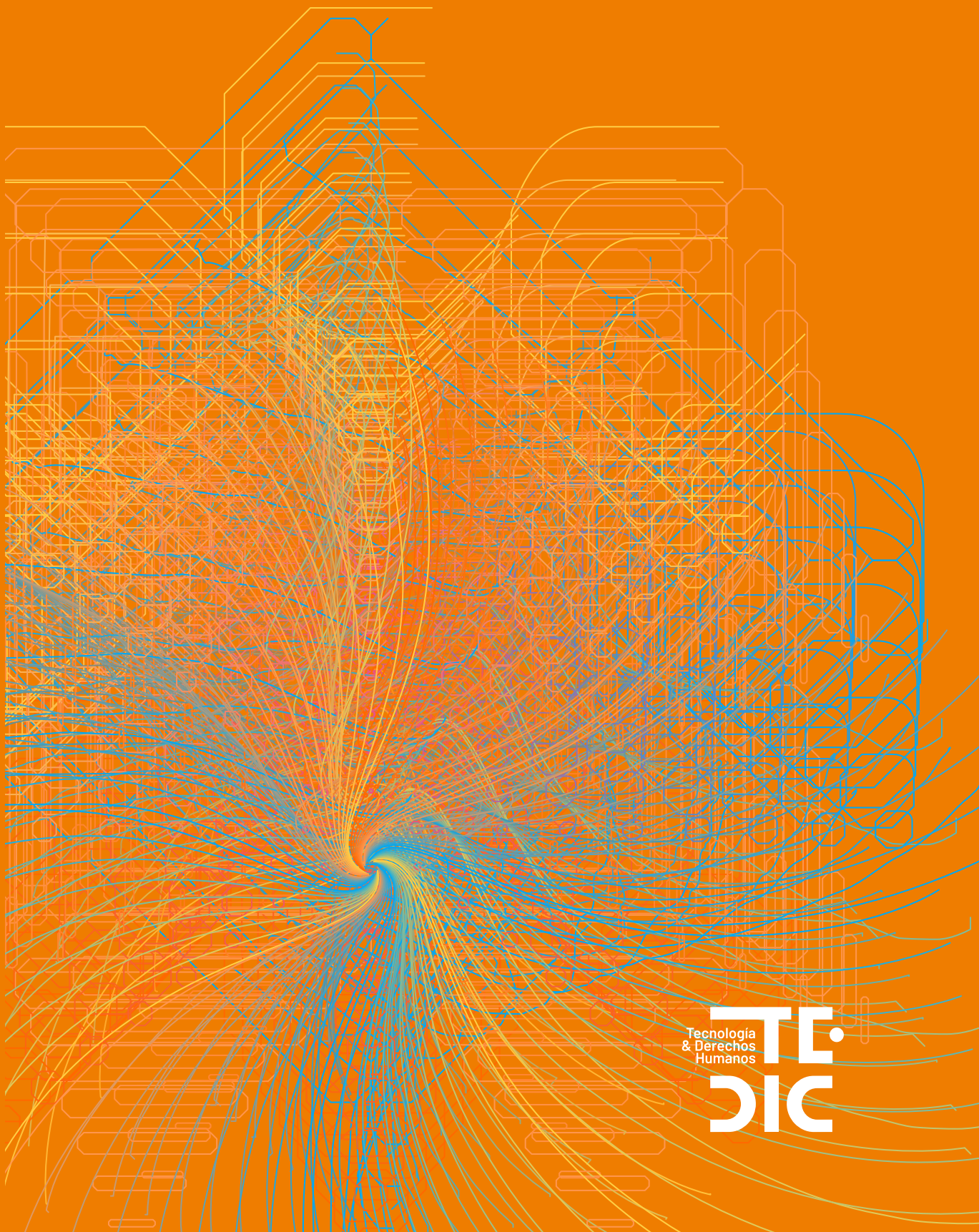
CON MI CARA NO

Implementación de las cámaras de reconocimiento facial por el Estado paraguayo



Tecnología & Derechos Humanos

TEDIC

CON MI CARA NO

Implementación de las cámaras de reconocimiento facial por el Estado paraguayo

Tecnología & Derechos Humanos

Esta investigación fue elaborada en el marco del Proyecto **#MásCiudadaníaMenosCorrupción**, con el apoyo de la Fundación Cird y de INDELA – AVINA.

