que el sistema incluye "la tobillera para el imputado y un dispositivo electrónico (celular) para la víctima para comunicación directa con la policía". La misma fuente aclaró que ese uso es voluntario y que "el 90 % acepta", pero que si la víctima no acepta el celular, entonces la policía se limita al control de la tobillera del agresor. También se indicó que el Estado provee el celular y los datos para ese uso.

La respuesta operativa remitida por la autoridad encargada del sistema coincide con esa descripción y la vuelve más precisa: el dispositivo de la víctima se denomina UMA (Unidad de Monitoreo Ambulatorio) y funciona con una aplicación llamada Empower. El dispositivo del victimario es un transmisor ReliAlert XC. El dispositivo para la víctima incluye un botón de pánico y comunicación directa con el centro de monitoreo (OMDEC). A su vez, el protocolo de respuesta indica que, ante una alarma o tras el agotamiento de las persuasiones, el operador debe contactar a la víctima para alertar sobre la proximidad del agresor y brindarle orientaciones de autoprotección. Es decir, la víctima no queda por fuera del circuito tecnológico: también es localizada, alertada e incorporada en el flujo de reacción del sistema.

Las estadísticas aportadas por el Consorcio TRACK permiten dimensionar con mayor precisión cuánto peso tiene la vigilancia centrada en la víctima dentro del volumen total de alertas. Solo en el tercer trimestre de 2025 se registraron 2.555 alertas por "Violación de proximidad de la víctima", y en el primer trimestre de 2026 ese tipo de alerta volvió a contabilizar 162 eventos. Cada uno de esos registros implica, por definición, un monitoreo efectivo del movimiento de la víctima respecto del agresor, y por lo tanto un rastreo sostenido de su propia ubicación. Es decir, la protección tecnológica no se limita a vigilar al agresor: necesariamente produce datos sobre la víctima, su trayectoria y su proximidad relativa.

Este punto se vuelve más crítico cuando se incorpora la mirada del Ministerio de Defensa Pública (MDP). En esa entrevista Osvaldo Prates Grassi representante del MDP afirmó que "la víctima debe tener Internet o datos móviles siempre activos para que su sistema de defensa funcione", y se subraya que esto constituye "una barrera económica". También se advierte que el software vinculado al sistema requiere permisos que obligan a entregar datos constantemente y que, en las mesas técnicas, "nadie aborda cómo la exposición de los movimientos de la víctima ante terceros vulnera su privacidad".

Leídas en conjunto, estas fuentes permiten sostener que la protección tecnológica no solo amplía capacidades estatales de monitoreo, sino que también podría redistribuir cargas técnicas hacia las víctimas. Aunque formalmente el Estado provea el teléfono y los datos en algunos casos, el uso cotidiano del sistema exige batería, conectividad, disponibilidad del dispositivo, manejo mínimo de la herramienta y exposición sostenida a un régimen de localización y alerta. Desde una perspectiva feminista y de derechos humanos, esto obliga a preguntarse hasta qué punto la promesa de protección tecnológica termina desplazando parte del trabajo de sostener la seguridad hacia quienes ya se encuentran en situación de vulnerabilidad.

La desigualdad en la transparencia estatal

Los pedidos de acceso a la información pública permitieron advertir un patrón claro de asimetría institucional. La respuesta más robusta provino del Ministerio del Interior, institución encargada de la operativa del sistema, que remitió datos ampliados sobre factibilidad técnica, instalaciones, número de usuarios activos, clasificación de eventos, registros mínimos, acceso a datos y continuidad operativa. Gracias a esa respuesta fue posible reconstruir con bastante precisión la lógica práctica del SIMDEC y algunos de sus principales límites.

En cambio, la respuesta del Ministerio de la Mujer fue bastante más básica y general. La institución identificó como herramientas tecnológicas principales la Línea 137 "SOS Mujer" y el canal de atención vía WhatsApp, y afirmó que ambas cuentan con "protocolos, manuales operativos, guías de intervención y resoluciones ministeriales". Sin embargo, a continuación indican que esos documentos "son de uso interno y no pueden ser remitidos, garantizando confidencialidad y protección de datos". También informan categorías generales de datos recolectados y mencionan acciones de accesibilidad y alfabetización digital, pero sin poner a disposición documentación técnica o normativa suficiente para auditar externamente la gobernanza de esas herramientas. La respuesta sobre barreras y revictimización fue igualmente reveladora. El Ministerio de la Mujer reconoció que "las barreras tecnológicas, económicas y territoriales constituyen factores estructurales que limitan el acceso equitativo a los servicios", y sostuvo que los contextos digitales pueden generar "situaciones de exposición permanente, control o presión sobre las víctimas", con efectos posibles de revictimización. Sin embargo, esas afirmaciones no estuvieron acompañadas de evaluaciones específicas, métricas, informes diagnósticos o documentación sustantiva sobre cómo se abordan concretamente esos riesgos en las herramientas tecnológicas bajo su órbita. En ese sentido, la respuesta admite el problema, pero no ofrece suficiente evidencia pública sobre su tratamiento institucional.

El caso de la Policía Nacional merece una consideración particular. A diferencia del Ministerio del Interior, que respondió directamente con información institucional, la Policía Nacional canalizó su respuesta a través del proveedor privado (Consorcio TRACK), lo que es en sí mismo un dato significativo: quien termina produciendo la información operativa que alimenta el análisis público no es una dependencia estatal, sino una empresa contratada. Además, la respuesta llegó fuera de los plazos establecidos por la normativa de acceso a la información pública. Paradójicamente, y pese a esa demora, fue una de las respuestas más detalladas en materia de estadísticas trimestrales, fechas concretas de capacitación e incidentes técnicos puntuales. Esta doble condición, extemporaneidad y densidad informativa, expone una tensión estructural: la información granular existe y está disponible en los sistemas del proveedor, pero su circulación hacia la ciudadanía no está organizada bajo estándares de publicación proactiva, sino que depende de pedidos puntuales respondidos fuera de plazo y mediados por un actor privado.

Desde una perspectiva de transparencia, esto es relevante porque una respuesta administrativa no equivale automáticamente a una política pública auditable. La calidad de la información entregada, su nivel de detalle y la disponibilidad de documentos concretos siguen siendo muy desiguales entre instituciones, lo que dificulta el escrutinio público del sistema en su conjunto.

La debilidad del debate sobre privacidad, tratamiento de datos y auditoría

Otro de los hallazgos más preocupantes del análisis es la fragilidad del debate institucional sobre privacidad, protección de datos y controles de acceso. Desde el Ministerio de Defensa Pública se sostuvo de manera explícita que "no hay una recomendación formal" sobre estas cuestiones y que, en la práctica, "la privacidad parece pasar a un segundo plano, tanto para la víctima como para el victimario", aunque se reconoce que la vulneración de la intimidad puede ser "peor que la enfermedad". Esta formulación tiene un peso particular porque no proviene de una crítica externa, sino del interior mismo de una institución que participa en la activación y gestión de estas medidas.

La misma entrevista agrega que en las mesas técnicas se discuten fallas de precisión del GPS o cuestiones de seguridad operativa, pero "nadie aborda cómo la exposición de los movimientos de la víctima ante terceros vulnera su privacidad". También se advierte que nunca se trató de manera sustantiva la auditoría del software, la retención y eliminación de datos o la necesidad de controlar quién accede a la información y con qué justificación. Incluso se habla de una "confianza ciega" en que la tobillera es la "receta mágica", y se plantea que la tecnología funciona como un "arma de doble filo".

Ahora bien, esta debilidad en la discusión institucional convive con una narrativa de seguridad técnica más consolidada. La respuesta operativa indica que el acceso a los datos es "estrictamente jerárquico y limitado al personal autorizado de la OMDEC y el Centro de Monitoreo", que los datos están cifrados "tanto en reposo como en tránsito" y que la información se almacena durante la vigencia del contrato para luego eliminarse de los sistemas del proveedor y ser entregada a la OMDEC.

La respuesta del Consorcio TRACK suma detalles importantes y nuevas preguntas. Según el proveedor, el acceso a los datos de geolocalización y a los reportes "se encuentra restringido a los usuarios del Área de Control y Monitoreo, conforme a los perfiles y privilegios asignados dentro de la plataforma", mientras que un "Equipo de Soporte" opera sobre la misma plataforma con "privilegios diferenciados que permiten la administración de usuarios y perfiles, sin intervenir en las tareas operativas de monitoreo". La creación de nuevos perfiles de usuarios estaría restringida exclusivamente a perfiles con rol de administrador. Cuando un operador es reasignado, la empresa tercerizada es notificada formalmente para dar de baja el perfil; y, para nuevas incorporaciones, se gestiona el alta mediante solicitud formal. Además, "se realizan controles operativos mediante la verificación diaria de la nómina de oficiales asignados a cada turno". Finalmente, se informa que la plataforma registra las actividades de las personas usuarias "mediante *logs* de acceso y operación", lo que "permite la trazabilidad de las acciones ejecutadas dentro del sistema" y habilita "la verificación posterior de accesos y la detección de eventuales usos indebidos".

