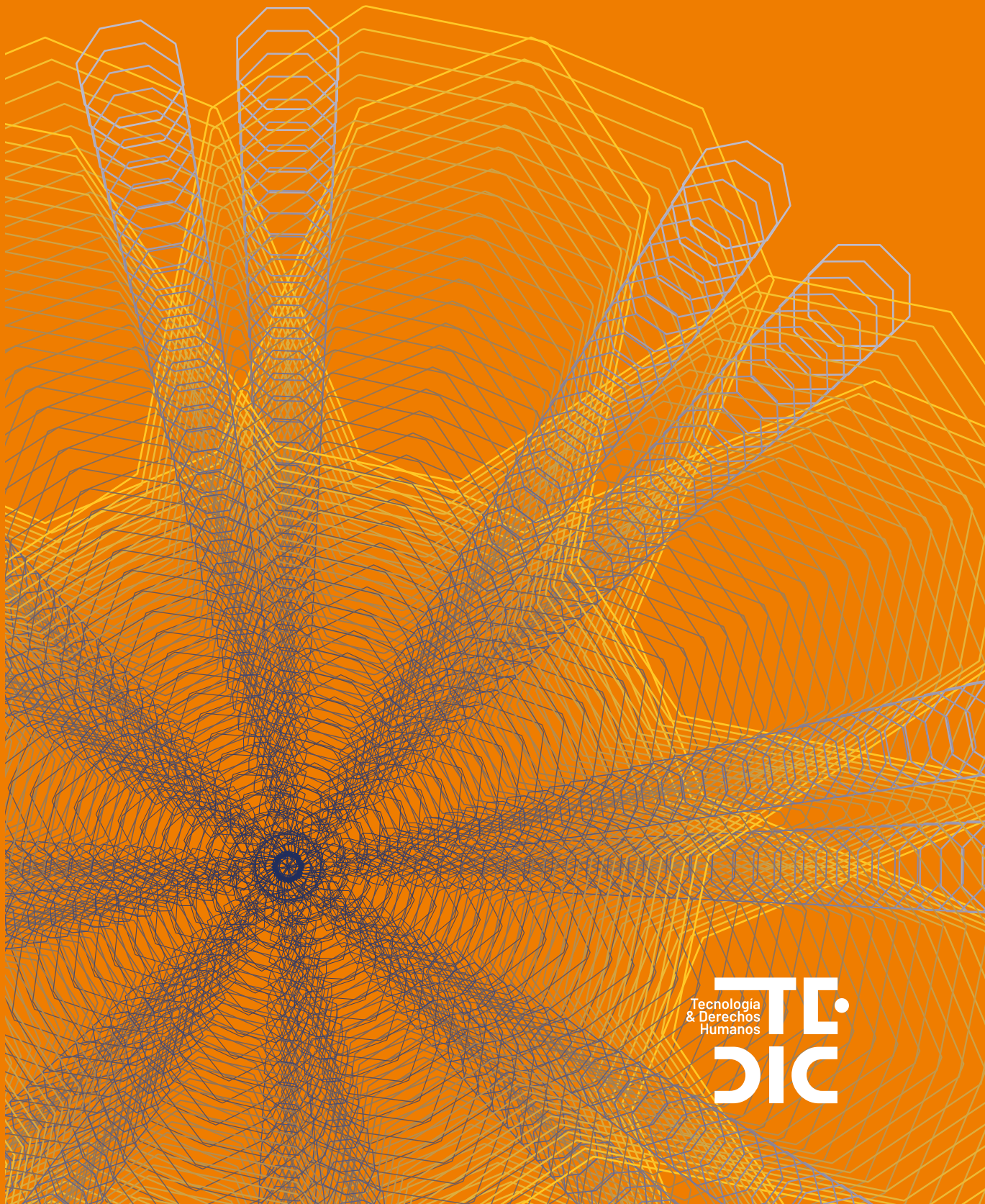
DRONES

Regulación y uso de drones en Paraguay desde una perspectiva de derechos digitales



Tecnología & Derechos Humanos

TEDIC

DRONES

Regulación y uso de drones en Paraguay desde una perspectiva de derechos digitales

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.

Financiado por la Unión Europea

CON EL APOYO DE
La gente cambia el mundo Diakonia

Tecnología & Derechos Humanos TEDIC

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

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.

DRONES

Regulación y uso de drones en Paraguay desde una perspectiva de derechos digitales

SETIEMBRE 2025

COORDINACIÓN
Maricarmen Sequera

INVESTIGACIÓN
Antonia Bogado
Hugo Mendieta

ASISTENCIA
Maricel Achucarro

COMUNICACIÓN
Romina Aquino

DIAGRAMACIÓN
Horacio Oteiza

ACERCA DE LOS INVESTIGADORES

Antonia Bogado Rodas: Abogada, LL.M por la London School of Economics and Political Science y Máster en Gobernanza Ética de la IA por la Universidad Pontificia de Salamanca. Su interés de investigación abarca los derechos digitales y la intersección entre derecho y tecnología.

Hugo Mendieta Cuevas: Egresado de la carrera de Derecho por la Universidad Nacional de Asunción (UNA), integrante del Consejo Editorial de la revista Liberoamérica y miembro del Colectivo Asunción Flores. Escribe regularmente en Adelante! Noticias.

TABLA DE CONTENIDO

INTRODUCCIÓN Y METODOLOGÍA DE INVESTIGACIÓN 6

MARCO TEÓRICO 9

- Tecnologías de drones: definición, usos, y capacidades 9
- Tipologías técnicas, capacidades de vigilancia y clasificaciones 9
- Drones como tecnologías duales: usos civiles, comerciales y militares 11
- Breve genealogía del uso estatal 13

DRONES Y DERECHOS HUMANOS EN LA ERA DIGITAL 17

- Marco conceptual 17
- Privacidad en el espacio público digitalizado 21
- Libertad de expresión y derecho a la protesta ante la amenaza de vigilancia aérea 24
- Legalidad y proporcionalidad en medidas de vigilancia tecnológica 26
- Vigilancia estatal, control social y estructuras de poder 28
- El panóptico digital y el control aéreo 29
- Drones y la militarización del espacio civil 31

PERSPECTIVA INTERSECCIONAL Y VIGILANCIA SELECTIVA 34

- Género, racialización y tecnologías de control 34
- Asimetrías en el acceso y uso de tecnologías 37

GOBERNANZA GLOBAL, GEOPOLÍTICA Y REGULACIÓN 39

- El caso paraguayo: fragmentación normativa y soberanía tecnológica 41

LIMITACIONES DEL ESTUDIO 44

RECOMENDACIONES 45

CONCLUSIONES 46

REFERENCIA BIBLIOGRÁFICA 47

DRONES
REGULACIÓN Y USO DE DRONES EN PARAGUAY DESDE UNA PERSPECTIVA DE DERECHOS DIGITALES

PALABRAS CLAVES: *Drones, derechos digitales, privacidad, vigilancia, Paraguay, derechos humanos, militarización, tecnologías emergentes, libertades civiles, género, políticas públicas.*

INTRODUCCIÓN Y METODOLOGÍA DE INVESTIGACIÓN

El creciente uso de drones[1] por parte de instituciones estatales y privadas en Paraguay plantea desafíos urgentes en materia de privacidad, vigilancia y derechos humanos. Si bien su utilización puede justificarse en tareas legítimas como monitoreo ambiental, agricultura de precisión o respuesta a emergencias, también se han documentado usos problemáticos con fines de control territorial, vigilancia de protestas sociales y hostigamiento a comunidades en zonas militarizadas.

Esta dualidad —entre utilidad social y potencial represivo— se agrava por la ausencia de garantías regulatorias y mecanismos efectivos de transparencia y rendición de cuentas en Paraguay. El vacío normativo expone a la ciudadanía a formas de vigilancia cada vez más sofisticadas y complejas, donde la tecnología amplifica las capacidades de control estatal sin contrapartidas equivalentes en términos de protección de derechos humanos.

La relevancia de esta investigación radica en la necesidad de anticipar y documentar los efectos negativos del despliegue de tecnologías emergentes de vigilancia en contextos de débil institucionalidad. En un país donde las tensiones sociales se expresan frecuentemente a través de protestas y movilizaciones ciudadanas, y donde persisten conflictos territoriales con comunidades campesinas e indígenas, el uso no supervisado de drones representa un riesgo significativo para el ejercicio de derechos fundamentales como la privacidad, la libertad de expresión, el derecho a la protesta y la libre circulación.

La presente investigación adopta un enfoque crítico basado en Derechos Humanos, tomando como referencia marcos normativos y experiencias internacionales comparadas. Nuestro análisis se centra específicamente en los usos que pueden resultar intrusivos, desproporcionados o carentes de control, buscando visibilizar los riesgos asociados a la vigilancia, persecución o control social mediante estas tecnologías.

El estudio está guiado por las siguientes preguntas centrales:

- ¿Cuál es el grado de transparencia público sobre la adquisición y uso de tecnologías de drones por parte del Estado paraguayo?
- ¿Qué instituciones controlan estas tecnologías y bajo qué marcos normativos operan?
- ¿Existen mecanismos de supervisión independiente o control parlamentario sobre su uso?
- ¿Cómo afecta el despliegue de drones el derecho a la privacidad en espacios públicos y privados?
- ¿Qué impacto tiene su uso en el ejercicio de la libertad de expresión y el derecho a la protesta pacífica?
- ¿Cómo se manifiestan los efectos diferenciados según género, etnia y clase social?

1 Este trabajo se enfoca en drones aéreos, aunque la tecnología no se limita a ese formato. Como señala Chamayou (2016), cualquier vehículo no tripulado —aéreo, terrestre o submarino— puede ser "dronizado", ampliando así el alcance del concepto más allá de lo aeronáutico.

- ¿Qué justificaciones oficiales sustentan el uso de drones en diferentes contextos operativos?
- ¿Existe proporcionalidad entre los fines declarados y los medios tecnológicos empleados?
- ¿Qué salvaguardas existen para prevenir abusos o uso indebido de la información recolectada?

Para cumplir con los objetivos del proyecto, se propone una **metodología mixta cualitativa**, que combina la revisión documental sistemática con trabajo de campo de recolección de casos de uso. Este enfoque permitirá tanto mapear el panorama normativo e institucional como documentar prácticas concretas —tanto a nivel nacional como internacional— y sus impactos en diferentes contextos sociales. La investigación se estructura en tres fases complementarias que se desarrollarán de manera parcialmente simultánea para maximizar la triangulación de fuentes y la validación cruzada de hallazgos.

La **primera fase** se centrará en el mapeo normativo e institucional, con el objetivo de caracterizar el marco legal vigente e identificar los actores institucionales involucrados en la adquisición y uso de drones. Esta etapa incluirá el análisis documental de la normativa vigente, particularmente los reglamentos de la Dirección Nacional de Aeronáutica Civil (DINAC), decretos del Poder Ejecutivo, resoluciones ministeriales y toda otra regulación aplicable. Paralelamente, se realizará una revisión de proyectos legislativos archivados o en trámite relacionados con la regulación de drones y tecnologías de vigilancia, así como un mapeo sistemático de adquisiciones públicas disponibles en el portal de la Dirección Nacional de Contrataciones Públicas (DNCP), identificando compras de equipos, servicios de mantenimiento y capacitación relacionados con drones. Se complementará esta fase con solicitudes formales de acceso a información pública dirigidas a instituciones clave como el Ministerio del Interior, Policía Nacional, Ministerio de Defensa, Secretaría Nacional de Inteligencia (SNI), Ministerio de Agricultura y Ganadería (MAG), y Fuerza de Tarea Conjunta (FTC). Como productos de esta fase se espera contar con una matriz normativa comparativa entre el marco nacional y los estándares internacionales de Derechos Humanos, una base de datos de adquisiciones públicas relacionadas con tecnologías de vigilancia aérea, y un mapeo detallado de actores institucionales y sus competencias específicas.

La **segunda fase** se enfocará en la documentación de prácticas y casos concretos, buscando identificar y analizar usos específicos de drones en diferentes contextos operativos, con especial atención a aquellos que puedan afectar derechos fundamentales. Esta etapa contempla el análisis de casos documentados donde se haya reportado el uso de drones en contextos de protesta social, operativos de seguridad, o control territorial en zonas rurales, complementado con una revisión hemerográfica sistemática de la cobertura mediática sobre el uso de drones por parte de fuerzas de seguridad y otras instituciones estatales. Se incorporará también el monitoreo de redes sociales para rastrear testimonios, imágenes y videos que documenten el despliegue de estas tecnologías desde la perspectiva ciudadana, así como entrevistas con actores afectados, incluyendo dirigentes sociales, activistas, líderes comunitarios y organizaciones que hayan experimentado vigilancia mediante drones. Los criterios de selección de casos priorizarán el uso de drones en manifestaciones o protestas sociales, operativos de seguridad en territorios con conflictos socioambientales, vigilancia en zonas fronterizas y áreas rurales, y casos que hayan generado denuncias por violación a derechos humanos.

La **tercera fase** se dedicará al análisis comparativo y la construcción de recomendaciones, contextualizando los hallazgos nacionales en el marco de experiencias regionales e internacionales para identificar patrones comunes y buenas prácticas. Esta etapa incluirá estudios de casos comparativos de experiencias en países de la región que hayan enfrentado desafíos similares, como Colombia, Brasil, México y Chile, junto con entrevistas a especialistas en derechos digitales, tecnologías de vigilancia y políticas de seguridad tanto a nivel nacional como regional. Se complementará con una revisión exhaustiva de literatura especializada, incluyendo investigaciones académicas, informes de organizaciones internacionales y documentos de políticas públicas sobre regulación de drones y protección de derechos humanos. Se realizarán entrevistas con diferentes perfiles de expertos, incluyendo especialistas en derechos digitales y tecnologías de vigilancia, académicos con experiencia en políticas de seguridad y militarización, funcionarios públicos de instituciones reguladoras como DINAC y Policía Nacional, activistas y organizaciones de Derechos Humanos con experiencia en vigilancia estatal, y expertos internacionales en regulación de drones y protección de privacidad.

Dado que la investigación aborda temas sensibles relacionados con seguridad y vigilancia estatal, se implementarán consideraciones éticas y metodológicas específicas para garantizar la rigurosidad y responsabilidad del proceso. Se priorizará la triangulación metodológica mediante el cruce de información entre diferentes fuentes documentales para validar hallazgos y minimizar sesgos, documentando explícitamente las limitaciones de acceso a información, los sesgos potenciales de las fuentes y las restricciones temporales que puedan afectar la exhaustividad del estudio.

Al finalizar la investigación, se espera contar con un diagnóstico integral que visibilice prácticas problemáticas, identifique riesgos específicos para los derechos humanos y proponga recomendaciones concretas para el uso responsable de drones desde una perspectiva de protección de derechos humanos y gobernanza pública basada en principios de legalidad, proporcionalidad y transparencia. Los productos específicos incluirán un mapeo completo del ecosistema institucional y normativo, la documentación de casos paradigmáticos y sus impactos diferenciados, un análisis comparativo con experiencias internacionales y recomendaciones dirigidas a diversos actores.

Esta investigación se alinea con la misión institucional de TEDIC de promover los derechos digitales y fortalecer el control democrático sobre el uso de tecnologías, contribuyendo a una agenda que garantice transparencia, equidad y respeto a los derechos humanos en el entorno digital y físico, y posicionando a Paraguay en el debate regional sobre la regulación responsable de tecnologías emergentes de vigilancia.

MARCO TEÓRICO

TECNOLOGÍAS DE DRONES: DEFINICIÓN, USOS, Y CAPACIDADES

Un dron o vehículo aéreo no tripulado (VANT) es un dispositivo tecnológico con formatos y usos variados. La Organización de Aviación Civil Internacional (OACI) utiliza varias denominaciones para referirse a estos dispositivos o sus sistemas, incluyendo: RPA (Aeronave pilotada a distancia), RPAS (Sistema de aeronave pilotada a distancia), UA (Aeronave no tripulada), y UAS (Sistema(s) de aeronave(s) no tripulada(s)). Sin embargo, el término "dron" es el más popular para referirse a aeronaves no tripuladas.

Según el Concepto Operacional de Gestión del Tránsito Aéreo Mundial (Doc 9854) de la OACI, un vehículo aéreo no tripulado (UA) es una aeronave sin piloto a bordo, que vuela sin un piloto al mando, y que se controla a distancia y plenamente desde otro lugar (tierra, otra aeronave, espacio) o que ha sido programada y es plenamente autónoma. Esta definición fue respaldada por la 35ª Asamblea de la OACI en 2011 (OACI, 2011). Las coordenadas georeferenciales de vuelo son programadas por software o controladas por control remoto.

Los drones pueden presentar diferentes tamaños, capacidades y una variedad de modelos, que van desde lo recreacional hasta usos más complejos. Se clasifican de diversas maneras según su estructura, tamaño, capacidades técnicas y aplicaciones. Por tipo de alas, existen los multirrotores, fáciles de maniobrar pero con poca autonomía; los ala fija, ideales para vuelos largos y estables; los helicópteros monomotor, capaces de transportar cargas pesadas; y los VTOL híbridos de ala fija, que combinan despegue vertical con autonomía extendida.

TIPOLOGÍAS TÉCNICAS, CAPACIDADES DE VIGILANCIA Y CLASIFICACIONES

Clasificación estructural de los drones

- **Dron de ala fija:** su diseño es similar al de los aviones, con una composición pensada para ahorrar energía y generar una sustentación aerodinámica adecuada. Tienen mejor estabilidad para operaciones de largo alcance y una gran mayoría de drones de equipo militar cuenta con el diseño de ala fija, incluso los drones HALE[2], que son mayormente utilizados para vigilancia y reconocimiento territorial en operativos militares.

- **Dron monorotor:** su composición es similar a la de un helicóptero, con un rotor que impulsa al dron. Por lo general tiene la capacidad de incorporar hélices más grandes para darle mayor eficiencia. Es utilizado para topografía y transporte de cargas pesadas.

- **Dron multirrotor o de ala rotatoria:** se compone de múltiples hélices sostenidas por el chasis centralizado, para lograr la estabilidad y la sustentación. Es un modelo versátil y simple pero con una autonomía reducida. Es el más común en el mercado de uso civil y estatal, usualmente para vigilancia o fotografía aérea, etc.

  - **Trirotor:** Cuenta con tres rotores ubicados en tres brazos que proporcionan control y movimiento. Este formato es el más económico y el menos autónomo.

2 *High-altitude long endurance* (mucha altitud y gran resistencia).

- **Cuadricóptero:** Modelo de común utilización civil. Está compuesto por cuatro rotores sostenidos por un armazón. Dos de las hélices giran en sentido opuesto al otro par. Tiene mayor estabilidad que los drones trirotor.
- **Hexacóptero:** Seis rotores sostenidos por un chasis de tamaño proporcional. Los rotores están ubicados de forma tal que cada brazo pueda brindar equilibrio y potencia. Tres de las hélices trabajan en sentido opuesto a las restantes. Su consumo energético es alto.
- **Octocóptero:** Mejora la estabilidad del hexacoptero al incorporar ocho rotores. Las hélices trabajan emparejadas en cuatro por sentido de rotación lo que permite un control de estabilidad excepcional. Usualmente es de utilización profesional.
- **Multirotor coaxial:** Está compuesto por brazos pares que sostienen dos o más rotores en cada uno de ellos, mientras que esos rotores giran en sentido opuesto. El multirotor coaxial permite alcanzar mayores altitudes y obtener mayor versatilidad que los otros diseños.