Este documento es parte de la campaña de TEDIC **#MisDatosMisDerechos** y de la subcampaña **#ConMiCaraNo**.

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.

CON MI CARA NO

Implementación de las cámaras de reconocimiento facial por el Estado paraguayo

DICIEMBRE 2024

INVESTIGACIÓN
Graciela Galeano
Gerardo Paciello
Leonardo Gómez Berniga

COLABORACIÓN
Maricarmen Sequera
Giuliana Galli

EDICIÓN EDITORIAL
Maricarmen Sequera

COMUNICACIÓN Y REVISIÓN DE ESTILO
Araceli Ramírez

DIAGRAMACIÓN
Horacio Oteiza

TABLA DE CONTENIDOS

RESUMEN EJECUTIVO

Este estudio analiza la implementación de cámaras de reconocimiento facial en Paraguay, destacando preocupaciones clave relacionadas con la transparencia, los derechos humanos y la corrupción. Desde 2018[1], TEDIC ha alertado sobre los riesgos y la ineficacia potencial de estas tecnologías. Sin embargo, su expansión ha continuado sin una regulación adecuada, lo que agrava problemáticas como la falta de documentación sobre cámaras robadas o extraviadas y la compra de equipos ineficientes.

El informe señala que, desde 2018, la Policía Nacional de Paraguay ha incrementado significativamente el uso de cámaras con reconocimiento facial. No obstante, los resultados han sido ambiguos, generando inquietudes sobre la privacidad y la seguridad de los datos personales. Asimismo, se identificaron patrones preocupantes de adquisiciones cuestionables y una alarmante falta de transparencia en los procesos de licitación, que crean condiciones propicias para la corrupción.

El estudio también cuestiona la legalidad de utilizar los Fondos de Servicios Universales (FSU) de la Comisión Nacional de Telecomunicaciones (CONATEL) para financiar estas compras, argumentando que no se alinean con los objetivos del fondo. Además, resalta la necesidad urgente de una legislación integral de protección de datos personales y critica la opacidad de las respuestas institucionales a solicitudes de información pública.

En sus conclusiones, el informe enfatiza que la adquisición y uso de cámaras de reconocimiento facial se realizó sin un marco legal adecuado, vulnerando principios de derechos humanos y exponiendo a la población a vigilancia masiva y discriminación. Por ello, esta investigación insta a monitorear los proyectos en curso del sector público y a abordar estas problemáticas desde una perspectiva global y de derechos humanos, considerando la creciente tendencia a implementar tecnologías invasivas sin la debida protección de las libertades civiles.

PALABRAS CLAVES: *Reconocimiento facial, biometría, privacidad, datos personales.*

1 TEDIC. 2018. Biometría y vigilancia: la enajenación continua de nuestros derechos. Disponible en: https://www.tedic.org/wp-content/uploads/2018/12/La-enajenaci%C3%B3n-continua-de-nuestros-derechos_TEDIC_2018-2.pdf

GLOSARIO

ANNP	Administración Nacional de Navegación y Puertos
CJI	Comité Jurídico Interamericano
CONATEL	Comisión Nacional de Telecomunicaciones
CSE	Centro de Seguridad y Emergencias
DINAC	Dirección Nacional de Aeronáutica Civil
DNCP	Dirección Nacional de Contrataciones Públicas
EPH	Encuesta Permanente de Hogares
FSU	Fondo de Servicios Universales
IP	Protocolo de Internet (por sus siglas en inglés: Internet Protocol)
MEC	Ministerio de Educación y Ciencias
MITIC	Ministerio de Tecnologías de la Información y Comunicación
PIDCP	Pacto Internacional de Derechos Civiles y Políticos
PTZ	Panorámica, Inclinación y Zoom (por sus siglas en inglés: Pan, Tilt, Zoom)
RF	Reconocimiento Facial
SADLE	Sistema De Atención Y Despacho De Llamadas De Emergencia