Este nivel de detalle técnico, sin embargo, refuerza el hallazgo crítico más que disolverlo. Lo que el Consorcio describe es un régimen de auditoría interna gestionado por el propio proveedor y por la administración policial, no un mecanismo de auditoría independiente, externa o ciudadana. Los *logs* existen, pero no hay información pública sobre quién los revisa, con qué periodicidad, con qué criterios o con qué consecuencias en caso de detección de accesos indebidos. En otras palabras, el sistema documenta su propio uso, pero esa documentación no se traduce en una rendición de cuentas pública.

El hallazgo, entonces, no es que el sistema carezca por completo de previsiones técnicas, sino que existe una brecha entre seguridad tecnológica y gobernanza democrática de los datos. Hay controles de acceso, cifrado, almacenamiento y registros de actividad, pero no aparece con la misma claridad un marco público suficientemente desarrollado sobre auditoría independiente, trazabilidad verificable de accesos, límites materiales del tratamiento de datos o mecanismos de rendición de cuentas hacia las personas afectadas.

El sistema está diseñado para registrar pero no para rendir cuentas con el mismo nivel de intensidad

Finalmente, la evidencia empírica permite sostener otro hallazgo importante: el SIMDEC está diseñado para producir y almacenar una gran cantidad de información, pero esa capacidad de registro no se corresponde con el nivel de evaluación pública disponible. La respuesta operativa señala que el sistema almacena datos del victimario, geoposicionamiento en tiempo real, historial de movimientos, tipo de evento o alerta, fecha y hora y unidad policial interviniente. También se informa que toda la actividad queda asentada en el software, incluyendo comunicaciones del operador y cierre del evento por parte de las unidades policiales.

La información entregada por el Consorcio TRACK confirma y matiza este diagnóstico. Por un lado, aporta datos que sí permiten un cierto nivel de evaluación: series trimestrales desagregadas por tipo de alerta, fechas específicas de capacitación con cantidad de personal formado por jornada (por ejemplo, 37 operadores el 09/01/2025, 38 el 10/01/2025, y así sucesivamente hasta el 21/02/2025, sumando varios cientos de instancias de formación), contenidos de los programas de capacitación (operación general del sistema, gestión de alarmas, administración de beneficiarios, configuración de geocercas, asignación de dispositivos UMA, ejecución de comandos remotos, generación de reportes) y descripción de mejoras implementadas tras el primer año de ejecución, tales como la "reducción de los tiempos de respuesta mediante la aplicación de criterios de priorización y atención inmediata".

Por otro lado, esa misma información deja en evidencia los vacíos: si bien se informa que hubo una "optimización en la gestión de alarmas" y una "reducción de los tiempos de respuesta", no se adjuntan tiempos medios concretos, ni tablas comparativas antes/después, ni indicadores estandarizados de desempeño. El protocolo establece que, ante una alarma, el operador debe actuar con "la mayor celeridad posible", pero no fija un estándar numérico de tiempo de respuesta. Tampoco se incorporan, por ejemplo, informes consolidados sobre tiempos concretos de despacho policial, porcentaje de alertas confirmadas como verdaderas respecto del total, o indicadores comparables entre trimestres. La mención de capacitación "constante" se concreta para 2025, pero no se detalla qué ocurrió en 2026 ni cómo se evalúa su impacto.

El caso de las alarmas clasificadas como "falsas" es particularmente ilustrativo de esta asimetría. El Consorcio explica que estas se originan "principalmente como consecuencia de las limitaciones inherentes a las tecnologías de geolocalización", y que el fabricante recomienda un radio mínimo de 40 metros para delimitar las zonas de inclusión. Sin embargo, en la operativa actual las áreas se configuran "conforme a lo establecido en los oficios judiciales correspondientes", aun cuando estas puedan diferir de las recomendaciones técnicas del fabricante. Este desajuste entre parámetros técnicos recomendados y parámetros judiciales efectivamente aplicados no aparece discutido públicamente en ningún otro documento institucional, y ayuda a explicar por qué, de decenas de miles de alertas registradas, apenas 5 se consideraron violaciones efectivas de la medida durante el primer trimestre de 2026. Dicho de otro modo: la enorme mayoría de las alarmas del sistema son ruido técnico producido por el propio diseño de la medida judicial, y ese ruido no se reporta de manera pública bajo indicadores comparables, sino que queda como nota al pie en una respuesta tardía de un proveedor privado.

Este desfase entre capacidad de vigilancia y capacidad de rendición de cuentas es uno de los hallazgos más significativos de la investigación. El sistema parece estar mejor preparado para registrar personas monitoreadas, trayectorias y eventos que para ofrecer indicadores públicos robustos sobre su propia eficacia, sus límites y sus fallas. Desde una perspectiva crítica, esta asimetría es especialmente relevante porque muestra que la expansión de infraestructura no vino acompañada, al menos hasta donde fue posible relevar, por una expansión equivalente de transparencia democrática.

7.7. Del diagnóstico local a la perspectiva comparada: por qué mirar otras experiencias antes de recomendar

Los hallazgos presentados hasta aquí permiten dimensionar, con datos propios y voces institucionales paraguayas, cómo opera efectivamente el SIMDEC en su primer año de funcionamiento consolidado. Emerge una imagen consistente: un sistema cuya implementación está condicionada por la infraestructura material, que produce volúmenes masivos de información sin marcos equivalentes de rendición de cuentas, que incorpora a las víctimas dentro del circuito de vigilancia bajo el supuesto de "protección", que depende de un proveedor privado y que opera sobre una base de desigualdades territoriales, económicas y digitales que el propio dispositivo no puede corregir. Esta evidencia empírica, leída junto al análisis normativo previo, deja planteados interrogantes sustantivos sobre las condiciones institucionales, materiales y de gobernanza de derechos humanos que el sistema aún no tiene resueltas.

Ahora bien, antes de avanzar hacia recomendaciones concretas, esta investigación considera necesario abrir un apartado de análisis comparado internacional. Esta decisión metodológica responde a una apuesta argumentativa específica. En primer lugar, porque los propios antecedentes legislativos del SIMDEC recurrieron a la experiencia internacional para justificar su implementación. Si desde Paraguay se invoca modelos externos como fundamento para adoptar esta tecnología, resulta coherente revisar críticamente alguno de estos modelos para evaluar qué promesas cumplieron, cuáles fracasaron y qué tensiones estructurales reprodujeron.

En segundo lugar, porque varios de los problemas identificados como hallazgos en Paraguay —la dependencia de infraestructura eléctrica y conectividad, el volumen masivo de falsas alarmas, la opacidad en la gobernanza de datos, la redistribución de cargas técnicas hacia las víctimas, la dependencia de proveedores privados, la expansión impulsada por inercia contractual— no son particularidades locales. Son patrones recurrentes que otros países ya transitaron, en algunos casos durante más de una década. Argentina, Brasil, Uruguay y España ofrecen trayectorias con distintos grados de madurez institucional, marcos normativos más consolidados y, aun así, fallas estructurales documentadas que incluyen femicidios con agresores bajo monitoreo activo, pérdidas de datos históricos durante transiciones contractuales, sobreseimientos judiciales por fallas probatorias de los dispositivos y expansión cuantitativa sin mecanismos de evaluación. Analizar esas experiencias permite anticipar riesgos que, en el caso paraguayo, todavía no se han materializado pero resultan plausibles bajo las mismas condiciones estructurales.

En tercer lugar, porque formular recomendaciones sin esta capa comparada correría el riesgo de derivar en un ejercicio voluntarista o meramente normativo. La evidencia internacional aporta algo que el análisis local no puede aportar por sí solo: una visión longitudinal sobre cómo evolucionan estos sistemas una vez instalados, qué respuestas institucionales han sido insuficientes, qué reformas legales llegaron tarde, y qué lecciones transversales emergen cuando distintos Estados enfrentan problemas similares con recursos y marcos institucionales diversos. Recomendar sin ese telón de fondo sería recomendar a ciegas. En cuarto lugar, porque Paraguay se encuentra en una fase temprana y todavía moldeable de implementación. Esa oportunidad institucional es, paradójicamente, una ventaja analítica: permite identificar condiciones mínimas y salvaguardas antes de que el sistema cristalice con sus fragilidades, y aprender de errores que otros países ya cometieron y documentaron. La comparación, entonces, no busca trasplantar modelos, advertencia que la evidencia misma desaconseja, sino extraer umbrales de viabilidad institucional que permitan evaluar qué tan preparado está el Estado paraguayo para sostener la promesa tecnológica que ha adoptado.

Por último, la decisión de anteponer el análisis comparado a las recomendaciones también responde a una opción política del enfoque de esta investigación: evitar que las sugerencias aparezcan como propuestas aisladas, desconectadas de evidencia internacional, o vulnerables a la objeción de que "en otros países funciona". Al poner en diálogo los hallazgos empíricos paraguayos con las experiencias comparadas, las recomendaciones que se formularán en el apartado siguiente podrán anclarse tanto en lo que ocurre efectivamente dentro de Paraguay como en lo que la evidencia regional y europea ya documentó sobre las condiciones mínimas sin las cuales el monitoreo electrónico en contextos de violencia de género tiende a producir resultados inconsistentes o, incluso, contraproducentes.