- **Dron híbrido de ala fija (VTOL):** Combina las alas fijas con rotores conectados a la estructura. Este diseño tiene muchas ventajas en lo que se refiere a la estabilidad y la manejabilidad. Es de uso mayoritario para transporte y entrega de paquetes.

  Según el tamaño, se dividen en muy pequeños (nano), pequeños, medianos y grandes, con usos que van desde vigilancia encubierta hasta filmaciones o entregas. En cuanto a la capacidad de carga, se clasifican como drones ultraligeros, ligeros, medios y de carga pesada, adecuados para misiones que van desde la recreación hasta el combate militar. Según su alcance, los drones varían entre muy corto alcance (hasta 5 km) y largo alcance (más de 644 km), con tiempos de vuelo que pueden superar las 24 horas. También se categorizan por su fuente de energía, como baterías (más comunes), gasolina, hidrógeno o solar. En cuanto al tipo de motor, pueden tener motores con escobillas (económicos pero menos duraderos) o sin escobillas (más potentes y eficientes). Finalmente, según su funcionalidad, existen drones de juguete, fotográficos, de carreras, con GPS, profesionales, militares y de reparto, lo que refleja la creciente especialización y diversificación de esta tecnología (JOUAV, 2025).

  Estas son las clasificaciones básicas reconocidas internacionalmente, aunque existen muchas otras clasificaciones que se encuentran en reglamentaciones regionales y nacionales, por ejemplo la clasificación de la Agencia de la Unión Europea para la Seguridad Aérea[3] (EASA), que distingue a los drones en 6 clases de acuerdo a su peso o masa.

  La referencia de clasificación en Paraguay distingue dos tipos generales de drones: 1) aeronaves autónomas; y 2) aeronaves pilotadas a distancia (Reglamento de Aeronaves Pilotadas a Distancia (RPA) y Sistema de Aeronaves Pilotadas a Distancia, 2017). Estas tienen que ver con la capacidad autonómica del equipo. Luego se encuentran las clasificaciones técnicas de acuerdo al peso/masa al momento de despegue, al uso y a las categorías reglamentarias que definen si se realiza con licencia abierta, certificada o específica.

  Todas estos formatos de drones tienen capacidades para la vigilancia (tratamiento de datos, etc) y el uso militar, pero asimismo tienen potencialidades importantes para usos técnicos en muchos segmentos de bienes y servicios, incluyendo actividades de interés científico.

3 Ver más en el sitio de EASA: https://www.easa.europa.eu/en/document-library/general-publications/drone-class-identification-labels-and-information-notices

DRONES COMO TECNOLOGÍAS DUALES: USOS CIVILES, COMERCIALES Y MILITARES

Los drones, o UAVs, encarnan el carácter dual que define a muchas tecnologías contemporáneas. Por un lado, pueden potenciar capacidades estatales, corporativas y ciudadanas para fines legítimos y de interés público; por otro, su uso sin delimitaciones claras puede derivar en prácticas de control social, exclusión o vigilancia desproporcionada. Esta ambivalencia técnica exige un enfoque crítico que evite tanto su adopción entusiasta y acrítica por sus beneficios potenciales, como su descalificación automática ante los riesgos que conlleva.

Diversas organizaciones internacionales han destacado los beneficios de los drones en sectores clave. El Banco Mundial (2024) ha identificado cinco áreas prioritarias en las que su implementación ha generado impactos positivos: "la entrega de insumos médicos en zonas remotas, la agricultura de precisión, la gestión de riesgos de desastres, el monitoreo de infraestructuras críticas y la restauración de ecosistemas". Estas funciones no solo reducen costos operativos y superan barreras geográficas, sino que, en ciertos contextos, se convierten en herramientas indispensables para garantizar derechos sociales como la salud, el ambiente sano o el acceso a servicios básicos.

En América Latina, experiencias en Brasil, México, Perú y Argentina muestran aplicaciones emergentes para el monitoreo de incendios forestales, la planificación urbana, el control de enfermedades transmitidas por vectores, o la vigilancia de especies en peligro de extinción (World Bank, 2024; Jokura, 2021). En el ámbito de la salud sexual y reproductiva, el uso de drones ha sido clave para sortear restricciones normativas, como en el caso de la entrega de píldoras abortivas desde Alemania a Polonia, organizada por la organización Women on Waves (Browne, 2015). Asimismo, iniciativas en países como Ghana, Nepal o Botswana han demostrado la viabilidad del uso de drones para distribuir medicamentos, recolectar muestras médicas, e incluso enviar sangre para transfusiones a zonas rurales y aisladas (United Nations, 2021).

Estos usos no son ajenos a Paraguay, aunque su desarrollo sigue siendo incipiente. El sector privado ha comenzado a incorporar drones agrícolas en diversas actividades productivas, principalmente para la pulverización de cultivos como cereales, yerba mate y especies forestales, valorando su bajo costo operativo y versatilidad (ABC Color, 2025). También se emplean drones multiespectrales para mapeo MITICy análisis del estado de los campos, así como para el monitoreo de animales y tareas de siembra y fertilización. Mientras el Ministerio de Agricultura y Ganadería (MAG) reconoce el uso de drones solo para fines de prensa institucional desde 2024[4], sin lineamientos específicos para su regulación en el ámbito privado; otras instituciones como el Ministerio de Tecnologías de la Información y Comunicación (MITIC), los emplean con fines publicitarios, ajustándose a las disposiciones de la DINAC[5].

Por fuera del ámbito estatal, experiencias internacionales como las de Amazon o DHL muestran un creciente interés por la entrega automatizada de paquetes, y en eventos catastróficos como inundaciones o incendios forestales —como ocurrió en Texas o Los Ángeles— se han desplegado drones para búsqueda y evaluación de daños (Castleman & Toohey, 2025).

4 Esta información se basa en la respuesta oficial proporcionada por el MAG a la solicitud de acceso a la información pública (№ 93399), disponible en el Portal Unificado de Información Pública. (Ministerio de Agricultura y Ganadería, 2025).

5 Según respuesta oficial del MITIC a la Solicitud № 93400, el ente reconoció poseer un dron con cámara marca DJI, modelo MINI 4 PRO (SN° 1581f6z9c239k0038je2), utilizado exclusivamente con fines publicitarios y de producción institucional (MITIC, 2025).

Así, el carácter dual que define a esta tecnología abre también un campo de tensiones y cuestionamientos sobre los fines, contextos y marcos que orientan su implementación. El mismo dispositivo que permite entregar vacunas en zonas remotas puede, en ausencia de controles adecuados, ser utilizado para vigilar protestas, rastrear desplazamientos o ejercer persecución selectiva. De hecho, se han documentado interferencias entre drones privados y operativos de rescate, generando riesgos graves en contextos de emergencia (Castleman & Toohey, 2025).

En el ámbito militar, los UAVs armados o especializados en inteligencia han sido desplegados crecientemente en conflictos internacionales[6], transformado la guerra moderna de maneras significativas, introduciendo nuevos métodos de combate y planteando desafíos complejos en el ámbito de la defensa. Como ha advertido Seth J. Frantzman (2021), en los últimos años, los drones han desempeñado un papel estratégico en guerras alrededor del mundo, consolidándose como herramientas tanto de ataque como de vigilancia.

En la guerra entre Rusia y Ucrania[7], por ejemplo, se ha documentado el uso intensivo de drones tanto por fuerzas estatales como por grupos irregulares, lo que ha contribuido a redefinir la lógica del campo de batalla a partir de tecnologías de bajo costo y alta precisión. Algunos reportes incluso han sostenido que los "drones y vehículos no tripulados ya están empezando a sustituir a los soldados" (Kardoudi, 2025).

Asimismo en el contexto del conflicto Israel y Palestina[8], drones equipados con cámaras térmicas y armamento han sido utilizados para el reconocimiento y el ataque, generando graves denuncias por daños colaterales, vigilancia masiva e impactos psicológicos sobre todo, en la población civil. También se han reportado incidentes recientes de drones lanzados entre Irán e Israel[9], lo que ha intensificado las tensiones regionales y ha evidenciado la creciente automatización del conflicto armado.

En palabras de Frantzman (2021), el futuro de la guerra con drones se dirige hacia una mayor autonomía y el uso de inteligencia artificial (IA), con los humanos en un rol de "human on the loop" (supervisión) en lugar de "human in the loop" (control directo). En línea con esto, distintas organizaciones nacionales e internacionales —entre ellas TEDIC— han planteado interrogantes éticos sobre el uso de drones armados, en particular en lo que respecta a la posibilidad de que estos sistemas tomen decisiones letales sin supervisión humana directa[10].

---

6 Si bien este trabajo se centra particularmente en los drones aéreos, resulta relevante destacar la complementariedad de este tipo de tecnologías en otros entornos, como lo demuestra el uso el uso del dron submarino "Blue Whale" por parte de Alemania para patrullajes defensivos en el mar Báltico (DCD, 2025).

7 El conflicto entre Rusia y Ucrania ha sido uno de los primeros enfrentamientos convencionales en los que los drones —comerciales y militares— han sido desplegados masivamente por ambos bandos, redefiniendo tácticas de guerra, reconocimiento y ataques selectivos (Edmonds & Bendett, 2022; Naciones Unidas, 2025).

8 Se ha documentado el uso sistemático de drones armados por parte de Israel en la Franja de Gaza, tanto para vigilancia como para ataques selectivos, generando un alto número de víctimas civiles y afectaciones psicológicas prolongadas en la población. (Ver: Abualouf, R. (2025, junio 26). Israeli strike at Gaza market kills 18 Palestinians, doctor and witnesses say. BBC. https://www.bbc.com/news/articles/cly8dlzx918o.

9 En los últimos años, Irán e Israel han protagonizado una escalada tecnológica mediante el uso de drones armados en ataques selectivos y operaciones de represalia. Ver: Reuters. (2025). Mapping the conflict between Israel and Iran. https://www.reuters.com/graphics/IRAN-NUCLEAR/ISRAEL/dwvklgrgjpm/

10 Para conocer más sobre los argumentos alrededor, ver la campaña "Stop Killer Robots" o "Paren a los Robots Asesinos": https://www.stopkillerrobots.org/

Frantzman (2021) también arguye que, la transformación de la guerra por los drones es un proceso continuo, con avances rápidos en tecnología y proliferación que desafían las estrategias de defensa existentes y requieren una adaptación constante. A esto, sumamos que, la versatilidad funcional ampliamente documentada, impone una exigencia clara: evaluar cada implementación a partir de sus fines, su proporcionalidad, su impacto y los marcos de gobernanza que la acompañan. No se trata solo de quién opera el dron, sino de con qué propósito, con qué garantías y bajo qué sistema de rendición de cuentas. En un ecosistema tecnológico donde las fronteras entre usos civiles, comerciales y de seguridad se difuminan rápidamente, pensar los drones como tecnologías duales es el primer paso para garantizar que sus beneficios no terminen encubriendo nuevas formas de exclusión, vigilancia o violencia estructural.

BREVE GENEALOGÍA DEL USO ESTATAL

Para ahondar en la tecnología y su actualidad se hace necesario discutir materialmente la historiografía de los drones; y al entrar en esta cuestión también es imprescindible mencionar al Estado, factor fundamental que, según Friedrich Engels, es una estructura de unidades territoriales basadas en relaciones de propiedad que desplazó definitivamente a "la sociedad antigua, basada en las uniones gentilicias" (Engels, 2017, p. 1). Este contexto histórico y la consolidación de la organización social estatal influyó en el devenir de los drones, en su evolución y modos de uso.

Una mayoría de los antecedentes importantes que se mencionan a continuación[11] se dieron en el marco de campañas de acción bélica y de la organización de seguridad de la naciones, esto sin obviar que durante el siglo XX fue encontrando amplitud de crecimiento en el sector civil y científico privado.

El uso de aviones sin tripulación en combate se remonta al año 1849, indica Rachel Sïmon Rushby (2017), cuando el ejército austriaco utilizó una flota de globos aerostáticos sin tripulación en un ataque contra Venecia. Está claro que a partir de ese momento se desarrolló un despunte en la aplicación de la tecnología por razones bélicas, posteriormente en la Primera y Segunda Guerra Mundial, en las que las partes en conflicto hicieron planificaciones para desarrollar aviones de combate sin tripulación. Estos avances fueron impulsados por Estados que vieron algunas de las posibilidades de esta tecnología en el campo bélico y de seguridad interna (mayormente vigilancia y reconocimiento), por lo que la aplicación de los drones se realizó conforme los Estados fueron consolidando sus programas de desarrollo tecnológico.

Uno de los ejemplos de uso bélico —de los tantos que existen en el siglo XX— es el que se puede rastrear hasta la guerra de resistencia de Vietnam, con los "drones Firebee"[12], que fueron usados extensamente por parte de los Estados Unidos de América (EUA), en territorio vietnamita. Sin embargo, la rápida evolución de las computadoras desde finales del siglo pasado permitieron que los drones armados se convirtiesen en armas más sofisticadas. Tanto es así que fue el arma

11 Así como el subtítulo del segmento advierte, no se citan todos los antecedentes ni se abarca todo el proceso historiográfico que involucra a esta tecnología. Se toman algunos momentos destacados para ilustrar de manera más o menos acabada la complejidad de ese proceso.

12 El modelo de dron AQM-34L fue utilizado en más de una treintena de ataques al norte de Vietnam. Puede verse una muestra del vehículo en el Museo de las Fuerzas Aereas Estad ounidenses: https://www.nationalmuseum.af.mil/Visit/Museum-Exhibits/Fact-Sheets/Display/Article/195747/teledyne-ryan-aqm-34l-firebee/

predilecta y representativa del régimen estadounidense dentro su "Global war on terror"[13], nombre de la campaña militar internacional dirigida por Estados Unidos de América, lanzada después de los ataques del 11 de septiembre de 2001 en el World Trade Center de Nueva York y algunos edificios gubernamentales. Este enfoque fue un parteaguas en el desarrollo estadounidense de la tecnología de los drones y su utilización generalizada.

La justificación predominante en este siglo para el desarrollo de programas de drones armados en una mayoría de países donde tienen operaciones militares es que el dron se presenta como una "herramienta quirúrgicamente precisa y efectiva", con mínimos inconvenientes o impactos colaterales. Estas afirmaciones son bastante cuestionables cuando se contrastan con los datos e informaciones recogidas por medios de prensa en los sitios en que se realizaron operativos militares con drones. Por ejemplo, en Pakistán se muestra que desde junio de 2004 hasta mediados de septiembre de 2012 los ataques con drones mataron entre 2.562 a 3.325 personas en ese país, de los cuales 474 a 881 eran civiles, incluidos 176 niños, y el número de objetivos de alto nivel muertos como porcentaje del total de bajas es extremadamente bajo, estimado en sólo el 2 % (International Human Rights And Conflict Resolution Clinic et al., 2012). De igual modo, en Palestina se registraron una gran cantidad de bajas civiles[14] en ataques con drones operados por las Fuerzas de Defensa de Israel (FDI). Al mismo tiempo en que colonos israelíes utilizan drones en varios sectores de Gaza (Abraham, 2025) para intimidar a la población palestina.

Los drones también se emplean como herramienta para la mediación en conflictos internacionales y exigir condiciones en la mediación de tensiones; en el marco del conflicto de la República Saharaui frente a la ocupación y anexión territorial por parte de Marruecos, el presidente saharaui, Brahim Ghali, afirmó que su ejército comenzará a utilizar drones armados contra las fuerzas marroquíes, apuntando hacia una guerra total si la ocupación no cesa (Resumen Latinoamericano, 2025). Estas situaciones ilustran que la tecnología se desarrolla en la medida de las necesidades de los Estados y en los ejemplos que se mencionan se observa que estas tienden a poner en peligro la vida de las poblaciones civiles.

Desde el punto de vista del Derecho Internacional Humanitario (DIH) y el Derecho Internacional de los Derechos Humanos (DIDH) el dron armado no está expresamente prohibido, debe cumplir con estos principios a la hora de su utilización: distinción, proporcionalidad, necesidad militar y humanidad. Comenta sobre esto Rushby (2017, pp. 24-25):

> No hay tratados ni derecho consuetudinario que prohíban el uso de drones armados per se. En el DIH convencional las reglas sobre los medios de guerra están contenidas principalmente en los artículos 35 y 36 del Protocolo I adicional de 1977 (Protocolo I) a los cuatro Convenios de Ginebra del 1949, relativo a la protección de las víctimas de los conflictos armados internacionales. Mientras el Protocolo I se aplica solo a los conflictos armados

13 Sobre esta "Global war on terror", también existen otras cuestiones discutidas en el ámbito del derecho internacional. Rushby (2017) cita que "la mayoría de comentadores jurídicos que han considerado el concepto estadounidense de 'guerra global contra el terror', concluyen que esta no es una interpretación legítima del concepto de conflicto armado no internacional. Sin duda la misma crea problemas cuando consideramos la aplicación del DIH".

14 La propia BBC recogió una declaración dada a la AFP, donde un residente del sur de Gaza afirmó lo siguiente: "La gente está actualmente dentro de sus casas porque cualquiera que se mueva es atacado por los drones israelíes". Ver más en: https://www.bbc.com/mundo/articles/c3gg8dn55mdo

> internacionales, las reglas consagradas en los artículos 35 y 36 forman parte del derecho internacional consuetudinario y por eso se aplican igualmente a ambos conflictos, internacionales y no internacionales. Adicionalmente, los armamentos tienen que ser capaces de cumplir con los principios del DIH, es decir, distinción, precaución y proporcionalidad.

En tanto el desarrollo tecnológico sigue su camino, también se plantean propuestas normativas para regular estas situaciones que se dan con la utilización bélica de este aparato. Cabe mencionar que, como paradigma, entre las recomendaciones en la audiencia de la CIDH del año 2013 (Comisión Interamericana de Derechos Humanos, 2013)[15], los exponentes internacionales destacaron la importancia de que los Estados puedan facilitar la creación de una articulación de supervisión civil a las operaciones militares y policiales con esta tecnología. En esa misma audiencia del 2013, el representante de la Fundación Robert F. Kennedy Human Rights, enumeró las principales razones por las que las que está en auge la utilización militar de esta tecnología en la región:

> Las razones para acceder a esta tecnología son varias, pero se pueden sintetizar en tres argumentaciones: el costo de estos aviones es menor que el de aviones de última generación, hay un efecto en la medida en que la adquisición por un país crea una necesidad ficticia de acceder a la misma tecnología por parte de otro estado, y frente a los recortes de impuestos a la mayorías de las fuerzas armadas de la región, los militares ansían tener nuevos juguetes para mantener su espacio institucional[16].

Ya desde la década pasada las organizaciones internacionales abogan por disminuir y limitar los programas de vigilancia, como dejan sentado en un comunicado conjunto la relatora especial de las Naciones Unidas (ONU) para la protección y promoción del derecho a la libertad de opinión y de expresión y la relatora especial para la libertad de expresión de la CIDH de la Organización de Estados Americanos (OEA), conforme a las normativas internacionales:

> (...) prohíben injerencias arbitrarias o abusivas en la vida privada, incluidas las comunicaciones, y a obtener la protección del Estado contra ese tipo de injerencias. De conformidad con lo anterior, los Estados deben garantizar que la intervención, recolección y uso de información personal, incluidas todas las limitaciones al derecho de la persona afectada a acceder a información sobre las mismas, estén claramente autorizadas por la ley a fin de proteger a la persona contra interferencias arbitrarias o abusivas en sus intereses privados. La ley deberá establecer límites respecto a la naturaleza, alcance y duración de este tipo de medidas, las razones para ordenarlas, las autoridades competentes para autorizar, ejecutar y supervisarlas y los mecanismos legales para su impugnación" (Relator Especial de las Naciones Unidas (ONU) para la Protección y Promoción del Derecho a la Libertad de Opinión y de Expresión & Relatora Especial para la Libertad de Expresión de la Comisión Interamericana de Derechos Humanos de la OEA, 2013).