INTRODUCCIÓN

En 2018, la Policía Nacional, el Ministerio del Interior y la Comisión Nacional de Telecomunicaciones (CONATEL) anunciaron la implementación de un nuevo sistema de videovigilancia con tecnología biométrica[2]. En ese momento, TEDIC ya expresaba[3] su preocupación acerca de la posible ineficacia de esta medida para abordar la inseguridad. Sin embargo, lo más importante era la advertencia sobre los riesgos asociados a la introducción de tecnologías de reconocimiento facial.

Estas preocupaciones se centraban en las implicaciones para la privacidad y los derechos individuales, así como en la posibilidad de que estas prácticas perpetúen un legado de autoritarismo. Además, se evidenciaba una preocupante falta de transparencia y rendición de cuentas en la adquisición y gestión de estas tecnologías.

En la investigación mencionada más arriba, TEDIC ya alertaba sobre los riesgos asociados a la gestión de datos obtenidos mediante softwares de reconocimiento facial. Estos riesgos no solo se refieren a la privacidad y seguridad de los datos personales, sino también a las posibles consecuencias para la democracia en un país aún marcado por las sombras de su pasado dictatorial. El estudio subrayaba la importancia de una mayor supervisión y regulación en el uso de tecnologías de vigilancia para proteger las libertades civiles y prevenir el abuso de poder.

Seis años después de la publicación de ese informe titulado “La enajenación continua de nuestros derechos”, este nuevo estudio busca evaluar las acciones emprendidas por las diversas instituciones gubernamentales para adoptar tecnologías de reconocimiento facial en Paraguay.

El argumento principal detrás de las adquisiciones analizadas en esta investigación se basó en la expansión de dispositivos y sistemas diseñados para almacenar información sensible con el objetivo de ejercer un mayor control. Sin embargo, estas iniciativas han ignorado aspectos críticos relacionados con la seguridad de los datos personales, su uso adecuado y su exposición a vulnerabilidades, debido a la ausencia de las precauciones necesarias.

Este análisis busca proporcionar una perspectiva sobre cómo el Estado ha manejado estas tecnologías , sus implicaciones en la privacidad y la seguridad de la ciudadanía y la eficacia real de estas herramientas en una supuesta mejora de la seguridad pública. Además, destaca la continua falta de un marco legal adecuado y de medidas de protección de datos que garanticen los derechos de las personas ciudadanas de Paraguay.

Con esta investigación buscamos ofrecer una visión integral del proceso y la evolución en la adquisición y uso de estas tecnologías por parte del Estado entre 2018 y 2023. Además, se analiza críticamente los resultados obtenidos, cuestionando si durante este período se implementaron medidas efectivas para garantizar la seguridad de los ciudadanos. El enfoque en acumular datos sensibles sin adoptar las precauciones necesarias en materia de seguridad y privacidad expone graves deficiencias en la gestión y protección de la información personal.

---

2 La videovigilancia biométrica implica el uso de cámaras de seguridad que integran sistemas de identificación y autenticación de la identidad de las personas. Aunque comúnmente se emplea el reconocimiento facial para la identificación, también pueden utilizarse otras tecnologías biométricas, como el análisis de iris, movimiento corporal, huellas dactilares, entre otras.

3 TEDIC. 2018. Biometría y vigilancia: la enajenación continua de nuestros derechos. Disponible en: https://www.tedic.org/wp-content/uploads/2018/12/La-enajenaci%C3%B3n-continua-de-nuestros-derechos_TEDIC_2018-2.pdf

METODOLOGÍA DE LA INVESTIGACIÓN

CONSIDERACIONES METODOLÓGICAS

La revisión metodológica se llevó a cabo a través de varios procedimientos para obtener información sobre la adquisición de tecnologías de reconocimiento facial por parte del Estado y más específicamente de la Policía Nacional. Puntualmente, se trabajó a partir de distintos métodos:

- Revisiones documentales de leyes e información tanto nacionales como internacionales en materia de derechos humanos y la buena gestión de la información privada.
- Búsquedas de información en la página oficial de la Dirección Nacional de Contrataciones Públicas (DNCP), en la página de Comisión Nacional de Telecomunicaciones (CONATEL) y en los medios de prensa.
- Solicitudes de acceso a la información a instituciones del Estado sobre la compra de cámaras o softwares de reconocimiento facial.