Con ese objetivo, el apartado que sigue examina cuatro casos seleccionados: Argentina, Brasil, Uruguay y España, buscando identificar condiciones de efectividad, patrones de fallo recurrente y tensiones estructurales anticipables. No se trata de presentar un modelo ideal, sino de reconstruir un mapa de experiencias desde el cual leer, en perspectiva crítica, las posibilidades y los límites del SIMDEC paraguayo.

Análisis comparado internacional: lecciones, fallas y tensiones en perspectiva comparada.

Según los propios antecedentes legislativos, que recurrieron a la comparación internacional para apelar a la necesidad de implementación del sistema de monitoreo, este análisis comparado tiene por objetivo identificar condiciones de efectividad, patrones de fallo recurrente y tensiones estructurales que resultan anticipables cuando se introduce el monitoreo electrónico en sistemas judiciales y de seguridad.

Los países seleccionados para el análisis comparado —Argentina, Brasil y Uruguay en el contexto regional, y España en el europeo— presentan trayectorias diversas en la implementación del monitoreo electrónico: algunos con más de una década de experiencia acumulada, otros con despliegues recientes y evaluaciones aún en curso[67]. En todos los casos, la evidencia disponible advierte sobre la brecha entre la promesa tecnológica y la capacidad institucional real para sostenerla.

Como se sostuvo en apartados más arriba, tanto de la literatura y de la evidencia empírica disponible surge que el monitoreo electrónico no constituye, por sí mismo, una medida de protección. Su eficacia —en el sentido de reducción efectiva de riesgo para víctimas— depende de condiciones externas al dispositivo: respuesta operativa del Estado, coordinación interinstitucional, recursos humanos capacitados, protocolos claros ante alertas, y marcos de gobernanza sobre los datos recolectados. Sin estas condiciones, al menos lo que emerge del estudio de casos a nivel internacional, es que la tecnología puede generar una falsa sensación de seguridad y no de protección material efectiva (Erez et al., 2012).

67 La selección de estos cuatro países responde a criterios metodológicos combinados. En el caso de Argentina, Brasil y Uruguay, la proximidad jurídica e institucional con Paraguay, es decir, son sistemas de derecho continental, marcos regionales compartidos como la Convención de Belém do Pará, y desafíos estructurales similares en términos de capacidad estatal, brecha digital y violencia de género, lo que hace que sus experiencias sean relevantes para identificar condicionantes transferibles. Uruguay merece especial atención por haber sido referencia explícita en el diseño institucional del SIMDEC, según surge de las entrevistas realizadas en el marco de esta investigación. Brasil se incluye además por la escala y la densidad normativa de su sistema, que permite observar con mayor detalle los efectos de la expansión acelerada. España fue incorporada por tratarse del sistema europeo con mayor desarrollo en la integración de monitoreo electrónico y evaluación de riesgo en violencia de género, y por operar bajo un marco de referencia en materia de gobernanza de datos. Se excluyeron deliberadamente países como Australia o Reino Unido —relevantes en la literatura especializada— por presentar condiciones institucionales, tradiciones jurídicas y niveles de desarrollo de infraestructura difícilmente comparables con Paraguay en esta etapa de la investigación. Estados Unidos, si bien pionero en el uso de GPS en violencia doméstica, no fue incluido como caso comparado por su marcada descentralización y tradición punitiva, aunque sí se utilizan hallazgos de su literatura académica como evidencia de respaldo teórico en el marco conceptual.

Argentina: dispositivos duales, adquisiciones y desafíos de coordinación

En Argentina, el sistema de monitoreo electrónico en casos de violencia de género se implementó de forma relativamente temprana, con experiencias piloto en la Ciudad Autónoma de Buenos Aires y posterior extensión provincial. El modelo adoptado privilegia el llamado "dispositivo dual" (Gobierno de Argentina, 2021), que implica la utilización simultánea de un dispositivo por parte de la persona agresora y otro orientado a la víctima, permitiendo calcular en tiempo real la distancia entre ambas partes y disparar alertas cuando se viola la zona de exclusión (UNFPA Argentina, 2023).

Sin embargo, la implementación se caracteriza por una institucionalidad segmentada. Si bien el Estado nacional interviene en la adquisición y distribución inicial de los dispositivos, la gestión operativa, el monitoreo y los protocolos de respuesta recaen en las provincias. Esta configuración genera una implementación heterogénea, con diferencias significativas en disponibilidad, capacidad de monitoreo y estándares técnicos entre jurisdicciones, lo que dificulta tanto la evaluación comparada del sistema como la garantía de estándares mínimos de protección uniformes (UNFPA Argentina, 2023).

A nivel operativo, el relevamiento nacional sobre dispositivos de protección identifica limitaciones estructurales que afectan la eficacia del sistema: problemas de conectividad, fallas en la señal, cobertura territorial desigual y debilidades en la articulación interinstitucional —especialmente entre fuerzas de seguridad, poder judicial y organismos especializados en violencia de género (UNFPA Argentina, 2023)—. Estas condiciones inciden directamente en la capacidad de respuesta ante alertas, particularmente en contextos con menor infraestructura tecnológica. El funcionamiento del sistema también ha sido objeto de debate público en torno a su eficacia. Se han documentado casos de vulneración del sistema[68], e incluso femicidios con agresor portando dispositivo activo[69], lo que generó motivó revisiones protocolares[70]. Más allá de los casos extremos, la evidencia empírica muestra que el uso de dispositivos duales no elimina la sensación de inseguridad ni las restricciones en la vida cotidiana de las personas usuarias, quienes continúan asumiendo cargas operativas y emocionales significativas asociadas a su funcionamiento (Paz-Ruíz, 2025). La respuesta predominante del debate público ha tendido a centrarse en mejoras técnicas y ampliación de cobertura (Sohr, 2019; Carbajal, 2021), mientras que desde perspectivas críticas se ha señalado que estas respuestas sobredimensionan la dimensión tecnológica en detrimento de un enfoque integral de protección: el monitoreo electrónico puede amplificar la visibilidad del riesgo sin garantizar su reducción efectiva.

En cuanto a la dimensión contractual, la descentralización del sistema argentino genera una diversidad de esquemas de adquisición y gestión entre jurisdicciones que dificulta el establecimiento de estándares homogéneos de control sobre aspectos críticos como interoperabilidad, continuidad del servicio y seguridad de la información. Se han documentado controversias públicas sobre costos, condiciones de adjudicación y transparencia en la selección de proveedores (Dolabjian, 2025), lo que evidencia que la dimensión contractual no es neutra: incide directamente en la calidad del servicio, la dependencia tecnológica y la sostenibilidad del sistema. Esta dimensión no es ajena al caso paraguayo, donde las adjudicaciones también han sido objeto de cuestionamientos públicos, aunque con menor visibilidad (ABC Color, 2024).

---

68 Cadena 3. (2026, marzo 24). *Rauch: un hombre rompió su tobillera y secuestró a su ex pareja*. Recuperado el 14 de abril de 2026, de https://www.cadena3.com/noticia/sociedad/rauch-un-hombre-rompio-su-tobillera-y-secuestro-a-su-ex-pareja_532837

69 Fahsbender, F. (2025, julio 28). Femicidio en Berisso: la víctima y el asesino tenían tobilleras electrónicas. Infobae. Recuperado el 14 de abril de 2026, de https://www.infobae.com/sociedad/policiales/2025/07/27/femicidio-en-berisso-la-victima-y-el-asesino-tenian-tobilleras-electronicas/

70 Un caso paradigmático es el de Carla Soggiu, quien, a pesar de contar con un botón de pánico como medida de protección, no recibió asistencia oportuna debido a fallas en el sistema de geolocalización, lo que impidió su correcta activación y contribuyó a que fuera posteriormente asesinada por su expareja. Observatorio Lucía Pérez. (s. f.). Carla Soggiu. Recuperado el 14 de abril de 2026, de https://observatorioluciaperez.org/femicidios/carla-soggiu/

Finalmente, el sistema produce flujos continuos de datos de geolocalización en tiempo real, históricamente acumulables y potencialmente reveladores de patrones de comportamiento (UNFPA Argentina, 2023). Si bien no se han documentado de manera sistemática brechas públicas específicas vinculadas a estos sistemas en Argentina, los estándares regulatorios vigentes[71] reconocen que este tipo de información constituye una categoría de datos altamente sensible, cuyo tratamiento exige garantías reforzadas en términos de acceso, seguridad y finalidad (AAIP, 2021). La fragmentación institucional y la participación de proveedores privados en la operación del sistema amplifican estos riesgos al dificultar la trazabilidad del uso de los datos y debilitar los mecanismos de supervisión —riesgo que incrementa ante la falta de auditoría efectiva sobre quién accede a la información, en qué condiciones y con qué finalidad—. El caso argentino ilustra así que los desafíos del monitoreo electrónico no se limitan a la eficacia del dispositivo, sino que se extienden a la gobernanza de los datos que produce.