La situación actual da cuenta de que sin control transparente e independiente a los Estados en las decisiones en el ámbito de la defensa y seguridad interna —que de por sí cuentan con una larga tradición de secreto en los desarrollos tecnológicos—, sin mencionar la falta de procedimientos reglamentados para el uso de estos drones en la vigilancia, conlleva un riesgo enorme. Ya no sólo por sus

15 Ver más en: https://www.youtube.com/watch?v=to0EImeza30&t=608s

16 Ver intervención en: https://youtu.be/to0EImeza30?si=7TS5Qqu2i7cHmSGZ&t=195

efectos sobre poblaciones civiles sino además por la posibilidad de obstaculizar la gestión democrática y por vulnerar los Derechos Humanos. Así como se mencionó anteriormente, la apuesta por el desarrollo de estos artefactos tiende hacia los propósitos bélicos y de seguridad estatal; ejemplo de esto son los datos que recoge Grégoire Chamayou (2016, p. 21) de la situación estadounidense:

> Esta arma se está desarrollando exponencialmente: el número de patrullas de drones armados norteamericanos aumentó un 1.200% entre 2005 y 2011. En Estados Unidos, se forman hoy más operadores de drones que pilotos de aviones de combate y de bombarderos juntos. Mientras el presupuesto de defensa bajó en 2013, con recortes en numerosos sectores, los recursos otorgados a los sistemas de armas no tripuladas aumentaron el 30%.

Si bien la tecnología está alcanzando niveles de accesibilidad y de eficacia sin precedentes, lo que podemos notar en el desarrollo histórico de los drones es que este se relaciona directamente con intereses belicistas y de vigilancia. Siendo así, se entiende que para revisar el proceso histórico de los drones hay que considerar a los estados y sus políticas, nacionales e internacionales.

DRONES Y DERECHOS HUMANOS EN LA ERA DIGITAL

MARCO CONCEPTUAL

El despliegue creciente de drones para tareas de vigilancia, control y seguridad, ya sea por parte del Estado o de actores privados, ha generado profundas tensiones sobre los derechos humanos. Si bien estas tecnologías presentan indiscutibles beneficios en diversos contextos como la agricultura, el monitoreo ambiental o la respuesta a emergencias, su utilización en entornos urbanos y para fines de control social plantea serias preocupaciones en materia de privacidad, autonomía, igualdad y libertades fundamentales (Gholami, 2024).

Particularmente, el uso de drones con fines de vigilancia masiva o selectiva puede derivar en la vulneración del derecho a la privacidad, consagrado en la Constitución de la República del Paraguay —en adelante, la Constitución Nacional— (art. 33), así como en el artículo 12 de la Declaración Universal de los Derechos Humanos y el artículo 11 de la Convención Americana sobre Derechos Humanos (Pacto de San José). Además, la captación de imágenes, sonidos o datos personales sin consentimiento ni control judicial puede convertirse en una forma de injerencia arbitraria[17] en la vida privada de las personas (Naciones Unidas, 2020; Risso, 2019).

Del mismo modo, el uso intensivo de estas tecnologías puede tener un efecto inhibitorio sobre el ejercicio de libertades fundamentales, como la libertad de expresión y la libertad de reunión, reconocidas en los artículos 26 de la Constitución Nacional, 19 y 20 de la Declaración Universal de los Derechos Humanos, y 13 y 15 de la Convención Americana., particularmente cuando se emplean para monitorear manifestaciones o espacios de protesta, cuestión que será desarrollada con mayor detalle en una sección posterior.

Este tipo de vigilancia, al ser percibida como una amenaza o una forma de intimidación, restringe el derecho de las personas a expresarse libremente y reunirse sin temor a represalias (Lara Castro, 2020). No obstante, es importante señalar que no todos los usos de drones implican, per se, una vulneración de derechos, y que el análisis debe realizarse caso por caso, en función del contexto, la finalidad, la tecnología empleada y la existencia o no de garantías jurídicas y mecanismos de control (Gholami, 2024). Por ejemplo, el uso de drones para inspeccionar cultivos no plantea las mismas preocupaciones que aquel destinado a vigilar una protesta ciudadana.

Por otro lado, también se debe mencionar el riesgo particular de discriminación cuando los drones son utilizados de forma desproporcionada en determinados territorios o dirigidos a poblaciones específicas, reproduciendo patrones de estigmatización y vigilancia selectiva (D'Ignazio & Klein, 2020). Estas prácticas, si no son reguladas pueden resultar incompatibles con instrumentos normativos nacionales e internacionales en materia de derechos humanos.

17 Según el Informe de la Alta Comisionada de las Naciones Unidas para los Derechos Humanos titulado *El derecho a la privacidad en la era digital* (A/HRC/48/31, 2021), toda injerencia en el derecho a la intimidad debe perseguir un fin legítimo, y además ser necesaria y proporcional para alcanzarlo. Esta exigencia cobra especial relevancia en la era digital, donde los avances tecnológicos permiten formas de vigilancia cada vez más sofisticadas e intrusivas. El informe advierte que la falta de garantías adecuadas puede convertir estas prácticas en violaciones sistemáticas de derechos fundamentales.

Adicionalmente, la problemática asociada al uso de drones también debe analizarse a la luz de los derechos digitales[18]. Como lo plantean Sequera y Lara Castro (2020), estos derechos surgen para brindar una respuesta jurídica precisa frente a las actividades vinculadas a los servicios de la sociedad de la información y la comunicación. Aunque derivan de los derechos humanos tradicionales, los derechos digitales poseen particularidades técnicas y normativas propias[19], que pueden verse severamente afectadas frente al uso de drones equipados con tecnologías de recolección de datos, sensores térmicos, cámaras de alta resolución y capacidades de transmisión remota de información, especialmente cuando estos operan sin consentimiento informado ni límites regulatorios definidos.

Esta preocupación cobra aún más relevancia cuando consideramos que derechos como la libertad de expresión, el derecho a la información o el derecho a la reunión y protesta en el espacio físico se interrelacionan cada vez más con el ecosistema digital. En este sentido, la capacidad de comunicarse libremente, ejercer la ciudadanía digital y proteger la integridad de la identidad en línea se ve amenazada cuando tecnologías como los drones se despliegan de manera opaca o intrusiva. La vigilancia aérea puede convertirse así en un mecanismo de control social, disuasión del discurso crítico y debilitamiento del derecho al acceso democrático a la sociedad del conocimiento, tal como fue señalado por el Relator Especial de las Naciones Unidas sobre los derechos a la libertad de reunión pacífica y de asociación (ONU, 2019).

En este escenario, es imprescindible reconocer que los derechos humanos deben ser considerados en todas sus dimensiones y ámbitos de ejercicio, tanto físicos como digitales. Aunque los drones puedan parecer parte de un plano "material", su funcionamiento depende intrínsecamente de infraestructura tecnológica y digital, incluyendo internet, software, sistemas de IA, algoritmos de reconocimiento facial y plataformas de análisis de datos, los cuales amplifican su capacidad de vigilancia e intervención, y por ende, su potencial de interferencia o explotación de derechos digitales fundamentales.

Para ilustrar con mayor claridad cómo el uso de drones puede vulnerar derechos fundamentales reconocidos tanto en el ordenamiento jurídico paraguayo como en instrumentos internacionales de derechos humanos, se presenta a continuación un cuadro comparativo. Este sintetiza los principales derechos afectados, su fundamento normativo, el nivel de riesgo identificado (alto o medio) y las posibles formas de afectación derivadas de su uso, especialmente en contextos de vigilancia y control social.

Ahora bien, cabe aclarar, que el cuadro no debe interpretarse de forma taxativa, ya que —como se ha advertido— el impacto de las tecnologías de vigilancia es transversal y puede extenderse a múltiples esferas de la vida social, política y privada. Sin embargo, busca señalar de manera sistemática aquellas garantías cuya afectación resulta más evidente y documentada frente al uso actual de drones con fines de control o supervisión.

18 Una categoría emergente que reconoce la necesidad de garantizar las libertades fundamentales en el entorno digital y frente al uso de tecnologías de vigilancia y control (Sequera & Lara Castro, 2020)

19 Como el derecho a la protección de datos personales, la neutralidad de la red, el acceso universal y el derecho al cifrado y al anonimato.

TABLA 1. Cuadro comparativo sobre los derechos afectados y niveles de riesgos

Derecho/ Garantia	Constitución de la República del Paraguay	Declaración Universal de DDHH	Declaración Americana de DDHH	Nivel de riesgo	Posible afectación por drones
Derecho a la vida	Art. 4 Del Derecho a la Vida	Art. 3	Art. 4 Derecho a la vida	ALTO	Drones armados en conflictos, uso policial letal, accidentes por mal funcionamiento
Derecho a la Libertad	Art. 9 Libertad y Seguridad de las personas	Art. 3 - Derecho a la Libertad	Art. 7 Derecho a la Libertad Personal	ALTO	Limitación de movimientos por vigilancia masiva, control de manifestaciones
Derecho a la Privacidad	Art. 33 Del Derecho a la Intimidad	Art. 12 - Protección contra injerencias arbitrarias	Art. 11 Protección a la honra, reputación personal y familiar	ALTO	Vigilancia no autorizada, grabación de actividades privadas, seguimiento de personas
Derecho a la inviolabilidad del Domicilio	Art. 34 Del Derecho a la Inviolabilidad de los Recintos Privados	Art. 12 - Protección del domicilio	Art. 11 Protección de la Honra y de la Dignidad	ALTO	Sobrevuelo de propiedades privadas, grabación de interiores, vigilancia domiciliaria
Libertad de Tránsito	Art. 41 Del Derecho al tránsito y a la Residencia	Art. 13	Art. 22 Derecho de Circulación y de Residencia	MEDIO	Restricciones de vuelo que limiten el tránsito, identificación y seguimiento de personas.
Libertad de Expresión	Art. 26 De la Libertad de expresión y de Prensa	Art. 18 Libertad de Pensamiento y Creencias y Art. 19 Libertad de Opinión y Expresión.	Art. 13 Libertad de Pensamiento y de Expresión	ALTO	Vigilancia de manifestaciones, identificación de participantes, efecto disuasivo o inhibidor.
Libertad de Reunión	Art. 32 De la Libertad de Reunión y de Manifestación	Art. 20 Libertad de reunión	Art. 15 Derecho de Reunión	ALTO	Vigilancia de reuniones, identificación de participantes, dispersión por intimidación.
Derecho a la Imagen	Art. 33 Del Derecho a la Intimidad (protege la imagen privada)	Art. 12 Protección contra injerencias	Art. 11 Protección de la Honra y de la Dignidad.	ALTO	Grabación no autorizada, difusión de imágenes, reconocimiento facial.

Protección de Datos	Art. 33 - Del Derecho a la Intimidad; Art. 34 Del Derecho a la Inviolabilidad de los Recintos Privados	Art. 12 Protección contra injerencias	Art. 11 Protección de la Honra y de la Dignidad.	ALTO	Recopilación masiva de datos biométricos[20], creación de perfiles, almacenamiento no autorizado de datos.
Derecho a la Seguridad	Art. 9 De la Libertad y seguridad de las personas	Art. 3	Art. 7 Derecho a la Libertad Personal (incluye el derecho a la seguridad personal)	AMBIVA-LENTE	Puede mejorar la seguridad pública pero existen riesgos de vigilancia excesiva.
Debido Proceso y presunción de inocencia	Art. 17 De los derechos procesales	Art. 10 - Derecho a ser oído públicamente; Art. 11 - Presunción de Inocencia	Art. 7 Derecho a la Libertad Personal; Art. 8 Garantías Judiciales	MEDIO	Uso de evidencia obtenida por drones sin autorización judicial. Posible vigilancia preventiva masiva que presume culpabilidad
De la no discriminación y la Igualdad ante la Ley	Art. 46 De la Igualdad de las personas y Art. 47 de las garantías de la igualdad.	Artículos 2 y 7	Art. 1 Obligación de Respetar los Derechos; Art. 24 Igualdad ante la Ley	ALTO	Vigilancia selectiva basada en perfiles discriminatorios; falsos positivos derivados de bases de datos sesgadas o no representativas; segmentación desigual del espacio público.

Fuente: De elaboración propia.

Como se desprende del análisis comparativo, los drones están lejos de ser una tecnología neutral. Su uso puede servir como herramienta de vigilancia altamente intrusiva, con impactos adversos sobre derechos humanos garantizados normativamente, especialmente cuando se carece de límites definidos o mecanismos adecuados de control. Esta preocupación no es abstracta, dado a que existen numerosos casos documentados a nivel regional[21] y global donde el uso de estas tecnologías ha derivado en afectaciones graves a derechos.

20 Los datos biométricos son "aquellos datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona humana, que permitan o confirmen su identificación única." (Vaninetti, 2020, Tomo I, p. 177).

21 Durante eventos masivos como el Carnaval de Río, las autoridades brasileñas han utilizado drones con cámaras de reconocimiento facial para monitorear multitudes. En 2019, en Salvador de Bahía, esta tecnología generó múltiples falsos positivos, incluyendo la detención injustificada de personas. Un informe de la Rede de Observatórios da Segurança reveló que el 96% de los alertas fueron ineficaces y el 90,5% de los detenidos eran personas negras. Estos casos ilustran los riesgos del uso combinado de drones y tecnologías biométricas, especialmente en espacios públicos festivos, donde pueden vulnerar derechos como la privacidad, la presunción de inocencia y la no discriminación. Véase: Lourenco, B. (2025, marzo 01). *O reconhecimento facial no carnaval não protege, ele controla*. Opinión. CartaCapital. https://www.cartacapital.com.br/opiniao/o-reconhecimento-facial-no-carnaval-nao-protege-ele-controla/.

En el caso específico del derecho a la seguridad ciudadana, entendido como el "conjunto de acciones estatales orientadas a garantizar la protección y bienestar de la población" (Izquierdo-Alvear, 2024), resulta indispensable que el uso de tecnologías de vigilancia, incluido los drones, no justifique bajo su nombre formas de control o monitoreo que generan temor o inhiban la participación ciudadana.

La experiencia histórica de nuestra región, incluido Paraguay, sirve de ejemplo para ilustrar sobre el riesgo de normalizar mecanismos de vigilancia sin transparencia ni garantías, especialmente cuando estas tecnologías se insertan en lógicas autoritarias o desiguales. Por ello, cualquier avance en materia de tecnología aplicada a la seguridad debe sostenerse sobre límites claros de respeto a la dignidad humana. La tecnología puede y debe contribuir al bien común, pero nunca a costa de erosionar derechos y garantías que costaron décadas de lucha y memoria.

PRIVACIDAD EN EL ESPACIO PÚBLICO DIGITALIZADO

La expansión del uso de drones, tanto por entidades públicas como privadas, plantea desafíos serios al derecho a la privacidad, especialmente en contextos donde los marcos normativos no evolucionan al ritmo de la innovación tecnológica. Estos desafíos se dan, debido a que los drones "realizan una peculiar recolección de datos fotográficos, fílmicos y sonoros de personas, en visión aérea y en algunos casos normalmente no detectables" (Vaninetti, 2020. Tomo I, p. 185).

En Paraguay, el derecho a la privacidad —en sentido amplio— goza de protección constitucional y está respaldado por instrumentos internacionales como el Artículo 12 de la Declaración Universal de Derechos Humanos y el Artículo 17 del Pacto Internacional de Derechos Civiles y Políticos —ya mencionados en la sección anterior—, pero su efectividad se ve limitada por la ausencia de una legislación integral sobre protección de datos personales[22]. Como ha señalado TEDIC en reiteradas ocasiones[23], si bien existen herramientas legales para invocar este derecho, su eficacia depende de la existencia de límites normativos claros que regulen prácticas como la captación de imágenes y datos personales sin consentimiento.

Aunque en Paraguay no existe jurisprudencia específica sobre el uso de drones, la Constitución Nacional protege la inviolabilidad del patrimonio documental y de las comunicaciones privadas (registros, escritos, llamadas telefónicas, etc.). El acceso a esta información solo puede ser autorizado judicialmente en casos expresamente previstos por la ley, y debe realizarse con estricta reserva de aquello que no guarde relación con la investigación. Además, el Artículo 30 de la Constitución establece que las autoridades deben garantizar que las señales de comunicación electromagnética no se utilicen para vulnerar la intimidad personal o familiar. Tal como sostiene Galli (2024), si bien el país carece de una legislación integral sobre protección de datos personales, ello no impide que el derecho a la privacidad pueda ser invocado y defendido jurídicamente en diversos contextos.

22 Al momento de redacción de este trabajo, el proyecto de Ley de Protección de Datos Personales (Exp. D-2162170) fue aprobado por Diputados el 27 de mayo de 2025 y está en estudio en Senadores. Más información en SilPy: https://silpy.congreso.gov.py/web/expediente/123459.

23 Véase: TEDIC. (2025, 17 de julio). *Paraguay necesita una ley de protección de datos personales robusta, con estándares internacionales y garantías reales* [Entrada de blog]. https://www.tedic.org/paraguay-necesita-una-ley-de-proteccion-de-datos-personales-robusta-con-estandares-internacionales-y-garantias-reales/

Ahora bien, a partir de las respuestas institucionales obtenidas mediante solicitudes de acceso a la información pública, se tiene que, ningún organismo estatal consultado ha reportado la existencia de protocolos específicos que anticipen los impactos de estas tecnologías sobre la privacidad. Aunque el MITIC (2025) ha mencionado que toda operación con drones requiere autorización de la DINAC y justificación legal documentada, ello no garantiza por sí solo una evaluación rigurosa de los impactos sobre derechos humanos. Por su parte, la Defensoría del Pueblo ha afirmado no registrar antecedentes específicos sobre denuncias vinculadas al uso de drones, lo que más que reflejar una inexistencia de afectaciones, evidencia un vacío institucional y una falta de mecanismos de monitoreo efectivos.

No obstante, incluso una revisión superficial de fuentes públicas revela indicios preocupantes sobre el uso de tecnologías de vigilancia con potencial intrusivo. En el portal de la Dirección Nacional de Contrataciones Públicas (DNCP) puede encontrarse, por ejemplo, la Licitación N.º 471787, titulada "Compra de drones de vigilancia y sus accesorios para la ANNP" (Administración Nacional de Navegación y Puertos), cuyo objetivo declarado es la seguridad institucional mediante controles diurnos y nocturnos[24].

Sin embargo, las especificaciones técnicas del pliego detallan la adquisición de drones con capacidades avanzadas, como cámaras gran angular de al menos 48 MP, zoom óptico, cámara térmica, grabación en 4K y estabilización mecánica de 3 ejes. Estas características permiten una captación precisa y continua de imágenes, incluso en condiciones de baja visibilidad, lo que excede con creces el monitoreo básico de instalaciones. Así, independientemente del fin alegado, instituciones públicas están adquiriendo equipos con alta capacidad de vigilancia, sin que exista informes sobre la realización de evaluaciones de impacto en derechos fundamentales, como la privacidad y la protección de datos personales.