REVISIÓN DOCUMENTAL

Para iniciar esta investigación, en la revisión documental se realizaron tres preguntas puntuales:

- ¿Qué leyes o acuerdos internacionales avalan la protección de los derechos humanos en materia de privacidad y protección de datos?
- ¿Hay información veraz, accesible y concreta que aporte transparencia a los procesos de compra y uso de tecnología de reconocimiento facial?
- ¿Qué iniciativas se están proyectando a nivel legislativo que pueden servir de protección o pueden significar un mayor riesgo en cuanto a la vigilancia y al manejo de datos personales?

ESTRATEGIAS DE BÚSQUEDA DE INFORMACIÓN

La investigación se llevó a cabo a partir de la consulta de cuatro tipos principales de fuentes de información: en primer lugar, se analizaron páginas web que registran la mayoría de las licitaciones nacionales y compras realizadas por instituciones públicas, así como sitios oficiales estatales relacionados con la seguridad. En segundo lugar, se revisaron medios de prensa para identificar coberturas relevantes. También se incluyeron investigaciones y artículos elaborados por organizaciones defensoras de derechos humanos. Por último, se consultaron plataformas con información detallada sobre proyectos de ley, normativas aprobadas y estándares internacionales, tal como se detalla en la Tabla 1.

TABLA 1. Lista de fuentes de información secundarias

Base de datos estatales	Medios de Comunicación	Investigaciones y artículos de organizaciones	Páginas internacionales
Dirección Nacional de Contrataciones Públicas (DNCP)	ABC Color	TEDIC	Naciones Unidas
Policía Nacional	Última Hora	AlSur	Global Investigative Journalism Network
Comisión Nacional de Telecomunicaciones (CONATEL)	La Nación	Red por los Derechos Digitales	
Sistema de información legislativa - Paraguay (SILPY)		Coordinadora de los derechos humanos (CODEHUPY)	

Para lograr la filtración de datos puntualmente en la página de la DNCP, el equipo de investigación buscó en la categoría 25, referente a "Equipos Militares y de Seguridad. Servicio de Seguridad y Vigilancia".

También combinaron palabras claves como "circuito cerrado", "cámaras", "reconocimiento facial", "Sistema 911" y "Policía Nacional". Estas mismas palabras claves fueron empleadas para las demás fuentes estatales y medios de prensa, así como señala la Tabla 2.

En este punto, el criterio para seleccionar la información de los medios de prensa es que hayan realizado estas publicaciones entre 2019 y 2023, considerando que en 2018 la Policía Nacional anunciaba oficialmente la implementación de tecnología de reconocimiento facial.

TABLA 2. Lista de palabras claves principales y alternativas

Palabras claves principales	Palabras claves alternativas
Cámaras	Sistema 911
Circuito cerrado	Policía Nacional
Reconocimiento facial	CONATEL
Seguridad	Software

PEDIDO DE INFORMACIÓN PÚBLICA

El equipo de investigación presentó más de 40 solicitudes de acceso a la información pública a un total de 35 instituciones del Estado entre agosto y septiembre de 2023. Estas instituciones incluyen direcciones, secretarías y ministerios del Poder Ejecutivo, así como entidades del Poder Judicial y Legislativo, además de municipalidades y gobernaciones, tal como se detalla en la Tabla 3.

Una de las principales consultas se enfocó en determinar si estas instituciones habían adquirido sistemas de tecnología biométrica, cámaras o software de reconocimiento facial, y si los integraron al sistema 911 de la Policía Nacional. También se indagó sobre la implementación de cámaras de circuito cerrado y otros sistemas de vigilancia, además de preguntar si cuentan con protocolos específicos para el manejo y almacenamiento de datos personales.