Brasil: expansión acelerada y fragilidades estructurales

Otro caso regional relevante que considerar es el de Brasil, que presenta uno de los despliegues más extensos de monitoreo electrónico en la región, tanto en materia penitenciaria como en violencia doméstica. La escala del sistema brasileño importa cientos de miles de personas bajo monitoreo electrónico en distintas modalidades (CNJ, 2022). Sin embargo, esa escala convive con fragilidades institucionales que cuestionan la efectividad real del modelo, y el Estado brasileño respondió con un proceso de reforma normativa que merece atención específica.

El marco legal brasileño, anclado en la Ley N.º 11.340/2006 (conocida como Ley María da Penha[72]), establece un conjunto robusto de medidas de protección para víctimas de violencia doméstica. Las reformas introducidas por la Ley N.º 13.871/2019 incorporaron explícitamente el monitoreo electrónico como medida cautelar aplicable a agresores (art. 1) pero con carácter optativo: el juez podía disponerlo, no estaba obligado a hacerlo. Esta lógica fue modificada progresivamente por dos reformas recientes que representan un salto cualitativo en el modelo brasileño.

En primer lugar, la Ley N.º 5.125/2025 autorizó expresamente el uso del monitoreo electrónico del agresor y la provisión de un dispositivo de alerta a la víctima ante aproximación indebida, dotando de mayor efectividad a las medidas protectoras de urgencia. En segundo lugar, la más reciente, Ley N.º 15.383/2026[73], que establece el monitoreo electrónico de agresores como medida protectora autónoma, fija criterios de prioridad para su aplicación, crea una agravante penal por incumplimiento de medidas protectoras, y torna permanente el programa de monitoreo (arts. 1–4). Esta última norma introduce además una habilitación de relevancia práctica para contextos de baja institucionalidad judicial: los delegados de policía podrán ordenar el uso de tobillera en localidades sin sede judicial, con obligación de comunicación al juez en 24 horas para confirmar o revocar la medida. La determinación de uso es inmediata cuando exista riesgo para la vida o integridad física o psicológica de la mujer o sus dependientes.

---

71 Argentina cuenta con la Ley 25.326 de Protección de Datos Personales y, más recientemente, con debates legislativos orientados a actualizar ese marco a estándares del Reglamento General de Protección de Datos de la Unión Europea (RGPD). Esto implica que, en el contexto del monitoreo electrónico, la normativa resulte aplicable al establecer que los datos de geolocalización son datos sensibles y su tratamiento requiere finalidades específicas, plazo de retención definido y salvaguardas contra usos secundarios (Ley 25.326/2000, art. 2 y 7; AAIP, 2021).

72 Esta ley recibe su nombre en referencia al caso de Maria da Penha Maia Fernandes, víctima de violencia doméstica durante más de dos décadas, que incluyó dos intentos de asesinato por parte de su entonces esposo, dejándola parapléjica. Ante la falta de respuesta efectiva del sistema judicial brasileño, el caso fue llevado ante la CIDH, que responsabilizó al Estado por omisión y tolerancia frente a la violencia de género. Este proceso generó presión internacional que derivó en la adopción de la ley en 2006, considerada una de las más avanzadas en la región (Wikipedia. (s. f.). *Ley Maria da Penha (Brasil)*. Recuperado el 14 de abril de 2026, de https://es.wikipedia.org/wiki/Ley_Maria_da_Penha_(Brasil)).

73 Para acceder al texto de la ley ver: Brasil. (2026, abril 9). *Lei N.º 15.383, de 9 de abril de 2026*. Recuperado el 14 de abril de 2026, de https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2026/Lei/L15383.htm

Estas reformas, además, incluyen iniciativas como el Projeto Alerta Mulher Segura, impulsado por el Ministério da Justiça e Segurança Pública (MJSP), y el Pacto Nacional Brasil contra o Feminicídio[74]. En particular, cabe mencionar que, el Projeto Alerta Mulher Segura refleja una tendencia hacia la profundización del uso de tecnologías de monitoreo, incorporando dispositivos también para las víctimas —por ejemplo, relojes inteligentes capaces de emitir alertas en tiempo real ante la proximidad del agresor[75]— integrados con las tobilleras electrónicas y los sistemas de respuesta de seguridad (Ministério da Justiça e Segurança Pública, 2026). En términos generales, estas políticas sugieren que la respuesta institucional ha tendido a orientarse hacia la expansión de la infraestructura tecnológica de vigilancia, lo que plantea interrogantes sobre el equilibrio entre innovación tecnológica y desarrollo de mecanismos integrales de protección.

Este encuadre normativo actualizado es más claro que el paraguayo en cuanto a la finalidad protectora del dispositivo, su articulación con el sistema de justicia y la definición de criterios de prioridad. No obstante, la distancia entre la norma y la práctica es una arista que no puede desconocerse (Valadão & Freitas Lima, 2025). Ante tal escenario, las fallas documentadas en el sistema brasileño operan en tres niveles (CNJ, 2023). Primero, a nivel técnico: dispositivos con baterías deficientes, fallos de señal en zonas con cobertura limitada y ausencia de mantenimiento adecuado; el propio relatorio advierte que muchas violaciones registradas como incumplimientos responden en realidad a problemas técnicos del dispositivo, y que el monitoreo no puede implementarse en todo el territorio por limitaciones de señal GPS (CNJ, 2023, p. 109). Segundo, a nivel operativo: centros de monitoreo con personal insuficiente para acompañar el volumen de casos activos; al momento de la Conferencia Internacional, Brasil contaba con 91.362 personas bajo monitoreo y la SENAPPEN estimaba que se necesitaban más de 1.500 profesionales adicionales para un acompañamiento adecuado, mientras que 11 estados aún no contaban con equipos multidisciplinares (CNJ, 2023, p. 77). Tercero, a nivel institucional: ausencia de protocolos uniformes sobre qué instancia responde ante una alerta y en qué tiempo; el relatorio documenta que cada estado clasifica un mismo incidente de formas distintas —desde enfoques que priorizan derechos humanos hasta enfoques más policiales—, lo que el propio sistema identifica como uno de sus principales desafíos pendientes (CNJ, 2023, p. 77).

Ahora bien, respecto de este último nivel, si bien la literatura ha identificado déficits estructurales en la coordinación interinstitucional y en la gestión de alertas, desarrollos normativos más recientes en Brasil han buscado subsanar estas falencias mediante el fortalecimiento de los protocolos de actuación y la delimitación más precisa de competencias entre las autoridades involucradas, con énfasis en la respuesta inmediata ante situaciones de riesgo y la articulación entre órganos judiciales, policiales y de persecución penal (Brasil, 2026). No obstante, la evidencia disponible sugiere que persisten desafíos en la implementación efectiva de estos mecanismos, especialmente en contextos de limitaciones operativas y desigualdades en la infraestructura. Las fallas también quedan expuestas al darse casos de femicidio con agresor bajo monitoreo activo, lo que es un hecho documentado en Brasil y ha motivado investigaciones parlamentarias que concluyen, invariablemente, que el dispositivo sin respuesta eficiente es inútil (Senado Federal do Brasil, 2021).

---

74 Estas medidas deben leerse a la luz de la magnitud del fenómeno, dado que según datos del Painel de Estatística do Conselho Nacional de Justiça (CNJ), solo en 2025 se concedieron más de 600.000 medidas protectivas en el país, lo que equivale a un promedio de aproximadamente 70 por hora (MJSP, 2026). Sin embargo, la elevada cantidad de medidas dictadas no se traduce automáticamente en una protección efectiva, ya que persisten los altos niveles de femicidio —incluyendo casos en los que las víctimas contaban previamente con medidas de protección (12,7 %)— lo que muestra limitaciones en su implementación y cumplimiento.

75 Según reportes oficiales, se trata de un proyecto que integra la tobillera electrónica del agresor con un dispositivo digital, tipo reloj inteligente, asignado a la víctima. Este sistema permite monitoreo en tiempo real y activa alertas automáticas ante la aproximación indebida, implicando un esquema de geolocalización continua de la víctima. La iniciativa evidencia la expansión del modelo de vigilancia tecnológica hacia dispositivos duales con seguimiento permanente.

En tal contexto, la evidencia confirma que la tobillera por sí sola no resuelve, sino que requiere de un sistema de monitoreo y respuesta eficiente y expeditivo. Además, cuando va acompañada de apoyo psicológico, orientación jurídica, visitas de seguimiento y vigilancia preventiva, la protección se vuelve sustancialmente más efectiva. La propia Ley N.º 15.383/2026 reconoce implícitamente esta tensión al establecer que el monitoreo no debe considerarse una solución autónoma o aislada, sino parte de una red de protección estructurada que incluya soporte jurídico, psicológico, social e institucional.