Recordemos que, los drones pueden recopilar datos con un nivel de detalle sin precedentes, desde imágenes en alta definición hasta la posible detección de señales de telefonía móvil (Boyle, 2020). Esta capacidad técnica, sumada a la ausencia de regulación, habilita un modelo de vigilancia persistente, en el que la observación se realiza de forma constante, remota y muchas veces silenciosa. La vigilancia deja de ser episódica para convertirse en una posibilidad omnipresente, erosionando progresivamente la expectativa razonable de privacidad en espacios públicos. Como advierten Balmaceda, Schleider y Pedace (2021), "la vigilancia ocupa cada vez más lugar en nuestras vidas. Y, para ocuparlo, está quitándole su espacio a la privacidad" (p. 23).

24 Véase: DNCP. (2025, junio 30). Convocatoria de la Licitación 471787. "Compra de drones de vigilancia y sus accesorios para la ANNP". https://www.contrataciones.gov.py/licitaciones/convocatoria/1f047be6-591c-68b6-86f1-cf1a04e1d9e5.html#pliego

Si bien, la Corte Interamericana de Derechos Humanos (CIDH), ha reconocido jurisprudencialmente, en el caso Tristán Donoso vs. Panamá[25] (2009), que el derecho a la privacidad no es un derecho absoluto. Aún así, ha establecido como regla que la limitación de dicho derecho debe observar a un análisis exhaustivo, analizando la proporcionalidad de las medidas de vigilancia adoptadas.

> El derecho a la privacidad [...] puede ser restringido por los Estados. Esto, siempre que las injerencias no sean abusivas o arbitrarias. Por lo cual, el límite a esas restricciones debe ser: (i) estar previstas en ley; (ii) perseguir un fin legítimo y (iii) cumplir con los requisitos de idoneidad, necesidad y proporcionalidad, es decir, deben ser necesarias para una sociedad democrática.

Siguiendo esta línea argumentativa, la misma CIDH, en el caso *Escher y otros vs. Brasil*[26] (2009), se refirió a lo que venimos advirtiendo en este trabajo, que el avance tecnológico plantea desafíos importantes con el derecho a la privacidad y está no puede ser ignorada.

> La fluidez informativa que existe hoy en día coloca al derecho a la vida privada de las personas en una situación de mayor riesgo debido a las nuevas herramientas tecnológicas y su utilización cada vez más frecuente. Este progreso [...] no significa que las personas deban quedar en una situación de vulnerabilidad frente al Estado o a los particulares. De allí que el Estado debe asumir un compromiso, aún mayor, con el fin de adecuar a los tiempos actuales las fórmulas tradicionales de protección del derecho a la vida privada.

Considerando este criterio, se debe considerar que, en la actualidad la privacidad ya no se refiere solamente al espacio solitario o individual de reclusión, en el entendimiento jurídico contemporáneo, esta incluye ya una serie de variables que van configurando la expectativa de privacidad con la que las personas esperan moverse en espacios públicos. Ya que incluso las actividades que las personas realizan en estos espacios pueden estar cubiertas con una *razonable expectativa de privacidad*[27]. La privacidad es crucial para la autodeterminación, porque define la forma en que una persona se presenta ante las demás personas, así como el tipo de relaciones sociales que se sustentan en el marco de este sistema.

Un ejemplo paradigmático en Paraguay fue el caso del monitoreo aéreo de una residencia privada vinculada al actual presidente, lo que generó un breve debate sobre los límites de esta tecnología y motivó pedidos de informes (El Nacional, 2025). Sin embargo, este tipo de cuestionamientos parecen activarse solo ante la afectación de personas con visibilidad pública. Esto conlleva preguntarnos: ¿qué sucede cuando las víctimas son personas comunes, sin acceso a mecanismos de defensa institucional? ¿Cuántos episodios de vigilancia silenciosa y no consentida deben reportarse para que se cuestione la naturalización del monitoreo masivo?

---

25 Corte Interamericana de Derechos Humanos. Tristán Donoso v. Panamá. Sentencia de 27 de enero de 2009. Serie C No. 193. https://www.corteidh.or.cr/docs/casos/articulos/seriec_193_esp.pdf

26 Corte Interamericana de Derechos Humanos. Escher y otros vs. Brasil. Sentencia de 6 de julio de 2009. https://www.corteidh.or.cr/docs/casos/articulos/seriec_200_esp1.pdf

27 La "expectativa razonable de privacidad" es un estándar jurídico originado en el caso *Katz v. United States* (1967), según el cual una persona puede esperar que ciertas acciones o comunicaciones permanezcan privadas, incluso en espacios públicos, siempre que esa expectativa sea socialmente reconocida como legítima. Por ejemplo, alguien caminando por un parque tranquilo podría razonablemente esperar no ser grabado ni seguido por un dron, a diferencia de quien asiste a una manifestación pública frente al Congreso, donde la vigilancia puede estar más justificada aunque no ilimitada. Esta distinción resulta clave al evaluar si una intervención vulnera o no el derecho a la privacidad.

La filósofa Shoshana Zuboff (2019), en su análisis del capitalismo de vigilancia, alerta sobre esta tendencia, advirtiendo que se espera ver drones, sensores corporales, neurotransmisores, asistentes digitales y otros dispositivos con sensores como nuevas fuentes de excedente de comportamiento, en un modelo que "ignora las normas sociales y anula los derechos elementales asociados con la autonomía individual" (p. 11).

Frente a este escenario, resulta crucial replantear los alcances del derecho a la privacidad más allá del ámbito doméstico. La intimidad también implica el derecho a desplazarse, expresarse y reunirse en espacios públicos sin estar bajo constante vigilancia. Por ello, urge la elaboración de marcos normativos que no solo limiten el uso de drones, sino que establezcan mecanismos efectivos de transparencia, rendición de cuentas y control judicial. Estos deben incluir regulaciones claras sobre el acceso, uso y almacenamiento de los datos recolectados, así como sanciones frente a abusos.

En última instancia, proteger la privacidad en el espacio público digitalizado no es solo una cuestión técnica o legal, sino una defensa fundamental del derecho de las personas a vivir sin ser observadas, sin ser objeto constante de extracción de datos, y sin que su libertad quede condicionada por el miedo a ser vigiladas.

LIBERTAD DE EXPRESIÓN Y DERECHO A LA PROTESTA ANTE LA AMENAZA DE VIGILANCIA AÉREA

El uso de drones en contextos de protesta social presenta una dinámica ambivalente. Por un lado, han sido empleados por activistas y medios comunitarios como herramientas de documentación y denuncia frente a episodios de represión, ampliando la capacidad de registro ciudadano. Por otro lado, su despliegue por parte de fuerzas estatales plantea serios riesgos para derechos fundamentales como la libertad de expresión, de reunión y el derecho a la protesta pacífica.

Aunque pueden ofrecer ventajas operativas, como vistas aéreas en tiempo real y detección de riesgos, su utilización como mecanismo de vigilancia selectiva e intimidación puede generar un efecto inhibidor sobre la participación ciudadana y el disenso. Estas libertades, pilares esenciales de toda sociedad democrática, no solo garantizan la expresión plural de ideas, sino que permiten el control social del poder público. En esta línea, la CIDH ha subrayado que la libertad de expresión es una piedra angular en la estructura de una sociedad democrática, y que su pérdida pone en riesgo los principios esenciales que sostienen dicho sistema[28].

Casos como el de Colombia durante el estallido social de 2021 (Fundación Karisma, 2021) o el de Argentina en 2023, dan cuenta de esta dinámica: drones sobrevolando manifestaciones, captando imágenes de personas sin su consentimiento y generando una sensación de monitoreo constante. En el caso argentino, incluso se utilizaron las imágenes captadas para amenazar a manifestantes con el recorte de beneficios sociales, demostrando cómo la vigilancia puede convertirse en una forma de disciplinamiento y castigo selectivo (R3D, 2023).

28 Véase: Corte Interamericana de Derechos Humanos (CIDH). (1985). *Opinión Consultiva OC-5/85 del 13 de noviembre de 1985. La colegiación obligatoria de periodistas (arts. 13 y 29 Convención Americana sobre Derechos Humanos).*https://www.corteidh.or.cr/tablas/a12040.pdf

Por su parte, en Paraguay, entes consultados en el marco de esta investigación, como el MITIC (2025) y la Defensoría del Pueblo (2025), han señalado que no se han utilizado drones para el monitoreo de manifestaciones o reuniones públicas. Asimismo, el Ministerio del Interior (2025) —institución responsable de la coordinación de las fuerzas de seguridad interna— no ha respondido de forma exhaustiva al cuestionario remitido, cuyo objetivo era conocer si las fuerzas policiales emplean drones para vigilar protestas o movilizaciones sociales. En su lugar, la respuesta se limitó a señalar que "en dependencias tecnológicas del Ministerio del Interior no existe ni se utilizan drones", sin aclarar si otras unidades o fuerzas subordinadas cuentan con este tipo de tecnología ni si se han realizado despliegues en coordinación con otras instituciones[29]. A pesar de ello, no se puede omitir que, TEDIC ha documentado formas de vigilancia durante manifestaciones "mediante cámaras con reconocimiento facial y drones" (Ramirez, 2015)[30].

El efecto inhibidor de estas prácticas no es menor. Tal como advierten López y Torres (2021), el uso excesivo de drones en protestas puede ser percibido como vigilancia masiva, lo que reduce el margen de expresión ciudadana y erosiona el principio de libertad en la participación democrática. En este sentido, cuando las personas sienten que están siendo vigiladas, pueden autocensurarse o desistir de asistir a manifestaciones, especialmente aquellas que pertenecen a colectivos históricamente estigmatizados o reprimidos. En palabras de García y Pérez (2023), cualquier restricción a la libertad de expresión o reunión debe ser "proporcional", de conformidad con los estándares internacionales de derechos humanos. Esto implica que la mera posibilidad de desórdenes o la supuesta necesidad de mantener el orden público no puede justificar por sí misma el uso intensivo de tecnologías de vigilancia aérea.

A nivel global, Rusia ha utilizado drones para vigilar protestas pro-democráticas desde 2012, y la Guardia Rusa emplea esta tecnología para monitorear manifestaciones políticas (Boyle, 2020). Otro caso más reciente, en la India, ilustra de forma elocuente el poder disuasorio y represivo de estas tecnologías (Saaliq, 2024). En febrero de 2024, la policía reprimió una protesta de agricultores arrojando gas lacrimógeno desde drones sobre una multitud que se dirigía a Nueva Delhi. Este tipo de prácticas, además de vulnerar el derecho a la protesta, ilustran un preocupante uso de tecnologías aéreas que reemplaza la mediación humana y agrava los riesgos de uso excesivo de la fuerza.

El escenario se agrava aún más en contextos autoritarios o con institucionalidad débil, donde el anonimato en la disidencia política se vuelve una condición de seguridad básica. Como advierte la literatura internacional, el avance de tecnologías como los drones podría hacer que "el disenso anónimo eventualmente se vuelva imposible", al permitir a los gobiernos monitorear, identificar y sancionar a manifestantes sin necesidad de presencia física (Boyle, 2020). En estos escenarios, el costo de la participación política se eleva drásticamente, consolidando regímenes de vigilancia que socavan la democracia desde su base ciudadana.

29 Para conocer el documento remitido, véase: Ministerio del Interior. (2025, julio 10). Memorándum DGTYC № 055/2025. Solicitud 93397. Portal Unificado de Información Pública. https://informacionpublica.paraguay.gov.py/#!/ciudadano/solicitud/93402https://informacionpublica.paraguay.gov.py/#!/ciudadano/solicitud/93397

30 Ver: Ramírez, A. (2025, mayo 13). IMSI catchers en Paraguay: La vigilancia invisible que amenaza tu derecho a manifestarte [Entrada de blog]. TEDIC. https://www.tedic.org/imsi-catchers-en-paraguay-la-vigilancia-invisible-que-amenaza-tu-derecho-a-manifestarte/

En vista de lo expuesto, resulta imprescindible subrayar que el uso de drones en contextos de protesta debe regirse por un irrestricto respeto a los derechos humanos. Estas tecnologías no pueden transformarse en instrumentos para criminalizar el disenso, vigilar de forma selectiva a cuerpos disidentes (Silva & Varón, 2021), ni para generar bases de datos sin consentimiento informado (Vaninetti, 2020, Tomo I, p. 180). Una sociedad verdaderamente democrática no se define solo por su capacidad de innovar, sino por su compromiso con proteger el disenso. En esta misma línea argumentativa, ya en 2020, la Alta Comisionada de las Naciones Unidas para los Derechos Humanos advirtió con firmeza que las nuevas tecnologías —como los drones con alta capacidad de vigilancia— no deben ser utilizadas para rastrear, intimidar o reprimir a quienes ejercen su derecho a la protesta pacífica (Naciones Unidas, 2020).

LEGALIDAD Y PROPORCIONALIDAD EN MEDIDAS DE VIGILANCIA TECNOLÓGICA

Cualquier análisis sobre los desafíos que plantea el uso de drones no puede realizarse de forma aislada, sino enmarcado en un contexto más amplio: el impacto que las tecnologías emergentes, particularmente aquellas destinadas a la vigilancia, tienen sobre el derecho. A este respecto, el despliegue de drones con fines de seguridad debe evaluarse conforme con estándares de derechos humanos. Aun en ausencia de una regulación específica, existen principios y herramientas jurídicas —como el examen proporcionalidad— que permiten establecer límites claros al poder estatal y privado, asegurando que toda intervención tecnológica respete el marco democrático y garantista.

En Paraguay no contamos con una legislación específica sobre el uso de drones con enfoque en Derechos Humanos, aunque se ha planteado su consideración. A nivel operativo, instrumentos como la Resolución DINAC Nº 2170/17[31] establecen requisitos técnicos y de seguridad aeronáutica, pero no abordan el impacto sobre derechos fundamentales. Ello no obsta que hablemos que la implementación de estas tecnologías no puedan observar criterios de legalidad, pues existe un marco normativo que exige la observancia de ciertas normas con el fin de proteger derechos humanos. Considerando ello, deberían observarse siempre las bases legales para justificar un uso no intrusivo de drones.

Según el Comité de Derechos Humanos de la ONU (1988)[32], toda medida de vigilancia debe estar "claramente delimitada por la ley", ajustarse a los principios de necesidad y proporcionalidad, y estar sujeta a supervisión judicial. En esta misma línea, desde el 2014, organizaciones de la sociedad civil como la Electronic Frontier Foundation (EFF)[33] ha insistido en que todo uso de tecnologías de vigilancia (en nuestro caso aplicado considerando los drones) debe respetar los principios de "necesidad y proporcionalidad", extendiendo dicha obligación a los actores privados. Asimismo, recordemos el caso citado de la CIDH más arriba donde también se hace énfasis en que medidas de vigilancia por actores estatales, y extendiendo un poco la consideración, actores privados con intereses de vigilancia masiva o intrusivas, deben también observar a criterios estrictos de legalidad y proporcionalidad.

---

31 Para acceder a la resolución, véase: DINAC. (2017). *Resolución N° 2170/2017: Por la que se aprueba el Reglamento DINAC R 1103 - Reglamento de Aeronaves Piloteadas a Distancia (RPA) y Sistema de Aeronaves Piloteadas a Distancia (RPAS)*. Dirección Nacional de Aeronáutica Civil. https://www.dinac.gov.py/v3/index.php/documentos1/leyes-decretos-resoluciones-circulares/item/1814-resolucion-n-2170-2017-por-la-que-se-aprueba-el-reglamento-dinac-r-1103-reglamento-de-aeronaves-piloteadas-a-distancia-rpa-y-sistema-de-aeronaves-piloteadas-a-distancia-rpas

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

33 Véase: EFF. (2014). *Necesarios y Proporcionados: sobre la aplicación de los Derechos Humanos a la vigilancia de las Comunicaciones*. https://necessaryandproportionate.org/es/principios/

Considerando estos argumentos, ante una ausencia regulatoria específica, el examen de proporcionalidad —con base en la doctrina de Robert Alexy[34]— ofrece un marco analítico robusto para evaluar la legitimidad del uso de drones. Este examen propuesto permite analizar si una medida que afecta derechos fundamentales puede considerarse constitucionalmente válida, a través de tres submandatos: idoneidad, necesidad y proporcionalidad en sentido estricto. Bajo la línea argumentativa de la doctrina de Alexy (1993), si una intervención estatal o privada no supera alguno de estos niveles de escrutinio, debe considerarse desproporcionada y, en consecuencia, jurídicamente inadmisible. En este sentido, el examen de proporcionalidad no solo permite valorar si el uso de tecnologías como los drones cumple con fines legítimos, sino también si lo hace de manera compatible con un orden democrático que prioriza la protección de derechos humanos. Tal como se ha advertido, en su estructura clásica, dicho test exige verificar de manera sucesiva, tres submandatos específicos:

1. **Idoneidad:** ¿La medida contribuye eficazmente al fin propuesto (por ejemplo, seguridad pública)?
2. **Necesidad:** ¿Existen medios menos lesivos, como cámaras fijas, mayor presencia humana o drones sin captura biométrica, para la concreción del fin buscado?
3. **Proporcionalidad en sentido estricto:** ¿El beneficio de la intervención justifica el impacto sobre derechos fundamentales como la privacidad o la libertad de reunión?

Este examen resulta especialmente importante en contextos donde existe un riesgo considerable a Derechos Humanos como protestas o patrullajes preventivos, donde el uso de drones puede generar efectos inhibidores o discriminatorios. Conforme al test de proporcionalidad, cuando la aplicación de un principio —como la seguridad pública— entra en colisión con otro principio contrapuesto —como la libertad de expresión o la privacidad—, corresponde evaluar si el beneficio que se deriva de proteger el primero justifica el grado de restricción impuesto sobre el segundo (Pérez-Trech, 2022. p. 66). Esta ponderación es esencial para evitar que medidas adoptadas en nombre del orden terminen erosionando garantías democráticas fundamentales. Asimismo, el test de proporcionalidad es especialmente crítica ante usos de drones por parte de actores privados, donde la falta de límites claros agrava la asimetría entre quienes desarrollan tecnologías intrusivas de vigilancia, las implementan y quienes las padecen.

En este contexto, la ausencia de salvaguardas como evaluaciones de impacto, participación ciudadana o límites jurídicos claros no solo compromete la legitimidad del despliegue masivo de drones, sino que habilita escenarios de abuso bajo el argumento de intereses legítimos. Por ello, en línea con las posturas citadas al inicio de este segmento, el examen de proporcionalidad debe ser entendido como una herramienta clave para orientar decisiones institucionales desde el inicio. Su aplicación no debería limitarse a una revisión posterior, sino integrarse en las etapas tempranas del diseño, regulación e implementación de tecnologías intrusivas, con el fin de prevenir violaciones de derechos fundamentales.

34 Robert Alexy es un reconocido jurista y filósofo del derecho alemán, cuya teoría de los derechos fundamentales y del principio de proporcionalidad ha tenido una influencia decisiva en la jurisprudencia constitucional contemporánea. Su formulación del test de proporcionalidad (compuesto por los subprincipios de idoneidad, necesidad y proporcionalidad en sentido estricto) se ha consolidado como una herramienta clave para evaluar la legitimidad de restricciones a derechos fundamentales. Su propuesta permite ponderar racionalmente conflictos entre principios y establecer límites jurídicamente justificados a medidas intrusivas, lo que la convierte en un estándar adoptado tanto por cortes constitucionales como por instrumentos internacionales de Derechos Humanos.

VIGILANCIA ESTATAL, CONTROL SOCIAL Y ESTRUCTURAS DE PODER

Esta sección se propone delimitar el contexto actual de la vigilancia estatal mediada por tecnologías digitales, un fenómeno que ha despertado creciente preocupación desde la perspectiva de los Derechos Humanos. Como señalan Secaf, Carrillo y Paschoalini (2023, p.12), la vigilancia no puede entenderse como una simple observación pasiva, sino como un proceso sistemático compuesto por tres elementos fundamentales: observar, generar conocimiento e intervenir. En este marco, tecnologías como los drones permiten una inspección focalizada y continua sobre individuos o poblaciones, con la capacidad de identificar patrones de conducta y, en última instancia, condicionar comportamientos. La vigilancia, así entendida, deja de ser neutral y se convierte en una herramienta activa de control social.