De manera particular, se solicitó a la Policía Nacional y al Ministerio del Interior información concreta sobre la cantidad de cámaras con reconocimiento facial adquiridas hasta la fecha y su ubicación actual.

TABLA 3. Lista de instituciones del Estado que recibieron una solicitud de acceso a la información pública.

Policía Nacional del Paraguay
Ministerio de Educación y Ciencias (MEC)
Gobernación de Misiones
Gobernación de Paraguarí
Administración Nacional de Navegación y Puertos (ANNP)
Dirección Nacional de Migraciones
Gobernación de Itapúa
Gobernación del Departamento Central
Secretaría Nacional de Administración de Bienes Incautados y Comisados (SENABICO)
Honorable Cámara de Senadores
Gobernación de Guairá
Ministerio de Obras Públicas y Comunicaciones (MOPC)
Dirección Nacional de Aeronáutica Civil (DINAC)
Gobernación de Presidente Hayes
Gobernación de Boquerón
Ministerio de Hacienda (MH)
Ministerio de Justicia (MJ)
Secretaría Nacional Antidrogas (SENAD)
Comisión Nacional de Telecomunicaciones (CONATEL)
Entidad Binacional Yacyretá (EBY)
Gobernación de Caaguazú

Municipalidad de Ciudad del Este
Municipalidad de Pedro Juan Caballero
Municipalidad de Caacupé
Gobernación de Cordillera
Honorable Cámara de Diputados
Ministerio de Tecnologías de la Información y Comunicación (MITIC)
Municipalidad de Caaguazú
Municipalidad de Caazapá
Dirección Nacional de Aduanas (ADUANAS)
Gobernación de Alto Paraná
Gobernación de Concepción
Gobernación de San Pedro
Ministerio del Interior (MDI)

BIOMETRÍA Y DERECHOS HUMANOS

Los datos biométricos, como el rostro, el iris, el tono de voz y la forma de caminar, son características únicas que permiten identificar a una persona[4]. Los sistemas de reconocimiento facial recopilan y tratan estos datos altamente sensibles, que no pueden modificarse fácilmente como otros datos personales como reimprimir una cédula de identidad o una tarjeta de crédito cuando se pierden o roban. Esto los hace especialmente vulnerables a filtraciones o robos, lo que pone en riesgo la privacidad y el control sobre la identidad de las personas. Además, el uso de esta tecnología facilita la vigilancia masiva y la creación de perfiles detallados, lo que la convierte en una herramienta intrusiva y desproporcionada que podría sustituirse por métodos menos invasivos y más respetuosos de los derechos humanos. (Privacy Internacional, 2013)

Los sistemas de vigilancia masiva con capacidad de recolección remota de estos datos pueden capturarlos en espacios públicos como estaciones de buses y calles[5]. La tendencia del uso de cámaras de reconocimiento facial se hizo común en algunos lugares, y para funcionar, estos dispositivos requieren bases de datos biométricos para comparar lo que registran (fotos o videos) con listados, generalmente de personas prófugas o con antecedentes criminales.

Estos sistemas son propensos a errores de identificación, especialmente en personas de tez oscura, mujeres y personas adultas mayores[6]. Cuando se detiene a alguien debido a un error del sistema que lo confunde con una persona con historial delictivo, se generan falsos positivos que pueden poner en riesgo la integridad de la persona afectada, desencadenando situaciones injustas y violaciones a sus derechos.

TRATAMIENTO DE DATOS PERSONALES EN VIDEOVIGILANCIA

El tratamiento de datos personales incluye la captura de imágenes de personas identificadas o identificables mediante cámaras, videocámaras u otros dispositivos tecnológicos, generalmente con fines de seguridad. Este proceso no solo abarca la grabación de dichas imágenes, sino también su almacenamiento y posterior utilización para diversos propósitos. Al implicar el manejo de información personal, estas actividades deben estar reguladas bajo una normativa específica de protección de datos.

La instalación y uso de estos sistemas de videovigilancia deben cumplir con estrictos requisitos legales y operativos, fundamentados en principios de protección de datos personales y privacidad. Este marco normativo busca garantizar que su implementación no exceda los límites legales ni vulnere los derechos fundamentales reconocidos tanto en el ámbito nacional como internacional.