En cuanto a la gobernanza de datos, Brasil cuenta con la Lei Geral de Proteção de Dados (LGPD, Ley N.º 13.709/2018), equivalente funcional al RGPD europeo. La ley clasifica los datos de geolocalización como datos personales sujetos a protección reforzada cuando revelan patrones de comportamiento o permiten inferencias sobre la vida privada (LGPD, art. 5, incs. I y II; art. 11). En el contexto del monitoreo electrónico, los datos generados son altamente sensibles: revelan rutinas, lugares frecuentados, redes relacionales, y pueden ser utilizados —en ausencia de controles— para vigilancia extrajudicial, revictimización o estigmatización del imputado. La LGPD establece bases legales específicas para el tratamiento de datos por parte del Estado, incluyendo el interés público y la seguridad, pero exige proporcionalidad y limitación de finalidad (LGPD, art. 23).

Al respecto, además, el Consejo Nacional de Justicia, en su resolución CNJ N.º 412/2021[76] establece que los datos recolectados en el monitoreo tienen finalidad específica y acceso restringido (art. 13); además, los sistemas deben preservar el sigilo de la persona monitoreada[77], de la mujer en situación de violencia y de terceros. La misma resolución dispone que el compartimiento de datos con órganos de seguridad pública depende de autorización judicial (art. 13, §2), salvo supuestos excepcionales de riesgo inminente, en cuyo caso debe quedar registro formal del acceso para control y eventual auditoría. Asimismo, prevé un plazo de conservación de los datos de seis meses tras la finalización de la medida, así como el derecho de acceso del titular a la información generada durante el monitoreo (art. 13). Así, más que un vacío normativo en materia de protección de datos, el desafío brasileño reside en la traducción efectiva de estas reglas en prácticas institucionales uniformes, particularmente en términos de trazabilidad, supervisión y rendición de cuentas.

Las sucesivas respuestas normativas brasileñas subrayan una lección que no se puede ignorar, y es que no alcanza con legislar. El monitoreo electrónico exige evaluación crítica continua, con relevamiento sistemático de datos y revisión periódica de su impacto real sobre las personas involucradas. Además, en materia de protección de datos, el modelo brasileño es ilustrativo en cuanto a que los datos derivados del monitoreo electrónico —en particular la geolocalización en tiempo real— son datos especialmente sensibles que exigen garantías estrictas de sigilo, autorización judicial para su acceso y trazabilidad de cada consulta. Este aporte es bastante relevante, en particular, considerando esquemas de implementación que involucran a proveedores privados, la integración de bases de datos entre múltiples actores estatales y arreglos contractuales en los que personal de empresas externas puede acceder al sistema, el riesgo de sobreexposición, dependencia tecnológica y debilitamiento del control público sobre la información. Paraguay, por ejemplo, enfrenta este mismo escenario en condiciones institucionales aún más precarias.

---

76 Para acceder al texto de la resolución, ver: Conselho Nacional de Justiça (Brasil). (2021, agosto 25). *Resolução N.º 412/2021, que dispõe sobre o monitoramento eletrônico de pessoas*. Recuperado el 14 de abril de 2026, de https://atos.cnj.jus.br/files/original004748202108256125933 4b9264.pdf

77 Este tipo de consideraciones de prevención y seguridad responden al riesgo estructural de sobreexposición derivado de la circulación de datos sensibles entre múltiples actores. De nuestra investigación, no surge que en Paraguay se verifiquen mecanismos uniformes como términos formales de tratamiento y protección de datos para todos los operadores, lo que subraya la necesidad de sigilo y control del acceso a la información que se procesa.

Uruguay: modelo orientado a víctimas y coordinación interinstitucional

Uruguay constituye uno de los casos más tempranos y sistemáticos en América Latina en la implementación de monitoreo electrónico en contextos de violencia de género. A diferencia de otros países donde estas tecnologías fueron adaptadas desde el ámbito penal general, el sistema uruguayo se desarrolló progresivamente en articulación con políticas públicas específicas en materia de violencia doméstica, en el marco del Plan Nacional de Lucha contra la Violencia Doméstica (MIDES, 2010). Esta orientación influyó directamente en el diseño institucional paraguayo. Actores clave del Poder Judicial han reconocido que el SIMDEC tomó como referencia el modelo uruguayo en su concepción inicial, aunque su desarrollo normativo posterior derivó en una arquitectura más amplia y menos focalizada en la protección de víctimas (Luraghi Sarubbi, entrevista, 2026). En este sentido, el caso uruguayo es relevante como modelo de referencia declarado y como espejo en el que observar la distancia entre el diseño original y la implementación efectiva.

En términos operativos, el sistema uruguayo se basa en dispositivos duales; es decir, una tobillera electrónica para el agresor y un dispositivo GPS asignado a la víctima, permitiendo calcular en tiempo real la distancia entre ambas partes y activar alertas ante violaciones de zona de exclusión. El ingreso al programa requiere evaluación de riesgo y orden judicial previa. La Dirección de Monitoreo Electrónico (DIMOE) es responsable de la instalación, desconexión y monitoreo permanente las 24 horas, articulada con el Centro de Comando Unificado (CCU) del Ministerio del Interior para la gestión de las coordinaciones operativas (Ministerio del Interior, Uruguay, 2020). Al ingresar al programa, ambas partes firman un acuerdo contractual sobre el uso de los dispositivos y son entrevistadas sobre su situación (Ministerio del Interior [Uruguay], s. f.). En efecto, este modelo dual implica que el número de personas monitoreadas excede al de dispositivos instalados, ya que cada caso involucra necesariamente a dos partes, la agresora y la víctima.

Una de las características más destacadas es su nivel de coordinación interinstitucional[78], con protocolos que establecen responsabilidades y flujos de información definidos entre el Poder Judicial, el Ministerio del Interior y organismos especializados en género (MIDES, 2019) . El protocolo del Área de Violencia de Género del CCU establece, además, obligaciones explícitas de confidencialidad: todo el personal debe prestar declaración jurada sobre la información relevada, bajo responsabilidad expresa y con notificación de las sanciones aplicables Ministerio del Interior [Uruguay], s. f.). Esta estructura reduce, en comparación con otros contextos regionales, la ambigüedad sobre quién debe actuar ante una alerta y bajo qué responsabilidad.

Asimismo, en términos formales, los protocolos analizados y la actuación de instituciones como el Ministerio de Desarrollo Social (MIDES) y el Instituto Nacional de las Mujeres (Inmujeres) sugieren la existencia de un enfoque orientado a la articulación del monitoreo electrónico con servicios de acompañamiento integral. No obstante, la evidencia disponible indica que el sistema continúa enfrentando tensiones estructurales propias de este tipo de tecnologías en la región. En particular, si bien se prevén mecanismos

78 La Resolución Ministerial B-1956 (2010) del Ministerio del Interior de Uruguay creó una Comisión de Trabajo Interinstitucional encargada de estudiar y asesorar sobre la implementación de mecanismos de protección para víctimas de violencia doméstica, incluyendo la evaluación del uso de tecnologías de verificación de presencia y localización (tobilleras electrónicas). Esta comisión, integrada por representantes del Poder Judicial, la Bancada Bicameral Femenina, el Instituto Nacional de las Mujeres (Inmujeres/MIDES) y la Red Uruguaya contra la Violencia Doméstica y Sexual, definió el marco inicial para la incorporación de dispositivos de monitoreo electrónico y delimitó las competencias institucionales.

de asistencia complementaria —como refugios, atención psicosocial y apoyo legal—[79], esta investigación identificó limitaciones en el acceso a información sistematizada sobre su funcionamiento en la práctica, especialmente en relación con tiempos de respuesta y resultados en casos concretos, lo que dificulta evaluar en qué medida el monitoreo electrónico se integra efectivamente con dichos servicios.

Ahora bien, todo este sistema, considerado como medida de protección, muestra una expansión significativa desde sus primeras consideraciones en el 2010. Según los indicadores presentados por el Ministerio del Interior en noviembre de 2025, el programa de tobilleras —operativo en todo el país desde 2017— registró un incremento superior al 1.000 % en los casos atendidos, pasando de 691 a 3.739 casos. Las mujeres representan 9 de cada 10 víctimas y los agresores 9 de cada 10 varones. Entre enero y octubre de 2025 se registraron 817 denuncias por retiro o destrucción de dispositivos, de las cuales 111 resultaron en formalización o condena por desacato (Ministerio del Interior, Uruguay, 2025). Es decir, esta expansión no está exenta de tensiones.

De hecho, sobre el punto, un relevamiento del propio Ministerio del Interior detectó que aproximadamente 250 de las 2.100 tobilleras disponibles para violencia doméstica estarían siendo utilizadas de forma "dudosa": casos de personas que se fueron del país, otras que portan el dispositivo desde hace más de dos años cuando lo recomendado es no extender la medida más de seis meses, e incluso personas que cargan simultáneamente dos tobilleras —una como agresor y otra como víctima, por dos relaciones distintas— (Tapia, 2025). Este hallazgo ilustra un problema recurrente en la evidencia comparada: la expansión cuantitativa no va necesariamente acompañada de mecanismos de evaluación y revisión que garanticen la pertinencia de cada caso activo. Cabe señalar, además, que esta investigación no ha identificado en las fuentes disponibles un protocolo público específico que establezca criterios para la categorización de los casos según nivel de riesgo —alto, medio o bajo—. En la práctica, esta determinación parecería quedar principalmente en el ámbito de la valoración judicial.