Por ello, el uso de drones y otras tecnologías similares no debe analizarse de forma aislada, sino como parte de un entramado más amplio que reproduce y amplifica dinámicas históricas de concentración de poder y debilitamiento de garantías individuales. Estas prácticas deben interpretarse a la luz de conceptos contemporáneos como el extractivismo de datos, desarrollado teóricamente por Shoshana Zuboff (2019). Bajo esta mirada, las tecnologías digitales no representan meras innovaciones funcionales, sino formas actuales de dominación que trasladan al entorno digital actual lógicas preexistentes de explotación, jerarquización y desigualdad.

El extractivismo de datos describe una práctica sistemática de recolección masiva, opaca y, a menudo, no consensuada de información personal —especialmente sensibles como los datos biométricos y geoespaciales— por parte de actores estatales o corporativos[35]. Esta forma de extracción replica las dinámicas coloniales asociadas al saqueo de recursos naturales, pero dirigidas ahora al plano informacional[36]. En este modelo, la ciudadanía produce los datos, pero no tiene control sobre su uso, procesamiento ni destino final, lo que evidencia una profunda asimetría de poder.

La arquitectura resultante normaliza un tipo de vigilancia omnipresente pero poco visible, que se justifica en nombre de valores aparentemente incuestionables como la seguridad, la eficiencia o la prevención del delito, sin que existan mecanismos de transparencia o control adecuados. Esta estructura institucionaliza la excepción: medidas introducidas como respuestas extraordinarias se consolidan como prácticas rutinarias. Como advierte Pérez Trench (2024, p. 65), nos enfrentamos a una tensión clásica —aunque no resuelta— entre el interés estatal por garantizar la seguridad pública y los derechos fundamentales constitucionalmente protegidos. “Se trata de la ya clásica tensión entre seguridad y libertad [...] y como cualquier avezado lector podrá darse cuenta, es un problema que no parece tener solución”.

Lo preocupante en el contexto actual es que esta tensión se resuelve sistemáticamente a favor de la expansión del poder estatal de vigilancia. El Estado justifica la ampliación de sus capacidades de monitoreo en nombre de su “poder de policía”[37], mientras debilita progresivamente la posibilidad ciudadana de resistir, cuestionar o incluso conocer el alcance real de dichas prácticas. Esta asimetría informacional constituye una forma silenciosa pero profunda de erosión del control democrático.

---

35 Sobre el punto, TEDIC ha señalado que, estos procesos suelen llevarse a cabo sin consentimiento informado, sin mecanismos claros de control ciudadano y sin transparencia respecto a quién administra los datos, con qué fines, durante cuánto tiempo y bajo qué condiciones de seguridad. Ver: TEDIC. (2025, julio 23). *Expo Paraguay 2025: Vigilancia, desprotección y exclusión a la ciudadanía* [Entrada de blog]. https://www.tedic.org/-expo-paraguay-2025-vigilancia-desprotecciony-exclusion-a-la-ciudadania/

36 El *colonialismo de datos* describe una nueva fase de apropiación sistemática de información personal que reproduce lógicas extractivas coloniales en el entorno digital, particularmente sobre poblaciones vulnerables (Couldry & Mejias, 2019).

37 Por *poder de policía* se entiende la facultad del Estado para intervenir en la vida de las personas a fin de mantener el orden y gestionar lo público, aun cuando ello implique imponer límites o restricciones.

Este patrón se manifestó con claridad durante esta investigación en las respuestas institucionales obtenidas. El Ministerio del Interior respondió de forma escueta y evasiva, mientras que la Secretaría Nacional Antidrogas (SENAD) negó proporcionar información, invocando genéricamente "razones de seguridad nacional". Sin embargo, las consultas no buscaban detalles operativos ni tácticos, sino determinar si el Estado paraguayo ha adquirido y desplegado drones, en qué contextos institucionales y bajo qué resguardos legales y procedimentales. Paradójicamente, parte de esta información es accesible en el portal de la DNCP, donde se publicó la adjudicación de la Licitación Nº 435980, correspondiente a la "Adquisición de drones con accesorios"[38] para dicho ente público —también adjudicada a DataSystems— por un monto superior a ₲ 150.000.000, incluyendo el modelo DJI Matrice 300 RTK.

Esta negativa sistemática, sumada a la falta de transparencia en los procesos de adquisición y uso, no solo confirma una preocupante opacidad institucional, sino que revela, en lo profundo, una cultura política que se resiste a ser controlada y que desestima el valor democrático del escrutinio público. Lo que Zuboff (2019) denomina "capitalismo de vigilancia" encuentra en este contexto, un correlato estatal donde se observa la acumulación de datos como forma de poder, como capital político al servicio del control, operando sin transparencia, sin garantías y sin rendición de cuentas.

Prácticas de monitoreo, como el uso de tecnologías de vigilancia como los drones, que en otro tiempo habrían sido consideradas excepcionales o incluso ilegítimas, hoy se incorporan a la rutina burocrática, justificadas por discursos de modernización o eficiencia. Lejos de ofrecer genuinamente mayor seguridad ciudadana, esta arquitectura tecnológica de vigilancia parece apuntar a la consolidación de un modelo sutilmente autoritario, disfrazado de innovación administrativa. No podemos perder de vista que, lo que está en juego no es solo el uso de nuevas herramientas, sino el modo en que éstas reconfiguran las relaciones entre Estado y ciudadanía, entre control y libertad.

EL PANÓPTICO DIGITAL Y EL CONTROL AÉREO

La arquitectura de vigilancia contemporánea encuentra sus antecedentes conceptuales en el panóptico, modelo de prisión ideado por el filósofo utilitarista Jeremy Bentham en 1791. Su diseño arquitectónico permitía vigilar a todos los internos desde una torre central, minimizando el uso de recursos humanos y materiales mientras maximizaba la eficacia del control. Inspirado en la raíz griega *panoptikon* ("verlo todo"), este modelo trascendió su función carcelaria original para convertirse en una poderosa metáfora que describe las nuevas modalidades de vigilancia estatal en el siglo XXI.

La genialidad del panóptico benthamiano no residía únicamente en su eficiencia operativa, sino en su dimensión psicológica: los prisioneros, al no poder determinar cuándo estaban siendo observados, internalizaban la vigilancia como una presencia constante. Esta lógica de la "mirada invisible pero omnipresente" se actualiza dramáticamente en el contexto de las tecnologías de vigilancia aérea contemporáneas, donde la incertidumbre sobre el monitoreo se convierte en un mecanismo de disciplinamiento social generalizado.

38 DNCP. (2023, octubre 10). Convocatoria de la Licitación Nº 435980 - "Adquisición de drones con accesorios". https://www.contrataciones.gov.py/licitaciones/adjudicacion/435980-adquisicion-drone-accesorios-1/resumen-adjudicacion.html

En este marco conceptual, el despliegue de drones equipados con sensores térmicos, cámaras de alta resolución y luces deliberadamente encendidas durante operaciones nocturnas refleja una evolución sofisticada de la lógica panóptica original. Esta tecnología opera bajo una doble estrategia de poder: por un lado, "ver sin ser visto" —capacidad de observación remota y discrecional—; por otro, "hacerse notar estratégicamente" para recordar a la población que se encuentra bajo vigilancia potencial permanente.

Esta dualidad táctica representa una innovación significativa respecto al panóptico clásico. Mientras Bentham diseñó un sistema de vigilancia arquitectónicamente fijo y espacialmente delimitado, los drones configuran un panóptico móvil, flexible y territorialmente expansivo. Su capacidad de desplazamiento tridimensional y de reconfiguración operativa en tiempo real permite extender la lógica de control carcelario a espacios urbanos, rurales y fronterizos, transformando potencialmente todo el territorio nacional en un espacio de vigilancia latente.

Estos dispositivos, cada vez más autónomos, ubicuos y económicamente accesibles, pueden incorporar tecnologías de IA como el reconocimiento facial, el análisis predictivo de comportamientos y la identificación biométrica remota, intensificando exponencialmente las capacidades de vigilancia selectiva del Estado (Mobilio, 2023; Berle, 2020). Esta convergencia tecnológica no solo amplifica el poder de observación estatal, sino que introduce elementos de automatización que pueden operar con mínima intervención humana, creando las condiciones para formas de control social algorítmicamente mediadas.

La selectividad de esta vigilancia resulta particularmente problemática desde una perspectiva de derechos humanos. La capacidad de estos sistemas para identificar, rastrear y catalogar individuos específicos —basándose en criterios potencialmente discriminatorios o políticamente motivados— transforma la vigilancia de un mecanismo general de seguridad pública en una herramienta de control político diferenciado.

En contextos de alta conflictividad política y contestación social, como el documentado en Venezuela tras las controvertidas elecciones presidenciales (Alarcón, 2024), la presencia conspicua de drones sobrevolando manifestaciones ciudadanas y la exhibición oficial de modelos armados —como los ANSU 100 y 200, vinculados a transferencia tecnológica iraní— (Bermúdez, 2022) representan una escalada cualitativamente preocupante hacia formas de represión tecnológicamente mediadas y potencialmente letales.

Esta evolución marca una transición crítica desde la vigilancia hacia la coerción directa. Cuando los dispositivos de observación incorporan capacidades ofensivas, el panóptico digital se transforma en lo que podríamos denominar un "panóptico armado", donde la amenaza de violencia se integra estructuralmente en la arquitectura de vigilancia. Esta convergencia entre observación y capacidad letal automatizada plantea interrogantes fundamentales sobre los límites constitucionales del poder estatal y los mecanismos de control democrático sobre tecnologías inherentemente duales.

En escenarios caracterizados por la militarización progresiva del orden público, esta convergencia entre vigilancia aérea omnipresente y capacidad ofensiva automatizada configura lo que podríamos conceptualizar como un "régimen de control territorial algorítmico". En este régimen, el poder estatal de observación se entrelaza sistémicamente con la amenaza credible de fuerza, operando frecuentemente sin garantías claras de legalidad, proporcionalidad ni supervisión democrática efectiva.

Este modelo representa una síntesis problemática entre las lógicas de control interno características de los Estados policiales y las tecnologías de guerra desarrolladas para conflictos externos. Su implementación en contextos civiles erosiona progresivamente las fronteras entre seguridad pública y control militar, creando las condiciones institucionales para formas inéditas de autoritarismo tecnológicamente potenciado.

DRONES Y LA MILITARIZACIÓN DEL ESPACIO CIVIL

El uso de drones en contextos de seguridad ha contribuido a una creciente militarización de la vida civil, donde tecnologías originalmente concebidas para fines bélicos son trasladadas —sin mayor escrutinio público ni regulación específica— a funciones de control poblacional, vigilancia interna y represión. Siguiendo una lógica de seguridad intensificada, se ha logrado integrar este tipo de tecnologías en la gestión cotidiana de espacios aéreos urbanos y rurales, desdibujando las fronteras entre lo civil y lo militar, consiguiendo una naturalización de la excepcionalidad.

En este marco, el Plan de Seguridad para el Desarrollo 2023-2028[39], identifica el espacio aéreo como un ámbito de creciente vulnerabilidad e interés estratégico, al tratarse de uno de los llamados "espacios comunes globales" donde se vuelve más complejo el ejercicio soberano de control estatal. Entre las amenazas señaladas se encuentran el tráfico de drogas, el contrabando y otras actividades ilícitas aéreas, cuya proliferación pone en riesgo tanto la seguridad como el desarrollo. Sin embargo, las propias autoridades reconocen que las carencias estructurales en radares, equipos y presupuesto debilitan la capacidad estatal para ejercer un control efectivo, lo que ha abierto paso a la incorporación de nuevas herramientas como los drones.

En el caso paraguayo, el actuar de la Fuerza de Tarea Conjunta (FTC) en zonas del norte del país ilustra con claridad este fenómeno. Reportes e investigaciones periodísticas han documentado el despliegue de drones en operativos contra el Ejército del Pueblo Paraguayo (EPP)[40], muchas veces en escenarios de escasa transparencia, sin supervisión judicial efectiva y con débiles mecanismos de rendición de cuentas.

Asimismo, en estas zonas de supuesta actividad del EPP, existen múltiples denuncias de que esta militarización responde más a intereses privados que a la protección social de las comunidades[41], como refleja el comentario de Sindulfo Agüero, residente de Alfonso Kue, Horqueta, en referencia a la presencia sostenida de estas fuerzas represivas en sus comunidades y al abuso de poder: "Opyta okyjyjepa lo mitã. Upevaera ojapo hikuei la ojapova. Omogyýje hagua (La gente quedó con miedo. Para eso hicieron lo que hicieron. Para hacerle tener miedo a la gente)" (Benegas Vidallet, 2024).

39 Para acceder al documento completo, ver: Consejo de Defensa Nacional (2023). Plan Seguridad para el Desarrollo 2023-2028. https://mdn.gov.py/wp-content/uploads/2024/11/Plan-Seguridad-para-el-Desarrollo-2023-2028.pdf

40 El Ejército del Pueblo Paraguayo (EPP) es un grupo armado insurgente de orientación marxista-leninista que opera en el norte de Paraguay desde la década del 2000. Fue señalado por el Estado paraguayo como responsable de secuestros, atentados y actividades vinculadas al narcotráfico, y declarado organización terrorista por el gobierno paraguayo (Wikipedia, s/f).

41 Entre los antecedentes más relevantes de la Fuerza de Tarea Conjunta (FTC) se encuentra el caso del fallecimiento de María del Carmen y Liliana Villalba, niñas de 11 años, ocurrido el 2 de septiembre de 2020 durante un operativo contra el Ejército del Pueblo Paraguayo (EPP). El Comité de los Derechos del Niño de las Naciones Unidas concluyó, tras una investigación, que el Estado paraguayo incurrió en graves violaciones de Derechos Humanos en relación con estos hechos (Paraguay, responsable de graves violaciones de Derechos Humanos por la muerte de dos niñas, según un comité de la ONU, 2025). Ver resolución en: https://www.ohchr.org/es/press-releases/2025/01/paraguay-responsible-grave-rights-violations-over-deaths-two-young-girls-un

Bajo ese contexto de opacidad, el Estado paraguayo busca "modernizar" a sus fuerzas represivas, ejemplo de esto es la reciente capacitación de unos 40 militares del Ejército Paraguayo en el manejo de drones[42] con capacidad de búsqueda, rescate y uso ofensivo para control fronterizo (La Nación, 2025). Además, según reportado por un medio internacional, la Armada paraguaya adquirió drones EVO MAX 4N (tecnología china), capaces de vigilancia multiespectral y audio, y continuará su incorporación con apoyo de empresas como Datasystems para tareas de monitoreo infranqueable en zonas fronterizas, supervisadas por fuerzas estatales (Saba Manzo, 2024). Estas intervenciones consolidan un modelo de seguridad híbrido, donde entidades militares y empresas privadas expanden sus capacidades de vigilancia sobre la población civil.

Estos reportes coinciden con la información disponible en el portal de la Dirección Nacional de Contrataciones Públicas (DNCP) en relación con la Licitación Nº 452492, titulada "Adquisición de drones para la Armada Paraguaya"[43]. Según consta en dicha publicación, se invirtieron ₲ 557.632.107 mediante el Contrato Nº 40/2024, adjudicado a la empresa DataSystems, para la provisión de drones de alta gama. Entre las especificaciones técnicas requeridas se incluyen: cámara gran angular de 50 megapíxeles, cámara térmica con resolución de 640×512, cámara nocturna con sensibilidad ISO de hasta 300.000, alcance de transmisión de hasta 20 km, sistema anti-colisión por radar, compatibilidad con múltiples sistemas GNSS (GPS, GLONASS, BeiDou y Galileo), y autonomía de vuelo mínima de 42 minutos. Estas características evidencian la adquisición de equipos con alto poder de captación, geolocalización y operación en distintos contextos ambientales, incluyendo vigilancia nocturna o en condiciones extremas.

A nivel internacional, el fenómeno no es aislado. Estados Unidos ha institucionalizado el uso de drones tanto en operaciones militares extraterritoriales —incluyendo ejecuciones selectivas— como en la vigilancia fronteriza doméstica (Amnesty International, 2013; Alston, 2010; García et al., 2024). Israel, por su parte, ha desarrollado sistemas avanzados de control aéreo, como la Cúpula de Hierro, y utiliza regularmente drones para operaciones de vigilancia y represión en los territorios ocupados, lo que ha generado denuncias sobre el uso excesivo de la fuerza y vigilancia sistemática de civiles (Dworkin, 2013; Melzer, 2013).

En América Latina, Colombia ofrece un antecedente relevante con el uso de drones en operaciones de contrainsurgencia contra las FARC (DeYoung, 2011). México ha documentado el empleo de estas tecnologías en tareas de patrullaje fronterizo, control migratorio y apoyo a operativos militares en zonas urbanas (García et al., 2024). Honduras, por su parte, ha registrado denuncias sobre el uso de drones para intimidar a más de 175 familias de comunidades campesinas y defensoras del territorio por parte de empresas privadas del sector agroindustrial (Forner, 2024).

42 Hasta el momento de redacción de este trabajo, las fuerzas militares paraguayas no respondieron un pedido de acceso a la información pública que solicitaba datos e información sobre sus reglamentaciones en torno a los operativos con drones y otras cuestiones relacionadas. Ver solicitud en: https://informacionpublica.paraguay.gov.py/#!/ciudadano/solicitud/93452

43 Véase: DNCP. (2024, octubre 09). Convocatoria a Licitación Nº 452492, titulada "Adquisición de drones para la Armada Paraguaya" https://www.contrataciones.gov.py/licitaciones/adjudicacion/1ef81a27-0ad0-69dc-9e86-f7c6d914c1a2/resumen-adjudicacion.html

Por otro lado, la preocupación no se limita al uso estatal. La militarización del espacio civil implica una profunda transformación del territorio, dado que no solo se trata de intervención con fuerzas armadas, sino de un ecosistema sustentado en vigilancia constante, anonimato tecnológico y agentes mixtos (estatal y privados). Además del sector privado, cada vez existen más indicios del uso de drones por parte de actores armados como grupos insurgentes o redes vinculadas al narcotráfico, que los emplean como mecanismos de vigilancia, intimidación o ataque. De hecho, según Frantzman (2021), numerosos grupos terroristas y actores no estatales, como ISIS, Hezbolá, los hutíes y Boko Haram, han desarrollado o utilizado UAVs, a menudo armando drones comerciales.

En julio de 2025, el medio internacional Reuters reportó que militantes islamistas paquistaníes utilizaron drones armados para atacar posiciones de las fuerzas de seguridad, revelando los riesgos que representa esta tecnología en manos de actores sin responsabilidad pública (Ali & Shahzad, 2025). Asimismo, se ha documentado el uso de "narcodrones" en países como México (Bayoud, 2025), lo que ha generado respuestas represivas tanto por parte de las autoridades mexicanas como estadounidenses (Muñoz Lima, 2025; El Financiero, 2025). Estas dinámicas de confrontación terminan afectando principalmente a la población civil, que queda expuesta a formas constantes de vigilancia y control por parte de ambos actores.