4 EFF. 2018. Biometrics: facial recongnition. Disponible en: https://www.eff.org/document/facial-recognition-one-pager

5 TEDIC. 2023 “Con mi cara no”: la vigilancia masiva a través del reconocimiento facial en Paraguay. Disponible en https://www.tedic.org/wp-content/uploads/2022/08/Fanzine-Biometria-web.pdf

6 Muchas aplicaciones de técnicas de clasificación facial y biométrica, que intentan predecir aspectos como el género o las emociones, se basan en teorías científicamente insustentables como la frenología y la fisionomía. Esto lleva a inferencias no válidas que perpetúan la discriminación y aumentan el daño causado por la caracterización incorrecta y la vigilancia. Coalition for Critical Technology. 2020. Aolish the @TechToPrisonPipeline. Disponible en: https://medium.com/@CoalitionForCriticalTechnology/abolish-the-techtoprisonpipeline-9b5b14366b16

En países como Argentina, España y Perú, estas regulaciones incluyen medidas adicionales, como la obligación de instalar anuncios visibles en las áreas donde se encuentran las cámaras. Dichos anuncios deben proporcionar información clara sobre el responsable del tratamiento de los datos, así como medios de contacto accesibles, promoviendo la transparencia y el control ciudadano sobre el uso de estas tecnologías.

En este contexto, la biometría se reconoce como una categoría de datos personales sensibles debido a su vínculo con características únicas que permiten identificar a las personas. Según la investigación "La enajenación continua de nuestros derechos" (Alonzo et al., 2018)[7] y el fanzine "Con mi cara no"[8] de TEDIC (2023), los datos biométricos incluyen tanto rasgos físicos como comportamientos específicos y se clasifican en dos grandes grupos:

1. **Datos físicos y fisiológicos:** Comprenden características corporales únicas como huellas dactilares, rasgos faciales, geometría de la mano, patrones de ADN, estructuras de la retina e iris, forma de partes del cuerpo como la mano o la oreja, e incluso el mapa de venas.
2. **Datos de comportamiento:** Abarcan patrones conductuales como la voz, la firma, la forma de caminar o la manera de interactuar con dispositivos, como escribir en un teclado.

El reconocimiento facial, una de las tecnologías biométricas más utilizadas, plantea implicancias significativas en términos de derechos humanos y privacidad. Según Al Sur[9] (2021), "El reconocimiento facial es una tecnología biométrica que, a través del análisis de rasgos faciales característicos, busca establecer la identidad de una persona. Aunque es menos precisa que otras formas de identificación biométrica, como la lectura de huellas dactilares o del iris, su principal ventaja es que no requiere contacto físico".

Esta característica permite su despliegue en espacios públicos para vigilancia a gran escala, a menudo sin que las personas sean conscientes de que están siendo monitoreadas. Este tipo de vigilancia, conocido como vigilancia masiva, consiste en la supervisión de grandes grupos de personas sin que existan sospechas específicas sobre ellas. Según Maynier[10] (2023), la vigilancia masiva puede implementarse mediante tecnologías como el reconocimiento facial en cámaras ubicadas en áreas urbanas o mediante escuchas telefónicas.

La vigilancia masiva basada en datos biométricos, como el reconocimiento facial, expone a las personas a graves riesgos de vulneración de su privacidad. La Comisión Europea[11] (2023) señala que los datos biométricos son altamente sensibles y están sujetos a condiciones estrictas de tratamiento, incluyendo aquellos que revelan el origen racial o étnico, opiniones políticas, convicciones religiosas, afiliación sindical, datos genéticos, o información relativa a la salud, vida sexual u orientación sexual.