Por otra parte, también se comprueba en este caso analizado que la respuesta a los límites del sistema vigente, es más tecnología. A finales de 2025, el Ministerio del Interior presentó Élida 360, un dispositivo complementario que opera en los celulares de mujeres víctimas para cuyo agresor existen medidas cautelares de no acercamiento, dirigido a casos catalogados de riesgo medio o bajo una vez finalizado el seguimiento mediante tobillera (Ministerio del Interior, Uruguay, 2025). El dispositivo, que inició como plan piloto en Montevideo con 500 unidades a partir del 22 de diciembre de 2025, requiere resolución judicial previa, opera mediante biometría facial para garantizar acceso exclusivo de la víctima, e incorpora botón de emergencia, chat 24 horas y posibilidad de ampliar denuncia sin concurrir a la comisaría (Ministerio del Interior, Uruguay, 2025). El presupuesto quinquenal prevé una partida anual de 55 millones de pesos uruguayos para el arrendamiento de dispositivos a partir de 2027, con intención de sumar 1.000 unidades adicionales a los 2.300 equipos activos (Demirdjian, 2025).

79 En el caso paraguayo, la investigación no logró identificar ninguna consideración de esta naturaleza en el diseño institucional del SIMDEC. El único componente del sistema orientado específicamente a la víctima es la entrega voluntaria del dispositivo UMA —un teléfono celular con la aplicación Empower—, que incluye botón de pánico y comunicación directa con la OMDEC. Si bien la representante del Poder Judicial indicó que el Estado provee el dispositivo y los datos (Luraghi, entrevista, 2026), el representante del Ministerio de Defensa Pública advirtió que, en la práctica, la víctima debe mantener internet o datos móviles activos de forma permanente para que el sistema funcione, identificando esto como una barrera económica real (Prates, entrevista, 2026). Ante una alarma, la única interacción del sistema con la víctima consiste en contactarla para alertarla sobre la proximidad del agresor y brindarle "orientaciones de autoprotección" (Protocolo SIMDEC, 2024). No se relevó ninguna previsión relativa a casas refugio, acompañamiento psicosocial, asistencia legal autónoma o reinserción económica articulada al funcionamiento del sistema. El Ministerio de la Mujer, institución con competencia específica en estas materias, respondió a la solicitud de acceso a información pública de esta investigación con información general e institucional, sin remitir documentación técnica sobre mecanismos de acompañamiento integral vinculados al SIMDEC.

El patrón que ilustra Élida 360 es significativo para el análisis comparado, ya que no se proyecta como revisión del modelo de protección integral, sino un dispositivo adicional que amplía la vigilancia y los datos recolectados sobre la víctima. El operador accede ahora, en tiempo real, no solo a su ubicación sino también a sus datos personales, información del agresor y contactos de confianza (Ministerio del Interior, Uruguay, 2025). Ante esto, surge la pregunta sobre quién controla esos datos y con qué garantías permanece abierta, incluso en un sistema con marco normativo más consolidado que el paraguayo.

Por último, en cuanto a materia de gobernanza de datos, Uruguay cuenta con un marco normativo consolidado en materia de protección de datos personales a partir de la Ley N.º 18.331 de 2008, reglamentada por Decreto N.º 414 de 2009[80], y la actuación de la Unidad Reguladora y de Control de Datos Personales (URCDP). No obstante, el propio artículo 3 de dicha ley excluye de su ámbito de aplicación a las bases de datos vinculadas a la seguridad pública, la investigación penal y la represión del delito, lo que resulta directamente relevante para los sistemas de monitoreo electrónico.

Esta exclusión no implica la ausencia de regulación, sino la sujeción a regímenes específicos y a principios generales de protección de derechos fundamentales. En este contexto, los protocolos judiciales e institucionales refuerzan la limitación de finalidad al establecer que la información generada por el sistema solo puede utilizarse en relación con la medida cautelar dispuesta. Asimismo, el carácter interinstitucional del sistema —que involucra no solo a autoridades de seguridad, sino también a organismos de asistencia a víctimas y, potencialmente, a proveedores privados— plantea interrogantes sobre la aplicación diferenciada de estándares de protección de datos dentro de un mismo esquema operativo. En este sentido, si bien no se identifican pronunciamientos específicos de la URCDP sobre estos sistemas, el marco uruguayo ofrece condiciones robustas de estructuración institucional superiores a las observadas en el caso paraguayo, donde los estándares de protección aún se encuentran en proceso de consolidación.

España: fallas sistémicas, gobernanza y límites del enfoque tecnosolucionista

España es referencia obligada en cualquier análisis comparado sobre tecnología y violencia de género, tanto por la escala de su sistema como por las tensiones que ha generado su evolución hacia modelos predictivos y algorítmicos. El sistema español combina el monitoreo electrónico con un sistema de evaluación y gestión del riesgo denominado VioGén[81], administrado por el Ministerio del Interior (Ministerio del Interior, España, 2019).

El monitoreo electrónico en España se implementa a través del sistema COMETA (Control y Observación de Medidas y Penas Alternativas), que incluye dispositivos GPS para agresores condenados o sujetos a medidas cautelares (Secretaría General de Instituciones Penitenciarias, 2018). España tiene una de las coberturas más amplias de monitoreo electrónico en violencia de género en Europa, con miles de dispositivos activos simultáneamente. El sistema opera bajo la coordinación del Centro Nacional de Control del Seguimiento Telemático (CNCST).

---

80 Para ver el texto de la ley: Uruguay. (2008). Ley N.º 18.331 de protección de datos personales y acción de habeas data. Recuperado el 18 de abril de 2026. https://www.impo.com.uy/bases/leyes/18331-2008

81 VioGén es el Sistema de Seguimiento Integral en los casos de Violencia de Género implementado en España, que incorpora herramientas de valoración del riesgo, incluyendo componentes algorítmicos, para la gestión y protección de víctimas. Si bien no se vincula directamente con los sistemas de monitoreo electrónico analizados en este trabajo, constituye un ejemplo relevante del uso de tecnologías en la prevención de la violencia de género, cuya dimensión específica en materia de inteligencia artificial ameritaría un análisis autónomo. No obstante, se debe tener en cuenta el debate alrededor de este aplicativo tecnológico porque anticipa tensiones que Paraguay deberá enfrentar si incorpora más adelante componentes de evaluación algorítmica del riesgo en sus protocolos de monitoreo.

Ahora bien, la evidencia reciente en España revela que los problemas del monitoreo electrónico en violencia de género no se limitan a fallas técnicas aisladas, sino que responden a déficits estructurales de diseño, implementación y gobernanza. Informes periodísticos y documentación institucional identifican errores de diseño de los dispositivos, pérdidas de cobertura y falta de recursos, a lo que se suma una deficiente transición entre adjudicatarios en el servicio (RTVE, 2025).

De hecho, un punto especialmente crítico es la gestión de datos en contextos de cambio de proveedor. La transición en 2023 —de Telefónica (con Securitas Direct) a una UTE entre Vodafone y Securitas— generó fallos en el volcado de información que impidieron acceder a datos históricos de geolocalización durante varios meses. Según la Fiscalía General del Estado, ello supuso una "potencial desprotección de las víctimas", evidenciando que la continuidad y trazabilidad de los datos constituye un elemento central de la eficacia del sistema (El País, 2025a). Asimismo, se ha documentado que estas fallas han tenido impacto jurídico directo, incluyendo sobreseimientos y absoluciones de agresores debido a la imposibilidad de acreditar incumplimientos de medidas de alejamiento, lo que revela una interdependencia crítica entre tecnología y prueba penal (El País, 2025b). Esto trasciende la dimensión técnica y posiciona al monitoreo electrónico como un dispositivo probatorio frágil cuando no se garantiza la integridad de los datos.

La respuesta institucional española ha sido, en términos generales, de refuerzo técnico y expansión del sistema, sin revisión estructural de la lógica de respuesta (Ministerio de Igualdad, 2024; El País, 2025c). Sin embargo, este enfoque reproduce una lógica de corrección tecnológica incremental, es decir, "más tecnología como solución" (García Arenales, 2026), sin necesariamente abordar de forma integral los problemas de fondo vinculados a la contratación pública (RTVE, 2025; Maldita.es, 2025; RTVE, 2026), la interoperabilidad entre sistemas y la gobernanza de los datos. Desde una perspectiva comparada, estos desarrollos son particularmente relevantes para Paraguay. El diseño del sistema SIMDEC y la incorporación de tecnologías de monitoreo deben considerar no solo la funcionalidad del dispositivo, sino también garantías de continuidad de datos, estándares de interoperabilidad y mecanismos de control sobre proveedores[82]. La experiencia española demuestra que incluso en contextos con marcos normativos robustos —como el GDPR— persisten riesgos significativos cuando la infraestructura tecnológica depende de múltiples actores y procesos contractuales complejos.