Considerando la experiencia internacional, la eventual incorporación de drones en operaciones criminales o paramilitares tanto en nuestro país como región, también se presenta como un escenario preocupante, pues daría lugar a formas paralelas de control territorial sin garantías institucionales. Este proceso de militarización aérea —a veces explícito, otras veces sutil e informal— desafía los los principios de legalidad y proporcionalidad en el uso de la fuerza, y plantea la urgencia de establecer marcos normativos que limiten el uso de estas tecnologías en contextos que afecten Derechos Humanos y formas de vida democrática.

PERSPECTIVA INTERSECCIONAL Y VIGILANCIA SELECTIVA

GÉNERO, RACIALIZACIÓN Y TECNOLOGÍAS DE CONTROL

Como se observa en los capítulos anteriores, el despliegue de tecnologías de vigilancia, incluidos los drones, dista de ser una práctica neutral. Por el contrario, tiende a reproducir —y, en muchos casos, a intensificar— estructuras históricas de desigualdad, dominación y exclusión (Silva & Varón, 2021). Al respecto, Ruha Benjamin (2019), inspirada en la obra de Michel Foucault, advierte que, la exposición tecnológica no afecta por igual a todas las personas: ciertos cuerpos —racializados, feminizados, empobrecidos o disidentes— son objeto de una vigilancia desproporcionada. Esta vigilancia selectiva no solo se configura a partir de los fines declarados de la tecnología, sino también de los sujetos a quienes se dirige, sus condiciones sociales y su pertenencia a colectivos históricamente vulnerabilizados.

Aplicado al caso de los drones, el fenómeno se traduce en un uso intensificado en contextos como el control migratorio, el patrullaje de barrios populares, la gestión de protestas o la represión de demandas sociales (Benjamin, 2019; García et al., 2024; D'Ignazio & Klein, 2020; Zuazo, 2018). En América Latina, se han documentado usos de drones en protestas sociales en Chile (Clarín, 2019) y Argentina (R3D, 2023), así como en operativos de vigilancia sobre comunidades indígenas en aislamiento voluntario en Brasil (Iglesias, 2022), poblaciones campesinas en Panamá (Front Line Defenders, 2025) y durante eventos LGBTIQ+, donde los cuerpos disidentes son especialmente susceptibles de ser criminalizados o registrados sin consentimiento.

A nivel internacional, también se han reportado casos como el de Irán, donde drones son utilizados para identificar y perseguir a mujeres que no cumplen con el código de vestimenta impuesto por el régimen (Foulkes & McArthur, 2025). Como ya se ha advertido más arriba, este tipo de vigilancia no solo vulnera derechos fundamentales como la privacidad o la libertad de expresión, sino que produce un efecto inhibidor sobre la participación política y social de grupos históricamente marginados.

En contextos como el paraguayo, marcados por una alta diversidad étnica, lingüística y cultural[44], y considerando casos reportados a nivel internacional, se puede presumir que la incorporación de tecnologías de vigilancia aérea podría generar tasas de errores significativamente más altas en personas con tonos de piel oscuros, rasgos indígenas o no eurocéntricos, así como en mujeres, personas mayores y personas trans, intensificando patrones de exclusión y discrminacion.

44 Según el Censo Indígena Nacional (Instituto Nacional Indígena, 2022), aproximadamente el 2 % de la población se identifica como indígena, perteneciente a 19 pueblos originarios organizados en cinco familias lingüísticas. A esto se suma una creciente visibilidad de la comunidad afrodescendiente y una mayoría poblacional que se identifica como mestiza. Además, el 77 % de la población paraguaya declara ser bilingüe en guaraní y español, lo cual evidencia la centralidad de la identidad cultural indígena en la vida cotidiana del país (DGEEC, 2022). Esta pluralidad étnica, cultural y lingüística requiere enfoques diferenciados para prevenir sesgos algorítmicos y garantizar el respeto a los Derechos Humanos.

Ante esta circunstancia, es necesario recordar que la discriminación tecnológica no opera de forma aislada. Por ello, estos debates deben ser abordados desde una perspectiva interseccional[45] —considerando la interacción entre género, raza, clase, orientación sexual u otras categorías—, ya que los efectos del uso de drones con capacidades de vigilancia pueden volverse aún más lesivos cuando se superponen múltiples formas de vulnerabilidad.

Esto se evidencia en el caso del reconocimiento facial, tecnología que, al ser integrada en drones, puede amplificar errores algorítmicos preexistentes. La investigación de Buolamwini y Gebru (2019) demostró que los sistemas comerciales de reconocimiento facial presentan tasas de error interseccionales significativamente más altas, afectando con especial severidad a mujeres negras, quienes son hasta 44 veces más propensas a ser mal clasificadas que los hombres blancos.

Estas disparidades no son fallos accidentales, sino el reflejo de decisiones técnicas y políticas incorporadas en el diseño y entrenamiento de algoritmos. Como advierten D'Ignazio y Klein (2020), "una mejor detección de rostros de color" no implica necesariamente una mejora, si su uso se orienta a expandir las prácticas represivas. En esta línea, Safiya Noble (2018) conceptualiza la "reducción tecnológica" (*technological redlining*) como el proceso mediante el cual las infraestructuras digitales reproducen las lógicas históricas de exclusión, desplazando al plano algorítmico prácticas similares al perfilamiento racial. Así, los drones, como dispositivos potenciados por IA, lejos de ser ajenos a estas dinámicas, pueden convertirse en nodos activos de discriminación estructural.

Tampoco se puede ignorar la dimensión de género inscrita en estas tecnologías. Según el Grupo GIFT (2021), los artefactos digitales no son neutros, sino que reflejan —y a menudo refuerzan— imaginarios sociales sexuados. Las tecnologías "colaboran activamente en el establecimiento de la división y la diferencia sexual" (p. 12), y están atravesadas por los valores, intereses y sesgos[46] de quienes las diseñan (p. 8). Esta inscripción sociotécnica de la desigualdad se manifiesta, por ejemplo, en el hecho de que múltiples configuraciones algorítmicas pueden ofrecer rendimientos técnicos similares, pero con impactos dispares sobre distintos grupos demográficos.

Tal como señalan Black, Koepke, Kim, Barocas y Hsu (2024), las consecuencias discriminatorias de un sistema no son inevitables, sino producto de elecciones de diseño que no priorizan la equidad. Siendo así, en lugar de corregir desigualdades, el desarrollo tecnológico puede terminar consolidándolas. Por ejemplo, el uso de drones equipados con sensores visuales, térmicos o biométricos en operativos de seguridad, verificación o patrullaje automatizado representa un riesgo de vigilancia selectiva sobre cuerpos racializados y feminizados (Silva & Varón, 2021).

A fin de contrastar el análisis conceptual con la práctica institucional, en el marco de esta investigación se solicitó información pública a diversas entidades del Estado paraguayo para conocer si existen protocolos, diagnósticos o antecedentes sobre el uso de drones con enfoque de derechos humanos, género o impactos diferenciados en poblaciones vulnerables. Los hallazgos revelan

45 El concepto de interseccionalidad fue desarrollado por la jurista afroamericana Kimberlé Crenshaw (1989) para explicar cómo múltiples formas de discriminación —como el racismo, el sexismo y la desigualdad de clase— se entrelazan y generan experiencias específicas de opresión, particularmente sobre las mujeres negras. En el ámbito de las tecnologías, este enfoque permite analizar cómo los impactos no se distribuyen de forma homogénea, sino que afectan con mayor intensidad a quienes se encuentran en la intersección de múltiples vulnerabilidades.

46 En este trabajo, el término sesgo alude a errores sistemáticos en tecnologías como drones equipados con algoritmos de vigilancia o toma de decisiones automatizadas. Estos sesgos pueden tener raíces estadísticas, sociales o institucionales (Bellamy, 2019) y, en el caso de tecnologías aplicadas a la seguridad, derivar en patrones de vigilancia desigual o perfilamiento erróneo de ciertas poblaciones. Aunque muchas veces son involuntarios, suelen originarse en datos no representativos o en variables mal definidas, lo que contribuye a amplificar desigualdades al impactar de forma desproporcionada a grupos vulnerables (Barocas & Selbst, 2016).

una preocupante ausencia de marcos normativos y mecanismos de evaluación específicos. El MITIC (2025) reconoció que no cuenta con protocolos ni lineamientos con enfoque de Derechos Humanos o de género en relación con el uso de drones.

Del mismo modo, el MAG (2025) respondió que no está desarrollando actualmente esta tecnología en comunidades rurales, campesinas o indígenas, ni ha realizado estudios sobre sus impactos sociales o culturales. La Defensoría del Pueblo (2025), por su parte, indicó que no registra antecedentes de denuncias o intervenciones relacionadas con posibles afectaciones de derechos por el uso de drones. Finalmente, el Ministerio Público (2025) informó que no ha realizado operaciones con drones para el monitoreo de protestas, ni existen registros oficiales de solicitudes de autorización para ello ante la Dirección Nacional de Aeronáutica Civil (DINAC).

Las referidas respuestas institucionales —caracterizadas más por la omisión que por la previsión— no solo reflejan una ausencia de marcos reguladores, sino también una falta de sensibilidad estructural ante los efectos diferenciados de estas tecnologías. La ausencia de registros, diagnósticos o lineamientos específicos en el Estado paraguayo no equivale a una ausencia de riesgos; por el contrario, plantea un escenario donde la opacidad institucional puede normalizar formas de vigilancia discriminatoria, silenciosa y persistente. Esta omisión sistemática no es neutra, tiene efectos materiales y simbólicos que se traducen en impactos desiguales sobre distintos grupos sociales.

En este contexto, los efectos diferenciados del uso de drones —y de las tecnologías de vigilancia en general— se cristalizan en formas de invisibilización, hipervisibilización, exclusión o persecución (Benjamin, 2019). Estos efectos tienen consecuencias concretas en ámbitos como el acceso a derechos, la participación política y la circulación en el espacio público. Tomando en cuenta ello, en ausencia de un marco legal robusto que regule el tratamiento de datos biométricos o la supervisión de tecnologías aplicadas a la seguridad pública, existe una alta probabilidad de que herramientas como los drones afecten desproporcionadamente a grupos vulnerables o históricamente excluidos. Esta afectación puede manifestarse tanto a través de errores de identificación como de decisiones automatizadas que reproducen estigmas sociales.

Esto se agrava cuando el diseño tecnológico no contempla la inclusión de comunidades diversas en sus procesos de desarrollo. En contextos como América Latina—incluido Paraguay, donde el desarrollo de tecnologías suele depender de modelos importados desde centros globales de poder, existe el riesgo de reproducir arquitecturas tecnológicas construidas sobre datos, valores y lógicas externas (D'Ignazio & Klein, 2020; Criado Perez; 2020). Como advierte el Grupo GIFT (2021), la tecnología codifica visiones del mundo, decisiones de diseño y exclusiones estructurales. En sus palabras, la acción que sigue, para tratar de influir en el desarrollo de tecnologías con perspectiva de género, es:

> incluir recursos humanos interseccionales en los equipos que desarrollan tecnología. Necesitamos equipos de trabajo diversos que sean lo más parecido posible a la sociedad para la cual se crean las tecnologías digitales. Es necesario incluir en posiciones tanto técnicas como de toma de decisiones personas cuyas intersecciones no están habitualmente representadas en el desarrollo tecnológico, tales como mujeres que se identifican con pueblos originarios, hombres trans, migrantes o personas con discapacidad, entre otras muchas intersecciones. (Grupo GIFT, 2021, p. 14).

Ignorar estas recomendaciones conlleva el riesgo de consolidar mecanismos de exclusión más sofisticados, amparados en discursos de innovación, eficiencia o modernización. Argumentos que apelan a la supuesta falta de personal interseccional capacitado resultan insostenibles si, como también señala el Grupo GIFT (2021), "el número de recursos humanos altamente capacitados se amplía cuando se considera la multidisciplinariedad necesaria para desarrollar tecnología" (p. 14).

Observado el contexto expuesto, no se debería promover la implementación de tecnologías intrusivas como los drones sobre comunidades vulnerables sin mecanismos de consulta previa, participación informada ni evaluación de impacto en Derechos Humanos. El debate sobre su adopción debe ser abordado desde una crítica interseccional y feminista, que no se limite a exigir transparencia técnica, sino que también interpele la responsabilidad política de quienes diseñan, promueven o implementan estas herramientas.

ASIMETRÍAS EN EL ACCESO Y USO DE TECNOLOGÍAS

Como se desprende del análisis de las autoras y autores revisados —entre ellos Benjamin (2019), Criado Perez (2020), Noble (2018), Eubanks (2018), Lara Castro (2020) y Zuazo (2018)—, las profundas asimetrías en el acceso, diseño y aplicación de tecnologías como los drones no pueden abordarse únicamente desde soluciones técnicas. Por el contrario, se requieren intervenciones estructurales que combinen regulación legal, rediseño tecnológico consciente y movilización social. Desde la necesidad de evaluar la gobernanza de tecnologías con potencial de afectar Derechos Humanos, hasta la implementación de auditorías independientes y marcos normativos de alcance regional, se necesita repensar la tecnología como un espacio de disputa política y no como un entorno neutral o apolítico.

En este sentido, contar con un marco de gobernanza que priorice la equidad por sobre la eficiencia, así como incorporar diversidad en los procesos de diseño y fortalecer la participación comunitaria, constituyen pasos clave para evitar que estas tecnologías profundicen desigualdades históricas. A esto se suma la necesidad de democratizar el conocimiento sobre la tecnología, como estrategia clave para asegurar que sus avances se alineen con valores democráticos y de justicia social (Benjamin, 2019, p. 87), en lugar de reforzar regímenes de control opaco o dinámicas de exclusión estructural.

Como advierte Ruha Benjamin (2019), las tecnologías digitales suelen aterrizar sobre estructuras sociales desiguales que, lejos de neutralizarse por la innovación, tienden a reproducirse o incluso amplificarse. El acceso desigual a dispositivos, conectividad o formación no es una mera cuestión técnica o de infraestructura, sino un reflejo de relaciones de poder ancladas en desigualdades históricas de género, clase y raza (Noble, 2018, p. 18). Por ello, hablar de brecha digital en términos meramente cuantitativos, es decir, centrados en el acceso a computadoras, software y conectividad a Internet, puede resultar insuficiente o incluso engañoso si no se abordan sus raíces estructurales (p. 19-23).

En Paraguay, si bien el acceso a Internet ha aumentado considerablemente en los últimos años, aún persisten fuertes disparidades. Según el Instituto Nacional de Estadísticas (INE), en 2024 el 86,2% de la población urbana utiliza Internet, frente al 73,7 % en zonas rurales[47]. Además, el principal uso de Internet sigue siendo la mensajería instantánea y redes sociales (INE, 2024), lo que plantea interrogantes sobre la calidad y profundidad del acceso y su potencial emancipador. Como señala Eubanks (2018), las poblaciones vulnerables como personas de color, migrantes, y pobres, no solo acceden menos, sino que son las primeras en ser convertidas en objetos de monitoreo y prueba para tecnologías automatizadas, como drones o algoritmos predictivos.

Esto se agrava cuando el Estado, en lugar de facilitar el acceso igualitario a tecnologías, las despliega de forma selectiva para vigilancia o control sin garantizar al mismo tiempo espacios de participación, formación o apropiación social. Tal es el caso de Paraguay, donde, pese a contar con un Plan Nacional de Tecnologías 2022–2030[48] que menciona la inclusión digital, no existen programas específicos de formación o fomento del uso de drones en comunidades campesinas, indígenas o cooperativas rurales. Según la respuesta oficial del Ministerio de Agricultura y Ganadería (2025), el uso de drones no ha sido acompañado de evaluaciones de impacto ni líneas de acción orientadas a productores rurales.

No obstante, experiencias regionales demuestran que un uso democratizado de esta tecnología es posible. Tanto en Brasil como en Perú (Collyns, 2018), comunidades indígenas amazónicas utilizan drones para denunciar derrames petroleros y vigilar sus territorios; en Bolivia, una mujer aymara lidera procesos de tecnificación del agro con estos dispositivos (NTN24, 2024). Estos ejemplos no deben ser vistos como excepciones o curiosidades, sino como modelos de redistribución en el acceso a tecnología y las oportunidades que ella ofrece.

En definitiva, las asimetrías en el acceso, diseño y uso de los drones no se resolverán simplemente con expandir la cobertura digital. Requieren un cambio de paradigma que entienda la tecnología como un campo de disputa política y no como una solución preformateada. Democratizar su desarrollo y uso, incorporar pluralidad en los equipos técnicos y fomentar la apropiación comunitaria son pasos esenciales para que estas herramientas no refuercen jerarquías, sino que actúen como medios de redistribución de poder y garantía de derechos.

47 Para conocer a detalle los datos reportados, véase: Instituto Nacional de Estadísticas (INE). (2025, junio). *Tecnología de la Información y Comunicación en el Paraguay. EPHC 2024*. https://www.ine.gov.py/publication-single.php?codec=280

48 Para acceder al material, véase: MITIC. (2022). Plan Nacional de TIC 2022-2030. https://mitic.gov.py/plan-nacional-de-tic-2022-2030/

GOBERNANZA GLOBAL, GEOPOLÍTICA Y REGULACIÓN

El avance y la proliferación de drones no solo representan una innovación tecnológica, sino que también plantean, como señala Frantzman (2021), una reconfiguración sustantiva del equilibrio de poder global, acelerando la carrera por su dominio. Lejos de limitarse a sus aplicaciones civiles —como los mencionados en secciones más arriba— los drones se han consolidado como herramientas estratégicas de influencia geopolítica, defensa, seguridad y vigilancia.

Esta circunstancia también ha influido en los marcos regulatorios emergentes, determinando quién regula, con qué fines y para quiénes. Ejemplo de ello es la Executive Order firmada por Donald Trump en 2025, que establece la necesidad de garantizar el "dominio estadounidense de los drones", reforzando las cadenas de producción nacional y reduciendo la dependencia de insumos extranjeros (Trump, 2025). Esta medida forma parte de una lógica de reshoring[49] tecnológico con fuerte contenido estratégico, en respuesta a la creciente influencia de China en el mercado global de RPAS (Remotely Piloted Aircraft Systems).

Este contexto ha dado lugar a un nuevo tipo de "militarización encubierta" de tecnologías nominalmente civiles, habilitando su integración a funciones policiales, de control migratorio o inteligencia interior sin marcos jurídicos específicos. Lo anterior plantea interrogantes sustanciales sobre el principio de legalidad y el debido proceso, especialmente en contextos democráticos. En ausencia de estándares vinculantes, esta instrumentalización incrementa el riesgo de fragmentación normativa a nivel global, en un entorno internacional ya tensionado por rivalidades estratégicas, erosión del multilateralismo, y respuestas unilaterales frente a amenazas reales o percibidas (Cocchini & Bermejo García, 2020; Boyle, 2020). A esto se suman dinámicas complejas como el conflicto entre Israel y Gaza, el despliegue de drones en Ucrania, o la creciente militarización de fronteras en América y Europa (Korać, 2023).

Desde América Latina, este panorama plantea un dilema sustancial debido a que la importación de tecnologías de vigilancia estratégicas sin una arquitectura regulatoria sólida impone marcos técnicos y lógicas operativas diseñadas por jurisdicciones exportadoras (Access Now, 2021). Esta asimetría, como advierte el informe de Access Now, limita la capacidad de los países receptores para desarrollar regulaciones acordes a su realidad constitucional y sociopolítica. Esta problemática, como se verá en la subsección siguiente, resulta especialmente relevante en el caso de Paraguay.