---

7 Alonzo, Carrillo y Sequera, 2018. La enajenación continua de nuestros derechos. Sistemas de identidad: Biometría y cámras de vigilancia no reguladas en Paraguay. TEDIC. Disponible en: https://www.tedic.org/la-enajenacion-continua-de-nuestros-derechos-sistemas-de-identidad-biometria-y-camaras-de-vigilancia-no-reguladas-en-paraguay/

8 TEDIC. 2023 "Con mi cara no": la vigilancia masiva a través del reconocimiento facial en Paraguay. Disponible en https://www.tedic.org/wp-content/uploads/2022/08/Fanzine-Biometria-web.pdf

9 AL SUR. 2021. Reconocimiento facial en América Latina: tendencias en implementación de una tecnología. Disponible en: https://www.alsur.lat/reporte/reconocimiento-facial-en-america-latina-tendencias-en-implementacion-una-tecnologia

10 GIJN. 2023. Guía para investigar amenazas digitales: panorama de cibervigilancia. Disponible en https://gijn.org/es/recurso/guia-para-periodistas-investigar-el-panorama-de-las-amenazas-digitales/

11 Comisión Europea. ¿Qué datos se consideran sensibles? Disponible en: https://commission.europa.eu/law/law-topic/data-protection/

El uso indebido de estas tecnologías puede derivar en violaciones significativas de derechos fundamentales. Según Romero Cerdán[12] (2019), el reconocimiento facial permite acceder a información sensible como el origen racial o el género de las personas, y su mala utilización puede conllevar discriminación y exclusión.

Además, estudios recientes resaltan la alta probabilidad de errores en las tecnologías de reconocimiento facial. Según la Red en Defensa de los Derechos Digitales[13] (2023), estas tecnologías han fallado repetidamente en identificar correctamente a las personas, lo que ha resultado en numerosos casos de detenciones injustas de individuos inocentes, erróneamente vinculados con delitos.

Este conjunto de problemas evidencia la necesidad urgente de regular el uso de estas tecnologías bajo estándares estrictos de protección de datos y derechos humanos, para evitar que se conviertan en herramientas de control y discriminación, en lugar de soluciones efectivas para la seguridad.

LA PRIVACIDAD Y LA VIGILANCIA MASIVA A TRAVÉS DE DATOS BIOMÉTRICOS

La privacidad permite a cada persona decidir cuánto comparte con los demás sobre sus pensamientos, sentimientos y aspectos de su vida personal. Es a través de este derecho que se crean espacios para resguardar lo que define a los seres humanos: sus vínculos familiares, amorosos y de amistad, relaciones profesionales, gustos, pensamientos y todo aquello que conforma la personalidad.

Como destaca Martin Scheinin, ex Relator Especial de la ONU[14] “Además de ser un derecho en sí mismo, la privacidad es la base de otros derechos, sin la cual estos no podrían ser efectivamente disfrutados”.

La vigilancia estatal es una potestad que permite a los gobiernos monitorear y supervisar las actividades de los ciudadanos con el fin de mantener el orden y la seguridad pública. Sin embargo, esta potestad está sujeta a estrictos requisitos legales y debe estar justificada por supuestos específicos y excepcionales. La vigilancia puede estar justificada en situaciones como la prevención de delitos graves, la protección de la seguridad nacional o la lucha contra el terrorismo. Para que esta vigilancia sea legítima, debe cumplir con principios de necesidad, proporcionalidad y legalidad[15].

12 Romero Cerdán, T. (2019). La autenticación y verificación de la identidad a través de información biométrica como paradigma del tratamiento de datos personales en México. Revista Del Posgrado.

13 R3D (2023). Las tecnologías de vigilancia masiva son autoritarias y no resuelven los problemas de seguridad pública. Disponible en: https://r3d.mx/2023/07/11/las-tecnologias-de-vigilancia-masiva-son-autoritarias-y-no-resuelven-los-problemas-de-seguridad-publica/

14 ONU. 2019. Informe del Relator Especial sobre la promoción y protección de los derechos humanos y las libertades fundamentales en la lucha contra el terrorismo, Martin Scheinin, 2009, P.10-11. Disponible en: http://www2.ohchr.org/english/bodies/hrcouncil/docs/13session/A-HRC-13-37.pdf

15 Electronic Frontier Foundation. Necessary and proportionate on the application of human rights to commmunications surveillance. Disponible en: https://necessaryandproportionate.org/

La limitación del derecho a la privacidad, en este contexto, debe ser cuidadosamente regulada para evitar abusos. La privacidad es un derecho fundamental, y su restricción solo puede ser aplicada cuando sea estrictamente necesaria y proporcionada al objetivo legítimo perseguido. Cualquier forma de vigilancia estatal debe estar respaldada por una base legal clara, contar con supervisión judicial y ser transparente para garantizar que no se vulneren los derechos individuales de forma desproporcionada.