En este sentido, el desafío no radica únicamente en la adopción de tecnología, sino en la construcción de un modelo legal y técnico que asegure la fiabilidad del sistema, la protección de datos y la efectividad de la respuesta institucional. En Paraguay, el sistema SIMDEC aún se encuentra en fase incipiente de implementación, lo que abre una ventana crítica para discutir estos posibles riesgos. A diferencia del caso español, donde las fallas emergen en un sistema consolidado, Paraguay enfrenta el desafío de diseñar desde el inicio mecanismos de continuidad y portabilidad de datos, criterios claros de responsabilidad ante fallas (proveedor vs. Estado), estándares mínimos de infraestructura y cobertura y protocolos efectivos de respuesta ante alertas. En caso de no prever estas aristas, existe el riesgo de replicar fallas estructurales observadas en España, pero en un contexto con menores capacidades institucionales.

82 Desde una perspectiva comparada, la experiencia internacional confirma lo discutido en esta investigación, y es que la eficacia de los sistemas de monitoreo electrónico no depende solo de la funcionalidad del dispositivo, sino también de la gobernanza de los datos, en particular de la continuidad de la información, la interoperabilidad entre sistemas y la existencia de mecanismos efectivos de control sobre los proveedores tecnológicos.

Lecciones transversales para Paraguay: crear condiciones para un sistema con enfoque de derechos

Uno de los hallazgos transversales del análisis comparado es que todos los países examinados presentan una coincidencia relevante y es que, la implementación y efectividad del sistema de monitoreo electrónico depende en gran medida de condiciones materiales básicas de infraestructura. Al igual que en Paraguay, la imposición de la medida está condicionada a la viabilidad técnica de su cumplimiento, lo que implica verificar que la persona usuaria cuente con acceso continuo a energía eléctrica, conectividad suficiente para la transmisión de datos y condiciones mínimas de cobertura de red. Estas limitaciones evidencian que la implementación del sistema no es únicamente una decisión jurídica, sino también una cuestión operativa vinculada a desigualdades territoriales y de acceso a servicios básicos.

Otra cuestión considerable es que, todos los países revisados cuentan con previsiones normativas en relación con la protección de los datos personales procesados por los sistemas de monitoreo electrónico más desarrollados que el paraguayo. Esto no es una cuestión secundaria, sino una condición estructuralmente relevante para evaluar los riesgos del modelo que Paraguay está implementando. Los datos generados por tobilleras electrónicas, aplicaciones —como Empower y Nendive— y sistemas de alerta incluyen geolocalización en tiempo real, historial de movimientos, datos de contacto e incluso posibles inferencias sobre comportamiento y niveles de riesgo, por lo que requieren salvaguardas específicas.

Sin garantías ni controles adecuados, pueden ser instrumentalizados para revictimizar a la persona protegida, estigmatizar a la persona imputada antes de una condena firme, o habilitar usos secundarios no autorizados (Citron & Pasquale, 2014; TEDIC, 2023; UNHCHR, 2021). El análisis comparado confirma que esta discusión no surgió en ninguno de los países examinados de forma anticipada, sino siempre posterior y generalmente tras incidentes. Paraguay tiene la oportunidad y la responsabilidad de anticiparse aprovechando la etapa incipiente de implementación del SIMDEC.

Del recorrido por los países tomados como casos comparativos, también emergen patrones recurrentes que permiten identificar condiciones mínimas sin las cuales el monitoreo electrónico en violencia de género produce resultados inconsistentes o contraproducentes (Renzema & Mayo-Wilson, 2005; Hucklesby, 2008). Se enuncian a continuación no como modelo ideal, sino como umbral de viabilidad institucional.

La primera condición es la capacidad de respuesta operativa efectiva. En todos los casos analizados, el factor determinante no fue el dispositivo en sí, sino la calidad de la reacción estatal ante una alerta, que implica personal suficiente, disponible las 24 horas, con protocolos claros y articulación interinstitucional real (Carter & Grommon, 2016; CNJ, 2022; Defensor del Pueblo, España, 2019). Para Paraguay, la pregunta crítica no es cuántas tobilleras se instalan, sino qué capacidad reactiva existe cuando una alerta se dispara.

La segunda condición es que el monitoreo electrónico no puede operar como mecanismo de protección aislado ni ser considerado una respuesta en sí mismo. La evidencia comparada es consistente en señalar la necesidad de una red de protección integral: su utilidad depende de estar inserto en un entramado institucional más amplio que incluya, entre otros, dispositivos de acogida, acompañamiento psicosocial y asistencia legal, funcionando como complemento de esas políticas y no como su sustituto (Erez et al., 2012; ANROWS, 2020). Algunas experiencias internacionales han documentado riesgos asociados a la expansión del sistema sin un desarrollo paralelo de estas capacidades, incluso en contextos donde

los dispositivos se encontraban activos al momento de producirse el daño. En el caso paraguayo, esta investigación no ha identificado, hasta el momento, mecanismos formalmente articulados entre el SIMDEC y este tipo de redes de apoyo integral, más allá de la provisión voluntaria de un dispositivo celular a la víctima en determinados casos.

La tercera condición es la gobernanza de datos con marco normativo operativo, que incluye ley general de protección de datos, autoridad de control independiente, evaluación de impacto previa, limitación de finalidad y plazos de retención definidos. En el caso paraguayo, la aprobación de la Ley N.° 7593/2025 es un avance significativo, pero su período de vacancia de veinticuatro meses y la pendiente reglamentación implican que el sistema seguirá expandiéndose durante un tiempo considerable bajo el régimen sectorial y fragmentado que se analizó en los capítulos anteriores.

La cuarta condición es la evaluación de impacto obligatoria, con metodología pública y criterios vinculantes para la renovación del sistema. Relacionado con ello, la experiencia argentina y brasileña advierte sobre el riesgo de la expansión por simple inercia contractual, consistente en el modelo de pago por dispositivo activo genera presión sistémica hacia el crecimiento cuantitativo independientemente de los resultados (UNFPA Argentina, 2020; CNJ, 2022). En nuestras entrevistas fue posible identificar una tensión análoga en el caso paraguayo, asociada a la reciente disponibilidad de 3.000 dispositivos adquiridos cuya utilización opera como estímulo implícito de expansión.

La quinta condición es la no responsabilización tecnológica de la víctima. España ha documentado que cuando el sistema falla, la narrativa institucional tiende a depositar la carga sobre quién debería ser protegida (Nancarrow & Modini, 2018; Maffei, 2021; Dragiewicz et al., 2018). El diseño del SIMDEC —que requiere que la víctima porte el dispositivo, mantenga conectividad activa y active las alertas— podría reproducir esta lógica de forma estructural, como se analizó en la sección de hallazgos empíricos, si no se realizan los ajustes necesarios.

Paraguay se encuentra en una fase inicial de implementación efectiva. Aunque la ley data de 2017, el decreto reglamentario fue promulgado recién en 2023, la modificación legislativa más significativa en 2024, y los protocolos operativos en 2025 , lo que significa que el sistema lleva apenas un año funcionando con un andamiaje normativo mínimamente consolidado. Esa relativa juventud institucional representa una oportunidad concreta para incorporar las condiciones identificadas antes de que el sistema se expanda con las fragilidades que la evidencia comparada documenta. La pregunta que este análisis deja abierta es si el Estado paraguayo tiene la voluntad política y la capacidad institucional para no repetir los mismos errores.

8. RECOMENDACIONES

Los hallazgos de esta investigación permiten sostener que el problema no reside únicamente en la existencia de tecnologías de monitoreo, sino en las condiciones institucionales, materiales y normativas en las que estas se despliegan. En Paraguay, el SIMDEC aparece como una política que busca mayor seguridad y menor hacinamiento en cárceles, pero cuya eficacia real depende de una red mucho más amplia: capacidad de respuesta policial y judicial, infraestructura eléctrica y de conectividad, articulación con servicios de atención, reglas claras sobre datos personales, transparencia pública y mecanismos de control democrático. Por eso, las recomendaciones que siguen no parten de una oposición abstracta y simplista a esta tecnología, sino de una pregunta más concreta y políticamente relevante: bajo qué condiciones, con qué límites y con qué garantías una herramienta de este tipo puede operar sin ampliar los riesgos que dice mitigar.

RECOMENDACIÓN 1. La respuesta institucional como condición, no como complemento

La eficacia del monitoreo electrónico no depende del dispositivo sino de la capacidad efectiva del Estado y sus instituciones para reaccionar cuando ese dispositivo genera una alerta. Detectar que la persona agresora violó una zona de exclusión no protege a la víctima si no existe capacidad de respuesta y policial suficiente y coordinada. Sin esta previsión, el sistema se limitaría a registrar el incumplimiento sin que ello se traduzca en protección efectiva.

Se recomienda condicionar la expansión del SIMDEC a la verificación previa de que esa capacidad de respuesta existe en cada jurisdicción donde se pretende implementar, establecer estándares mínimos de tiempo de reacción ante alertas, y definir con precisión qué institución asume la responsabilidad operativa en cada momento del circuito. Mientras persistan algunas ambigüedades de coordinación entre el Poder Judicial, el Ministerio del Interior y la Policía Nacional que esta investigación documentó, incorporar más dispositivos sin resolver esa brecha solo expande la promesa sin ampliar la protección real.