De hecho, siguiendo el análisis del referido informe, países con institucionalidad débil y dependencia tecnológica —como Paraguay— esta tensión se manifiesta en múltiples niveles. La importación de infraestructura de vigilancia aérea sin control democrático adecuado implica no solo la adquisición de *hardware*, sino también la transferencia implícita de modelos de uso, protocolos operativos y concepciones sobre el equilibrio entre seguridad y derechos fundamentales.

49 El *reshoring* es la práctica de traer de vuelta al país actividades productivas que antes se realizaban en el extranjero. En EE. UU., el Estado ha impulsado esta estrategia especialmente en sectores tecnológicos clave.

Así, sin un diseño regulatorio contextualizado, se corre el riesgo de consolidar prácticas de vigilancia intensiva como si fueran normas tácitas, sin haber pasado por un debate público, control legislativo o revisión judicial. De hecho, autores Frandzman (2021) y Boyle (2020), como han advertido que, el uso generalizado de drones comerciales, como los de DJI —adquiridos por entes estatales en nuestro país según se reportó más arriba—, ha generado preocupaciones sobre la posible vigilancia por parte de China, ya que se han reportado incidentes de *hackeos* que comprometieron las transmisiones de drones como el MQ-1 Predator y los planes de MQ-9 Reaper.

A escala internacional, si bien no existe un régimen normativo explícito y vinculante que regule de manera específica el uso civil y militar de drones, autores como Cocchini y Bermejo García (2020) sostienen que "las normas que se aplican a las operaciones armadas de los drones son las mismas que se aplican a las otras armas" (p. 104). En este sentido, instrumentos como el Pacto Internacional de Derechos Civiles y Políticos (PIDCP) y la Convención Americana sobre Derechos Humanos (CADH) —que garantizan derechos como la privacidad, la vida y el debido proceso—, resultan aplicables, especialmente cuando el despliegue de drones amenaza a derechos fundamentales. No obstante, la implementación efectiva de estos estándares enfrenta tensiones persistentes en escenarios geopolíticos complejos, lo que continúa representando un desafío regulatorio relevante.

Igualmente, otros diversos instrumentos internacionales ofrecen marcos normativos importantes. En contextos de conflicto armado, los Convenios de Ginebra de 1949[50] imponen principios como la distinción, la proporcionalidad y la necesidad militar. Los Principios de Johannesburgo sobre seguridad nacional y libertad de expresión (1995)[51] agregan directrices interpretativas no vinculantes pero muy importantes, como que toda medida restrictiva debe ser legal, proporcional, y bajo control judicial efectivo.

Por su parte, la Relatoría Especial de la ONU sobre privacidad ha advertido reiteradamente sobre los riesgos del uso masivo de drones sin supervisión ni mecanismos de rendición de cuentas. La CIDH ha desarrollado estándares sobre vigilancia estatal y Derechos Humanos, mientras que UNESCO y la Organización para la Cooperación y el Desarrollo Económico (OCDE)[52] han propuesto principios éticos sobre tecnologías emergentes, promoviendo marcos centrados en derechos y principios como de transparencia y equidad.

50 Los Convenios de Ginebra de 1949 y sus Protocolos adicionales constituyen el núcleo del Derecho Internacional Humanitario. Son cuatro tratados internacionales que establecen normas para limitar los efectos de los conflictos armados y proteger a quienes no participan directamente en las hostilidades —como la población civil, el personal médico y humanitario— así como a quienes han dejado de participar, como los soldados heridos, enfermos, náufragos o prisioneros de guerra. Para conocer el texto completo y sus comentarios oficiales, véase: Comité Internacional de la Cruz Roja (CICR). *Los Convenios de Ginebra y sus Comentarios – Enlaces útiles*. Disponible en: https://www.icrc.org/es/derecho-y-politicas/los-convenios-de-ginebra-y-sus-comentarios

51 ARTICLE 19. (1996). *Los Principios de Johannesburgo sobre la seguridad nacional, la libertad de expresión y el acceso a la información.* ARTÍCULO 19. https://www.corteidh.or.cr/tablas/a22440.pdf

52 *La Recomendación de la UNESCO sobre la Ética de la Inteligencia Artificial* (2021) fue adoptada por consenso por los 193 Estados miembros, incluido Paraguay. Este instrumento establece principios y directrices para el diseño y uso responsable de tecnologías emergentes, incluyendo salvaguardas específicas para la protección de los Derechos Humanos, la inclusión y la justicia social. Por su parte, la OCDE ha desarrollado una serie de principios sobre inteligencia artificial (Principles on AI, 2019) que promueven el respeto a los Derechos Humanos, la transparencia, la rendición de cuentas y el desarrollo centrado en el ser humano. Ambos marcos, si bien no son vinculantes, constituyen referencias internacionales clave para la gobernanza ética y democrática de tecnologías como los drones y los sistemas automatizados.

Finalmente, el Reglamento Delegado (UE) 2023/659 de la Comisión Europea[53], centrada en los riesgos de los drones civiles, constituye también un ejemplo de respuesta normativa regional. Plantea medidas preventivas en trazabilidad, control de exportaciones y cooperación transfronteriza. No obstante, también revela las dificultades de una gobernanza coordinada en contextos marcados por agendas securitarias. Por su parte, dentro del MERCOSUR, no se ha identificado ninguna normativa similar.

En definitiva, los casos documentados —especialmente en escenarios de conflicto armado— evidencian que la existencia de marcos normativos aplicables no garantiza por sí sola su cumplimiento efectivo. Su implementación concreta depende de factores como la voluntad política, la capacidad institucional y la adecuación normativa al contexto local. No obstante, esta dificultad no debe interpretarse como una excusa para ignorar la vigencia de estándares jurídicos aplicables al uso intrusivo de tecnologías de vigilancia. En este sentido, Paraguay —y la región— enfrentan el desafío ineludible de traducir estos principios en marcos regulatorios robustos y efectivos.

EL CASO PARAGUAYO: FRAGMENTACIÓN NORMATIVA Y SOBERANÍA TECNOLÓGICA

En Paraguay, la regulación sobre el uso de drones se encuentra en una etapa incipiente y fragmentaria, con un marco jurídico que visibiliza principalmente aspectos técnico-operativos. La normativa vigente se estructura en torno a tres instrumentos principales[54]:

- Ley № 1860/2001 – Código Aeronáutico Paraguayo, que regula de forma general la navegación aérea civil;
- Resolución DINAC № 2170/2017, que aprueba el Reglamento R1103 sobre Aeronaves Pilotadas a Distancia (RPAC) y Sistemas de Aeronaves Pilotadas a Distancia (RPAS), estableciendo requisitos de registro, clasificación, autorizaciones, alturas de vuelo, condiciones climáticas y seguros;
- Convenio de Chicago de 1944[55], cuyo artículo 8 establece que toda aeronave sin piloto requiere autorización especial para sobrevolar territorio nacional.

Estos tres instrumentos configuran, en cuanto a su ámbito de aplicación concreta, el esqueleto normativo actual, aunque con limitaciones evidentes en materia de derechos y garantías. El marco vigente omite —como lo evidencian varios de los casos analizados en este trabajo— dimensiones críticas asociadas al uso estatal de drones con fines de vigilancia, control territorial, seguridad interna o actividades de inteligencia. En particular, se requieren previsiones expresas sobre privacidad, protección de datos personales, rendición de cuentas, supervisión judicial o evaluación de impacto en derechos fundamentales, para evitar el uso de estas tecnologías —sobre todo desde el sector estatal— en un terreno difuso, desregulado y potencialmente lesivo.

53 Véase: Reglamento Delegado (UE) 2023/659 de la Comisión de 2 de diciembre de 2022, que modifica el Reglamento (UE) n.º 452/2014 en lo relativo a los requisitos técnicos y procedimientos administrativos aplicables a operadores extranjeros en operaciones aéreas. https://noticias.juridicas.com/base_datos/Admin/749716-regl-2023-659-ue-de-2-dic-2022-modificacion-del-regl-ue-n-o-452-2014.html

54 Para consultar los documentos normativos pertinentes, puede acceder al sitio oficial de la DINAC en la sección “Leyes, Decretos, Resoluciones y Circulares”: https://www.dinac.gov.py/v3/index.php/documentos1/leyes-decretos-resoluciones-circulares

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

A su vez, esta laguna normativa debe analizarse en el contexto de una institucionalidad débil, centralizada y dividida, donde el marco de gobernanza tiende a ser reactivo, disperso y carente de participación multisectorial efectiva. Esta situación se agrava ante intentos recientes de redefinir la gobernanza del entorno digital desde una lógica securitaria y de defensa nacional[56].

De hecho, el debate actual sobre ciberseguridad en Paraguay permite visualizar con nitidez este conflicto. La Estrategia Nacional de Ciberseguridad 2025–2028[57], liderada por el MITIC, establece como objetivo central "proteger la infraestructura crítica del país y fortalecer la ciberseguridad nacional". Aunque propone una gobernanza interinstitucional, incorpora como actores centrales al Ministerio de Defensa Nacional, las Fuerzas Armadas y la Secretaría Nacional de Inteligencia. Esta "integración operativa" se presenta como necesaria ante amenazas híbridas, pero desplaza la rectoría desde un enfoque civil hacia uno militarizado.

Al respecto, TEDIC (2024) ha advertido que esta orientación contradice las buenas prácticas internacionales[58], que recomiendan que los marcos de ciberseguridad —y por extensión, la regulación de tecnologías emergentes como los drones— estén bajo la conducción de organismos civiles, con mecanismos de transparencia, participación multisectorial y respeto por el Estado de derecho. La propuesta de atribuir al Ministerio de Defensa Nacional la rectoría del sistema nacional de ciberseguridad —actualmente bajo debate legislativo— ilustra esta tendencia hacia la securitización del ecosistema digital, con consecuencias directas sobre la legitimidad democrática y la protección de derechos en entornos tecnológicos.

En paralelo, el Plan Estratégico de Seguridad para el Desarrollo 2023–2028[59], aprobado por el Consejo de Seguridad Nacional, promueve un enfoque de "urgencia sin precedentes" para combatir amenazas híbridas. Esta retórica —que justifica "actuaciones e inversiones extraordinarias e impostergables"— facilita la normalización del uso de tecnologías intrusivas como los drones en contextos sin control judicial ni marco regulatorio específico.

En este entorno, la adquisición o despliegue de drones, tanto por parte de actores públicos como privados, se da en escenarios de baja transparencia, ausencia de control parlamentario60 y débil fiscalización judicial. La falta de una legislación paraguaya específica que regule el uso de drones con fines de vigilancia —especialmente en contextos internos de seguridad— contrasta con los estándares internacionales previamente analizados, que insisten en que toda tecnología de vigilancia debe estar regulada por ley, proporcional al fin perseguido y sujeta a control judicial efectivo.

56 Ver: Sequera Buzarquis, M. (2025, 24 de junio). *La Evolución de la Ciberseguridad en Paraguay: MITIC como Pilar Estratégico*. TEDIC. https://www.tedic.org/ciberseguridad-en-paraguay-entre-la-urgencia-y-la-improvisacion-legislativa/

57 Documento completo disponible en la plataforma de archivos del MITIC. https://drive.mitic.gov.py/s/ZS7YXfEJrxfgdia?dir=/&editing=false&openfile=true

58 Ver: Sequera Buzarquis, M. (2025, 23 de junio). *Ciberseguridad en Paraguay: entre la urgencia y la improvisación legislativa*. TEDIC. https://www.tedic.org/ciberseguridad-en-paraguay-entre-la-urgencia-y-la-improvisacion-legislativa/

59 Documento completo disponible en https://mdn.gov.py/wp-content/uploads/2024/11/Plan-Seguridad-para-el-Desarrollo-2023-2028.pdf

60 Al momento de elaboración de este informe, se encuentra en trámite el *Expediente D-2478767*, correspondiente al proyecto de ley "Que crea el Registro de Drones y regula su uso en la República del Paraguay", presentado en 2024 por el diputado Luis Federico Franco. Sin embargo, no se registran avances significativos en su tratamiento legislativo. Ver: Silpy (s/f). https://silpy.congreso.gov.py/web/expediente/134187

Por su parte, la adopción del Convenio de Chicago establece compromisos internacionales mínimos, pero no suple la necesidad de una legislación nacional comprehensiva. Tampoco el Reglamento R1103 de DINAC, centrado en criterios operativos, puede responder a las exigencias de constitucionalidad, transparencia y protección de derechos en el uso estatal de drones.

Ante el panorama actual, el uso estatal de drones en Paraguay, se da como práctica discrecional, sin límites claros ni mecanismos adecuados de control. De no mediar garantías efectivas, el espacio aéreo podría convertirse en un nuevo espacio de excepción jurídica donde rige más la opacidad que el derecho. Por ello, resulta urgente articular una respuesta jurídica que combine estándares internacionales, garantías constitucionales y mecanismos de control democrático en el uso de tecnologías de vigilancia aérea.

TABLA 2. Normas aplicadas a tecnología como Drones

Instrumento normativo	Contenido Relevante
Ley Nro. 1860/2001 – Código Aeronáutico Paraguayo	Establece principios generales sobre aeronáutica civil. No regula específicamente el uso de drones ni aspectos vinculados a derechos fundamentales.
Resolución DINAC N.º 2170/2017, que aprueba el Reglamento DINAC R1103 sobre Aeronaves Pilotadas a Distancia (RPAC) y Sistemas de Aeronaves Pilotadas a Distancia (RPAS)	Clasifica y regula aspectos técnicos de los drones (RPAS), como alturas de vuelo, seguros y zonas restringidas.
Convenio de Chicago de 1944 sobre Aviación Civil Internacional (Artículo 8)	Obliga a contar con autorización especial para que aeronaves sin piloto sobrevuelan el territorio nacional.
Estrategia Nacional de Ciberseguridad 2025–2028	Incluye la integración del Ministerio de Defensa en gobernanza digital, por lo que podría considerar un riesgo de militarización de ámbitos antes no abarcados y debilidad en garantías de derechos.
Plan Estratégico Seguridad para el Desarrollo 2023–2028	Plantea respuestas urgentes a amenazas híbridas, justifica adquisiciones de alta tecnología. No incorpora controles sobre uso estatal de drones.

Fuente: De elaboración propia

LIMITACIONES DEL ESTUDIO

Como toda investigación exploratoria que aborda fenómenos sensibles relacionados con seguridad, vigilancia estatal y Derechos Humanos, este estudio enfrenta una serie de limitaciones que es necesario reconocer.

En primer lugar, persisten restricciones significativas en el acceso a la información pública. Estas dificultades se deben, por un lado, a la escasa transparencia activa de las instituciones estatales y, por otro, a la clasificación de ciertos datos bajo la categoría de "seguridad nacional" o directamente a la inexistencia de registros sistemáticos sobre el uso de tecnologías de vigilancia aérea como los drones. Si bien se han presentado solicitudes formales de acceso a la información —como se detalla en el cuerpo del informe— las respuestas obtenidas fueron en muchos casos parciales, ambiguas o directamente inexistentes. Específicamente, al momento del cierre de este trabajo, entidades clave como el Ministerio de Defensa no habían respondido a las consultas, lo cual limita la trazabilidad de las prácticas institucionales y dificulta la identificación de responsabilidades.

En segundo lugar, a nivel metodológico, se reconoce la dificultad inherente a la cuantificación del impacto de estas tecnologías sobre derechos como la privacidad, especialmente en contextos donde no existen mecanismos de registro ni protocolos de supervisión ciudadana. Además, al tratarse de un estudio de escritorio basado principalmente en fuentes públicas y secundarias, es posible que no se haya logrado mapear la totalidad de los casos de uso relevantes, especialmente considerando que en el contexto paraguayo no existe un monitoreo sistemático de este tipo de tecnologías, como sí ocurre en zonas de conflicto a nivel internacional.

Por último, estas limitaciones no invalidan los hallazgos presentados, pero sí exigen una lectura prudente y contextualizada de los resultados. En este sentido, se ha procurado fortalecer la validez del análisis mediante la triangulación de fuentes, la transparencia metodológica y una reflexión crítica constante sobre el alcance y los límites de la evidencia disponible.

RECOMENDACIONES

Ante el avance del uso de drones en Paraguay y sus implicancias en materia de derechos fundamentales, se recomienda:

- Regular estrictamente su uso, bajo el principio de precaución, para evitar abusos y garantizar que las libertades civiles no sean socavadas. Existen antecedentes internacionales donde políticas de reconocimiento facial fueron revertidas por incumplir estándares de seguridad y Derechos Humanos, lecciones que pueden extrapolarse a los sistemas aéreos no tripulados.

- Fortalecer los mecanismos de control institucional y difusión normativa, asegurando una adecuada asesoría legal especializada para todos los actores del ciclo de vida de los drones —desde ingenieros y diseñadores hasta distribuidores, pilotos y usuarios finales—.

- Mejorar los sistemas de monitoreo y trazabilidad, desde la fabricación hasta la operación de los dispositivos. Esto incluye la inspección regular de talleres, la fiscalización de estándares técnicos y el control efectivo de la cadena de suministro, para evitar la circulación de drones irregulares o sin registro.

- Diseñar una regulación clara, accesible y actualizada, que incorpore salvaguardas para la privacidad, la protección de datos, el debido proceso y otros derechos fundamentales, conforme a estándares internacionales.

- Implementar campañas educativas y materiales de formación, orientadas tanto a operadores como a instituciones públicas y privadas. Estas deberían incluir guías prácticas, talleres y materiales audiovisuales que expliquen de manera comprensible los requisitos legales, las zonas de restricción, las obligaciones en materia de privacidad y las consecuencias legales de un uso indebido.

- Establecer mecanismos de transparencia y rendición de cuentas para el uso de drones por parte del Estado, especialmente en tareas de seguridad. Se recomienda la creación de plataformas públicas de información, la publicación proactiva de datos sobre despliegues y adquisiciones, y la habilitación de canales efectivos de denuncia, acompañamiento y reparación ante posibles abusos.

CONCLUSIONES

El uso de drones plantea desafíos y oportunidades que requieren ser abordados con urgencia desde un enfoque democrático, centrado en Derechos Humanos y justicia tecnológica. A pesar de sus beneficios potenciales —en áreas como logística, agricultura o monitoreo ambiental—, su despliegue en contextos de vigilancia y seguridad, sin marcos normativos robustos, puede derivar en prácticas intrusivas, opacas y desproporcionadas.

Paraguay enfrenta una situación crítica: un marco jurídico fragmentado, una institucionalidad débil y una tendencia creciente hacia la securitización del entorno digital. En este contexto, el vacío normativo habilita un uso discrecional de tecnologías de vigilancia aérea, sin garantías suficientes de transparencia, supervisión ni reparación.

Urge entonces avanzar hacia una regulación integral del uso de drones, que combine estándares técnicos con principios de legalidad, proporcionalidad y control democrático. Solo así se podrá evitar que estos dispositivos, originalmente diseñados para innovar, se conviertan en instrumentos de control que erosionen las libertades fundamentales que sostienen nuestro Estado de derecho.

REFERENCIA BIBLIOGRÁFICA

1. Este trabajo se enfoca en drones aéreos, aunque la tecnología no se limita a ese formato. Como señala Chamayou (2016), cualquier vehículo no tripulado —aéreo, terrestre o submarino— puede ser "dronizado", ampliando así el alcance del concepto más allá de lo aeronáutico.

2. High-altitude long endurance (mucha altitud y gran resistencia).

3. Ver más en el sitio de EASA: https://www.easa.europa.eu/en/document-library/general-publications/drone-class-identification-labels-and-information-notices

4. Esta información se basa en la respuesta oficial proporcionada por el MAG a la solicitud de acceso a la información pública (No 93399), disponible en el Portal Unificado de Información Pública. (Ministerio de Agricultura y Ganadería, 2025).