RECOMENDACIÓN 2. Integrar el SIMDEC en una red de acompañamiento: el dispositivo no resuelve lo que causó la violencia

El monitoreo electrónico es un instrumento de control territorial, no de transformación relacional. Por sí solo no enfrenta las vulnerabilidades sociales, económicas y relacionales que subyacen a la violencia de género, ni garantiza que la persona agresora se desconecte de las dinámicas que llevaron al conflicto. Para que produzca resultados sostenibles, su uso debe combinarse con intervenciones profesionales complementarias: acompañamiento psicosocial para la víctima, asistencia legal, acceso a refugios, y en los casos que corresponda, programas de responsabilización para el agresor que vayan más allá del cumplimiento formal de la medida.

Se recomienda que la expansión del SIMDEC se articule formalmente con los servicios del Ministerio de la Mujer y organizaciones especializadas, estableciendo qué acompañamiento recibe la víctima desde el momento de la activación de la medida, y no solo cuando se dispara una alerta.

RECOMENDACIÓN 3. Formación continua con enfoque de derechos para todos los operadores del sistema

El funcionamiento adecuado del SIMDEC depende no solo de que los dispositivos funcionen correctamente, sino de que las personas que operan el sistema —jueces, fiscales, defensores, personal de la OMDEC, policías y equipos multidisciplinares— comprendan las múltiples implicancias de la política que implementan y actúen con criterios uniformes, proporcionales y respetuosos de los derechos de todas las personas involucradas. Esta investigación documentó que la capacitación del personal fue identificada como área de mejora por las propias instituciones, sin que se detallaran contenidos ni alcance real.

Los procesos de formación continua deben contemplar explícitamente la política de gestión del monitoreo electrónico con perspectiva de derechos humanos y de género, el manejo ético de los datos personales que el sistema genera, los criterios para evitar la responsabilización tecnológica de las víctimas, y la comprensión de que el incumplimiento registrado por el dispositivo no siempre refleja una conducta voluntaria del portador —a veces responde a fallas técnicas que el sistema debe distinguir con claridad antes de activar consecuencias penales. Esto es especialmente relevante para quienes aplican la medida en audiencias de turno sin especialización en violencia doméstica, y para quienes operan el monitoreo en horarios nocturnos o en zonas con infraestructura precaria.

RECOMENDACIÓN 4. Establecer una política específica de protección de datos, auditoría y trazabilidad del sistema

Uno de los déficits más notorios relevados por esta investigación es la ausencia de reglas públicas suficientemente claras sobre qué datos se recolectan, quién accede a ellos, cuánto tiempo se conservan, bajo qué protocolos se comparten y qué controles externos existen sobre su tratamiento. La opacidad en esta materia es especialmente importante porque el SIMDEC y las herramientas asociadas procesan datos altamente sensibles: ubicación en tiempo real, domicilios, rutinas, trayectorias, contactos y eventos críticos de personas en situación de violencia.

Se recomienda aprobar una política específica de gobernanza de datos para el sistema, con reglas de acceso diferenciadas, plazos de retención, trazabilidad de consultas, protocolos de seguridad y mecanismos de auditoría independiente. Esa política debe alcanzar no solo a las instituciones estatales, sino también al proveedor privado que interviene en la operación del sistema. Sin un marco de gobernanza claro de protección de datos, la expansión del monitoreo electrónico corre el riesgo de consolidar una infraestructura de vigilancia intensiva sin controles equivalentes de derechos.

RECOMENDACIÓN 5. Producir transparencia activa e indicadores públicos comparables sobre funcionamiento, fallas y resultados

La investigación mostró que el sistema parece estar mejor preparado para registrar trayectorias, eventos y personas monitoreadas que para rendir cuentas públicamente sobre su propia eficacia, sus errores y sus límites. También mostró que buena parte de la información más detallada no surge de publicaciones estatales sistemáticas, sino de respuestas parciales, tardías y en algunos casos mediadas por el proveedor privado.

Se recomienda crear un esquema de transparencia activa con publicación periódica de datos agregados y comparables sobre: cantidad de dispositivos activos, criterios de asignación, informes de factibilidad rechazados, tiempos de instalación, volumen y tipos de alertas, falsas alarmas, intervenciones policiales, fallas técnicas, sanciones por incumplimiento, cobertura territorial y resultados de las medidas. Publicar más dispositivos instalados no equivale a publicar mejor información. La rendición de cuentas debe permitir evaluar si el sistema protege efectivamente, dónde falla y sobre qué desigualdades materiales opera.

RECOMENDACIÓN 6. Recomendación 6. Evitar la responsabilización tecnológica de las víctimas y asegurar alternativas no dependientes de conectividad

Los hallazgos empíricos muestran que parte de la promesa de protección descansa sobre condiciones que recaen en la propia víctima: portar un dispositivo, mantenerlo cargado, tener conectividad, responder llamadas o activar alertas. Esta distribución de cargas es especialmente problemática en contextos de desigualdad territorial, precariedad económica o barreras tecnológicas, porque transforma la protección en una obligación cotidiana de sostenimiento técnico.

Se recomienda que ninguna estrategia de protección descanse exclusivamente en la disponibilidad material, la alfabetización digital o la reacción inmediata de la víctima. El Estado debe asegurar alternativas que no dependan solo de *smartphones*, datos móviles o energía eléctrica regular, y revisar los protocolos para que la eventual falla técnica del ecosistema no derive en una nueva carga sobre quien ya está en situación de riesgo. La tecnología puede asistir la protección, pero no debe convertirse en una condición de acceso a ella.

9. NOTA FINAL

En su estado actual, el SIMDEC no debería evaluarse únicamente por su novedad tecnológica ni por la cantidad de dispositivos adquiridos o instalados, sino por su capacidad real para garantizar una protección integral. La principal advertencia que deja esta investigación es que una política pública de este tipo puede volverse rápidamente expansiva sin haber resuelto todavía sus condiciones mínimas de legitimidad democrática: coordinación efectiva, control público, límites claros sobre la vigilancia, protección de datos, evaluación de impacto y una red de cuidados que no desplace la carga hacia las víctimas.

Si el Estado paraguayo decide sostener y ampliar este sistema, debería hacerlo bajo una premisa básica: la tecnología no puede reemplazar la política pública integral, y mucho menos corregir por sí sola las desigualdades estructurales sobre las que opera. Solo un enfoque que combine capacidad institucional, transparencia, cuidado y derechos humanos permitirá evitar que una herramienta presentada como protección termine consolidando nuevas formas de vigilancia, opacidad y exclusión.

Declaración sobre uso de herramientas de Inteligencia Artificial

En cumplimiento con estándares de transparencia académica se declara el uso de herramientas de inteligencia artificial (Claude.AI, NotebookLM, ChatGPT) exclusivamente para unificación de estilo, sistematización y organización bibliográfica, apoyo en identificación de fuentes bibliográficas en etapa de revisión de literatura. Todo el contenido analítico, desarrollo argumentativo e interpretación normativa es producto del trabajo intelectual directo de las autoras.

10. BIBLIOGRAFÍA

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. Recuperado el 13 de abril de 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. Recuperado el 13 de abril de 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. Recuperado el 14 de abril de 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. Recuperado el 14 de abril de 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. Recuperado el 18 de abril de 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. Recuperado el 14 de abril de 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. Recuperado el 14 de abril de 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. Recuperado el 14 de abril de 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. Recuperado el 14 de abril de 2026.

El País. (2025c, 17 de septiembre). Igualdad cambia las pulseras telemáticas por tobilleras para evitar su manipulación. Recuperado el 14 de abril de 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. Recuperado el 18 de abril de 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. Recuperado el 13 de abril de 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. Recuperado el 13 de abril de 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. Recuperado el 18 de abril de 2026.

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

Ministerio de Desarrollo Social (Uruguay). (2019). Protocolo de actuación en situaciones de violencia basada en género. Recuperado el 18 de abril de 2026.

Ministerio de Igualdad (España). (2024). Protocolo de actuación en el sistema de seguimiento por medios telemáticos en casos de violencia de género. Recuperado el 14 de abril de 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. Recuperado el 18 de abril de 2026.

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

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

Ministério da Justiça e Segurança Pública (Brasil). (2026, 17 de abril). [Publicación en Instagram sobre el Projeto Alerta Mulher Segura]. Instagram. Recuperado el 18 de abril de 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. Recuperado el 14 de abril de 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. Recuperado el 14 de abril de 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). Recuperado el 18 de abril de 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. Recuperado el 18 de abril de 2026.

Presidencia de la República (Uruguay). (2025, 21 de noviembre). Dispositivo de seguridad que complementa tobilleras electrónicas estará operativo a fines de diciembre. Recuperado el 18 de abril de 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. Recuperado el 14 de abril de 2026.

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

RTVE. (2026, 27 de enero). El Gobierno sustituye pulseras electrónicas por tobilleras tras fallos del año pasado. Recuperado el 14 de abril de 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. Recuperado el 14 de abril de 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. Recuperado el 18 de abril de 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. Recuperado el 14 de abril de 2026.

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

Tecnología
& Derechos
Humanos

ISBN 978-99989-999-1-6