5. Según respuesta oficial del MITIC a la Solicitud No 93400, el ente reconoció poseer un dron con cámara marca DJI, modelo MINI 4 PRO (SNo 1581f6z9c239k0038je2), utilizado exclusivamente con fines publicitarios y de producción institucional (MITIC, 2025).

6. Si bien este trabajo se centra particularmente en los drones aéreos, resulta relevante destacar la complementariedad de este tipo de tecnologías en otros entornos, como lo demuestra el uso el uso del dron submarino "Blue Whale" por parte de Alemania para patrullajes defensivos en el mar Báltico (DCD, 2025).

7. El conflicto entre Rusia y Ucrania ha sido uno de los primeros enfrentamientos convencionales en los que los drones —comerciales y militares— han sido desplegados masivamente por ambos bandos, redefiniendo tácticas de guerra, reconocimiento y ataques selectivos (Edmonds & Bendett, 2022; Naciones Unidas, 2025).

8. Se ha documentado el uso sistemático de drones armados por parte de Israel en la Franja de Gaza, tanto para vigilancia como para ataques selectivos, generando un alto número de víctimas civiles y afectaciones psicológicas prolongadas en la población. (Ver: Abualouf, R. (2025, junio 26). Israeli strike at Gaza market kills 18 Palestinians, doctor and witnesses say. BBC. https://www.bbc.com/news/articles/cly8dlzx918o.

9. En los últimos años, Irán e Israel han protagonizado una escalada tecnológica mediante el uso de drones armados en ataques selectivos y operaciones de represalia. Ver: Reuters. (2025). Mapping the conflict between Israel and Iran. https://www.reuters.com/graphics/IRAN-NUCLEAR/ISRAEL/dwvklgrgjpm/

10. Para conocer más sobre los argumentos alrededor, ver la campaña "Stop Killer Robots" o "Paren a los Robots Asesinos": https://www.stopkillerrobots.org/

11. Así como el subtítulo del segmento advierte, no se citan todos los antecedentes ni se abarca todo el proceso historiográfico que involucra a esta tecnología. Se toman algunos momentos destacados para ilustrar de manera más o menos acabada la complejidad de ese proceso.

12. El modelo de dron AQM-34L fue utilizado en más de una treintena de ataques al norte de Vietnam. Puede verse una muestra del vehículo en el Museo de las Fuerzas Aereas Estad ounidenses: https://www.nationalmuseum.af.mil/Visit/Museum-Exhibits/Fact-Sheets/Display/Article/195747/teledyne-ryan-aqm-34l-firebee/

13. Sobre esta "Global war on terror", también existen otras cuestiones discutidas en el ámbito del derecho internacional. Rushby (2017) cita que "la mayoría de comentadores jurídicos que han considerado el concepto estadounidense de 'guerra global contra el terror', concluyen que esta no es una interpretación legítima del concepto de conflicto armado no internacional. Sin duda la misma crea problemas cuando consideramos la aplicación del DIH".

14. La propia BBC recogió una declaración dada a la AFP, donde un residente del sur de Gaza afirmó lo siguiente: "La gente está actualmente dentro de sus casas porque cualquiera que se mueva es atacado por los drones israelíes". Ver más en: https://www.bbc.com/mundo/articles/c3gg8dn55mdo

15. Ver más en: https://www.youtube.com/watch?v=to0EImeza30&t=608s

16. Ver intervención en: https://youtu.be/to0EImeza30?si=7TS5Qqu2i7cHmSGZ&t=195

17. Según el Informe de la Alta Comisionada de las Naciones Unidas para los Derechos Humanos titulado El derecho a la privacidad en la era digital (A/HRC/48/31, 2021), toda injerencia en el derecho a la intimidad debe perseguir un fin legítimo, y además ser necesaria y proporcional para alcanzarlo. Esta exigencia cobra especial relevancia en la era digital, donde los avances tecnológicos permiten formas de vigilancia cada vez más sofisticadas e intrusivas. El informe advierte que la falta de garantías adecuadas puede convertir estas prácticas en violaciones sistemáticas de derechos fundamentales.

18. Una categoría emergente que reconoce la necesidad de garantizar las libertades fundamentales en el entorno digital y frente al uso de tecnologías de vigilancia y control (Sequera & Lara Castro, 2020)

19. Como el derecho a la protección de datos personales, la neutralidad de la red, el acceso universal y el derecho al cifrado y al anonimato.

20. Los datos biométricos son "aquellos datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona humana, que permitan o confirmen su identificación única." (Vaninetti, 2020, Tomo I, p. 177).

21. Durante eventos masivos como el Carnaval de Río, las autoridades brasileñas han utilizado drones con cámaras de reconocimiento facial para monitorear multitudes. En 2019, en Salvador de Bahía, esta tecnología generó múltiples falsos positivos, incluyendo la detención injustificada de personas. Un informe de la Rede de Observatórios da Segurança reveló que el 96% de los alertas fueron ineficaces y el 90,5% de los detenidos eran personas negras. Estos casos ilustran los riesgos del uso combinado de drones y tecnologías biométricas, especialmente en espacios públicos festivos, donde pueden vulnerar derechos como la privacidad, la presunción de inocencia y la no discriminación. Véase:
Lourenco, B. (2025, marzo 01). O reconhecimento facial no carnaval não protege, ele controla. Opinión. CartaCapital. https://www.cartacapital.com.br/opiniao/o-reconhecimento-facial-no-carnaval-nao-protege-ele-controla/

22. Al momento de redacción de este trabajo, el proyecto de Ley de Protección de Datos Personales (Exp. D-2162170) fue aprobado por Diputados el 27 de mayo de 2025 y está en estudio en Senadores. Más información en SilPy: https://silpy.congreso.gov.py/web/expediente/123459.

23. Véase: TEDIC. (2025, 17 de julio). Paraguay necesita una ley de protección de datos personales robusta, con estándares internacionales y garantías reales [Entrada de blog]. https://www.tedic.org/paraguay-necesita-una-ley-de-proteccion-de-datos-personales-robusta-con-estandares-internacionales-y-garantias-reales/

24. Véase: DNCP. (2025, junio 30). Convocatoria de la Licitación 471787. “Compra de drones de vigilancia y sus accesorios para la ANNP”. https://www.contrataciones.gov.py/licitaciones/convocatoria/1f047be6-591c-68b6-86f1-cf1a04e1d9e5.html#pliego

25. Corte Interamericana de Derechos Humanos. Tristán Donoso v. Panamá. Sentencia de 27 de enero de 2009. Serie C No. 193. https://www.corteidh.or.cr/docs/casos/articulos/seriec_193_esp.pdf

26. Corte Interamericana de Derechos Humanos. Escher y otros vs. Brasil. Sentencia de 6 de julio de 2009. https://www.corteidh.or.cr/docs/casos/articulos/seriec_200_esp1.pdf

27. La “expectativa razonable de privacidad” es un estándar jurídico originado en el caso Katz v. United States (1967), según el cual una persona puede esperar que ciertas acciones o comunicaciones permanezcan privadas, incluso en espacios públicos, siempre que esa expectativa sea socialmente reconocida como legítima. Por ejemplo, alguien caminando por un parque tranquilo podría razonablemente esperar no ser grabado ni seguido por un dron, a diferencia de quien asiste a una manifestación pública frente al Congreso, donde la vigilancia puede estar más justificada aunque no ilimitada. Esta distinción resulta clave al evaluar si una intervención vulnera o no el derecho a la privacidad.

28. Véase: Corte Interamericana de Derechos Humanos (CIDH). (1985). Opinión Consultiva OC-5/85 del 13 de noviembre de 1985. La colegiación obligatoria de periodistas (arts. 13 y 29 Convención Americana sobre Derechos Humanos).https://www.corteidh.or.cr/tablas/a12040.pdf

29. Para conocer el documento remitido, véase: Ministerio del Interior. (2025, julio 10). Memorándum DGTYC No 055/2025. Solicitud 93397. Portal Unificado de Información Pública. https://informacionpublica.paraguay.gov.py/#!/ciudadano/solicitud/93402https://informacionpublica.paraguay.gov.py/#!/ciudadano/solicitud/93397

30. Ver: Ramírez, A. (2025, mayo 13). IMSI catchers en Paraguay: La vigilancia invisible que amenaza tu derecho a manifestarte [Entrada de blog]. TEDIC. https://www.tedic.org/imsi-catchers-en-paraguay-la-vigilancia-invisible-que-amenaza-tu-derecho-a-manifestarte/

31. Para acceder a la resolución, véase: DINAC. (2017). Resolución N° 2170/2017: Por la que se aprueba el Reglamento DINAC R 1103 - Reglamento de Aeronaves Piloteadas a Distancia (RPA) y Sistema de Aeronaves Piloteadas a Distancia (RPAS). Dirección Nacional de Aeronáutica Civil. https://www.dinac.gov.py/v3/index.php/documentos1/leyes-decretos-resoluciones-circulares/item/1814-resolucion-n-2170-2017-por-la-que-se-aprueba-el-reglamento-dinac-r-1103-reglamento-de-aeronaves-piloteadas-a-distancia-rpa-y-sistema-de-aeronaves-piloteadas-a-distancia-rpas

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

33. Véase: EFF. (2014). Necesarios y Proporcionados: sobre la aplicación de los Derechos Humanos a la vigilancia de las Comunicaciones. https://necessaryandproportionate.org/es/principios/

34. Robert Alexy es un reconocido jurista y filósofo del derecho alemán, cuya teoría de los derechos fundamentales y del principio de proporcionalidad ha tenido una influencia decisiva en la jurisprudencia constitucional contemporánea. Su formulación del test de proporcionalidad (compuesto por los subprincipios de idoneidad, necesidad y proporcionalidad en sentido estricto) se ha consolidado como una herramienta clave para evaluar la legitimidad de restricciones a derechos fundamentales. Su propuesta permite ponderar racionalmente conflictos entre principios y establecer límites jurídicamente justificados a medidas intrusivas, lo que la convierte en un estándar adoptado tanto por cortes constitucionales como por instrumentos internacionales de Derechos Humanos.

35. Sobre el punto, TEDIC ha señalado que, estos procesos suelen llevarse a cabo sin consentimiento informado, sin mecanismos claros de control ciudadano y sin transparencia respecto a quién administra los datos, con qué fines, durante cuánto tiempo y bajo qué condiciones de seguridad. Ver: TEDIC. (2025, julio 23). Expo Paraguay 2025: Vigilancia, desprotección y exclusión a la ciudadanía [Entrada de blog]. https://www.tedic.org/-expo-paraguay-2025-vigilancia-desproteccion-y-exclusion-a-la-ciudadania/

36. El colonialismo de datos describe una nueva fase de apropiación sistemática de información personal que reproduce lógicas extractivas coloniales en el entorno digital, particularmente sobre poblaciones vulnerables (Couldry & Mejias, 2019).

37. Por poder de policía se entiende la facultad del Estado para intervenir en la vida de las personas a fin de mantener el orden y gestionar lo público, aun cuando ello implique imponer límites o restricciones.

38. DNCP. (2023, octubre 10). Convocatoria de la Licitación No435980 - “Adquisición de drones con accesorios”. https://www.contrataciones.gov.py/licitaciones/adjudicacion/435980-adquisicion-drone-accesorios-1/resumen-adjudicacion.html

39. Para acceder al documento completo, ver: Consejo de Defensa Nacional (2023). Plan Seguridad para el Desarrollo 2023-2028. https://mdn.gov.py/wp-content/uploads/2024/11/Plan-Seguridad-para-el-Desarrollo-2023-2028.pdf

40. El Ejército del Pueblo Paraguayo (EPP) es un grupo armado insurgente de orientación marxista-leninista que opera en el norte de Paraguay desde la década del 2000. Fue señalado por el Estado paraguayo como responsable de secuestros, atentados y actividades vinculadas al narcotráfico, y declarado organización terrorista por el gobierno paraguayo (Wikipedia, s/f).

41. Entre los antecedentes más relevantes de la Fuerza de Tarea Conjunta (FTC) se encuentra el caso del fallecimiento de María del Carmen y Liliana Villalba, niñas de 11 años, ocurrido el 2 de septiembre de 2020 durante un operativo contra el Ejército del Pueblo Paraguayo (EPP). El Comité de los Derechos del Niño de las Naciones Unidas concluyó, tras una investigación, que el Estado paraguayo incurrió en graves violaciones de Derechos Humanos en relación con estos hechos (Paraguay, responsable de graves violaciones de Derechos Humanos por la muerte de dos niñas, según un comité de la ONU, 2025). Ver resolución en: https://www.ohchr.org/es/press-releases/2025/01/paraguay-responsible-grave-rights-violations-over-deaths-two-young-girls-un

42. Hasta el momento de redacción de este trabajo, las fuerzas militares paraguayas no respondieron un pedido de acceso a la información pública que solicitaba datos e información sobre sus reglamentaciones en torno a los operativos con drones y otras cuestiones relacionadas. Ver solicitud en: https://informacionpublica.paraguay.gov.py/#!/ciudadano/solicitud/93452

43. Véase: DNCP. (2024, octubre 09). Convocatoria a Licitación No 452492, titulada “Adquisición de drones para la Armada Paraguaya” https://www.contrataciones.gov.py/licitaciones/adjudicacion/1ef81a27-0ad0-69dc-9e86-f7c6d914c1a2/resumen-adjudicacion.html

44. Según el Censo Indígena Nacional (Instituto Nacional Indígena, 2022), aproximadamente el 2% de la población se identifica como indígena, perteneciente a 19 pueblos originarios organizados en cinco familias lingüísticas. A esto se suma una creciente visibilidad de la comunidad afrodescendiente y una mayoría poblacional que se identifica como mestiza. Además, el 77% de la población paraguaya declara ser bilingüe en guaraní y español, lo cual evidencia la centralidad de la identidad cultural indígena en la vida cotidiana del país (DGEEC, 2022). Esta pluralidad étnica, cultural y lingüística requiere enfoques diferenciados para prevenir sesgos algorítmicos y garantizar el respeto a los Derechos Humanos.

45. El concepto de interseccionalidad fue desarrollado por la jurista afroamericana Kimberlé Crenshaw (1989) para explicar cómo múltiples formas de discriminación —como el racismo, el sexismo y la desigualdad de clase— se entrelazan y generan experiencias específicas de opresión, particularmente sobre las mujeres negras. En el ámbito de las tecnologías, este enfoque permite analizar cómo los impactos no se distribuyen de forma homogénea, sino que afectan con mayor intensidad a quienes se encuentran en la intersección de múltiples vulnerabilidades.

46. En este trabajo, el término sesgo alude a errores sistemáticos en tecnologías como drones equipados con algoritmos de vigilancia o toma de decisiones automatizadas. Estos sesgos pueden tener raíces estadísticas, sociales o institucionales (Bellamy, 2019) y, en el caso de tecnologías aplicadas a la seguridad, derivar en patrones de vigilancia desigual o perfilamiento erróneo de ciertas poblaciones. Aunque muchas veces son involuntarios, suelen originarse en datos no representativos o en variables mal definidas, lo que contribuye a amplificar desigualdades al impactar de forma desproporcionada a grupos vulnerables (Barocas & Selbst, 2016).

47. Para conocer a detalle los datos reportados, véase: Instituto Nacional de Estadísticas (INE). (2025, junio). Tecnología de la Información y Comunicación en el Paraguay. EPHC 2024. https://www.ine.gov.py/publication-single.php?codec=280

48. Para acceder al material, véase: MITIC. (2022). Plan Nacional de TIC 2022-2030. https://mitic.gov.py/plan-nacional-de-tic-2022-2030/

49. El reshoring es la práctica de traer de vuelta al país actividades productivas que antes se realizaban en el extranjero. En EE.UU., el Estado ha impulsado esta estrategia especialmente en sectores tecnológicos clave.

50. Los Convenios de Ginebra de 1949 y sus Protocolos adicionales constituyen el núcleo del Derecho Internacional Humanitario. Son cuatro tratados internacionales que establecen normas para limitar los efectos de los conflictos armados y proteger a quienes no participan directamente en las hostilidades —como la población civil, el personal médico y humanitario— así como a quienes han dejado de participar, como los soldados heridos, enfermos, náufragos o prisioneros de guerra. Para conocer el texto completo y sus comentarios oficiales, véase: Comité Internacional de la Cruz Roja (CICR). Los Convenios de Ginebra y sus Comentarios – Enlaces útiles. Disponible en: https://www.icrc.org/es/derecho-y-politicas/los-convenios-de-ginebra-y-sus-comentarios

51. ARTICLE 19. (1996). Los Principios de Johannesburgo sobre la seguridad nacional, la libertad de expresión y el acceso a la información. ARTÍCULO 19. https://www.corteidh.or.cr/tablas/a22440.pdf

52. La Recomendación de la UNESCO sobre la Ética de la Inteligencia Artificial (2021) fue adoptada por consenso por los 193 Estados miembros, incluido Paraguay. Este instrumento establece principios y directrices para el diseño y uso responsable de tecnologías emergentes, incluyendo salvaguardas específicas para la protección de los Derechos Humanos, la inclusión y la justicia social. Por su parte, la OCDE ha desarrollado una serie de principios sobre inteligencia artificial (Principles on AI, 2019) que promueven el respeto a los Derechos Humanos, la transparencia, la rendición de cuentas y el desarrollo centrado en el ser humano. Ambos marcos, si bien no son vinculantes, constituyen referencias internacionales clave para la gobernanza ética y democrática de tecnologías como los drones y los sistemas automatizados.

53. Véase: Reglamento Delegado (UE) 2023/659 de la Comisión de 2 de diciembre de 2022, que modifica el Reglamento (UE) n.o 452/2014 en lo relativo a los requisitos técnicos y procedimientos administrativos aplicables a operadores extranjeros en operaciones aéreas. https://noticias.juridicas.com/base_datos/Admin/749716-regl-2023-659-ue-de-2-dic-2022-modificacion-del-regl-ue-n-o-452-2014.html

54. Para consultar los documentos normativos pertinentes, puede acceder al sitio oficial de la DINAC en la sección “Leyes, Decretos, Resoluciones y Circulares”: https://www.dinac.gov.py/v3/index.php/documentos1/leyes-decretos-resoluciones-circulares

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

56. Ver: Sequera Buzarquis, M. (2025, 24 de junio). La Evolución de la Ciberseguridad en Paraguay: MITIC como Pilar Estratégico. TEDIC. https://www.tedic.org/ciberseguridad-en-paraguay-entre-la-urgencia-y-la-improvisacion-legislativa/

57. Documento completo disponible en la plataforma de archivos del MITIC. https://drive.mitic.gov.py/s/ZS7YXfEJrxfgdia?dir=/&editing=false&openfile=true

58. Ver: Sequera Buzarquis, M. (2025, 23 de junio). Ciberseguridad en Paraguay: entre la urgencia y la improvisación legislativa. TEDIC. https://www.tedic.org/ciberseguridad-en-paraguay-entre-la-urgencia-y-la-improvisacion-legislativa/

59. Documento completo disponible en https://mdn.gov.py/wp-content/uploads/2024/11/Plan-Seguridad-para-el-Desarrollo-2023-2028.pdf

60. Al momento de elaboración de este informe, se encuentra en trámite el Expediente D-2478767, correspondiente al proyecto de ley "Que crea el Registro de Drones y regula su uso en la República del Paraguay", presentado en 2024 por el diputado Luis Federico Franco. Sin embargo, no se registran avances significativos en su tratamiento legislativo. Ver: Silpy (s/f). https://silpy.congreso.gov.py/web/expediente/134187

Tecnología
& Derechos
Humanos