Los tratados internacionales sobre derechos humanos establecen las condiciones bajo las cuales se pueden limitar estos derechos. La Declaración Universal de Derechos Humanos, en su artículo 29.2, y la Convención Americana de Derechos Humanos, en su artículo 30, indican que las restricciones deben ser impuestas por ley y únicamente para proteger los derechos de otros, la moral, el orden público y el bienestar general. Además, el Comentario General No. 27[16] del Comité de Derechos Humanos en 1999 proporcionó directrices sobre los parámetros que deben considerarse al imponer limitaciones a los derechos del Pacto Internacional de los Derechos Civiles y Políticos, orientando el análisis de políticas públicas en relación con estos derechos fundamentales.

Al referirse a las tecnologías que permiten la identificación masiva de personas, es fundamental considerar el impacto de la vigilancia en el ejercicio y disfrute de los derechos humanos, un fenómeno conocido como efecto disuasorio (chilling effects[17]). Las personas que creen que el gobierno monitorea sus mensajes tienden a autocensurarse, evitando escribir o discutir ciertos temas, incluidos asuntos políticos y sociales que podrían enriquecer el discurso público. Además, esta vigilancia limita el uso de las plataformas digitales como espacios para explorar nuevas identidades, posiciones y argumentos, restringiendo la libertad de expresión y el debate abierto.

En relación con la privacidad y el uso de tecnologías biométricas, es fundamental contar con un marco legislativo que proteja los datos personales antes de su implementación. La falta de estas normativas, que es muy común, tiene un impacto significativo en las libertades individuales desde una perspectiva social y ética (Privacy International, 2013).

El monitoreo masivo e indiscriminado mediante tecnologías biométricas y cámaras de reconocimiento facial socava la presunción de inocencia, convirtiendo a todas las personas en potenciales sospechosas bajo constante vigilancia. A diferencia del mundo offline, donde el monitoreo encubierto con fines delictivos requiere un proceso judicial y está regulado por tareas de inteligencia criminal, el uso de estas tecnologías permite una vigilancia permanente sin distinción ni justificación específica. En lugar del patrullaje visible y específico que realizan las fuerzas de seguridad, la vigilancia con reconocimiento facial actúa de manera oculta, sin identificaciones claras, lo que amplifica la sensación de control y amenaza el ejercicio de las libertades individuales. (Access Now, 2021).

16 Toda legislación o iniciativa que restrinja la libertad de expresión “debe ser accesible al público” y debe ser “formulada con suficiente precisión para permitir que un individuo regule su conducta en consecuencia”. Dicha legislación “no debe conferir discrecionalidad absoluta para restringir libertad de expresión a los encargados de su ejecución”. Además, cualquier restricción a la libertad de expresión “debe ajustarse a estrictos criterios de necesidad y proporcionalidad” (Comentario General N.º 34). Por último, las medidas restrictivas “deben ser el instrumento menos intrusivo entre aquellos que podrían lograr su función protectora; deben ser proporcionales al interés a ser protegido”. ONU – CCPR. 1999. Comentario general 27. Disponible en https://www.acnur.org/fileadmin/Documentos/BDL/2001/1400.pdf

17 PEN. 2022. Chilling Effects. NSA Surveillance drives US writers to self-censor. Disponible en: https://pen.org/wp-content/uploads/2022/08/2014-08-01_Full-Report_Chilling-Effects-w-Color-cover-UPDATED.pdf

Además, los Estados deben analizar la necesidad y proporcionalidad considerando si existen alternativas que impacten menos los derechos de las personas y que puedan alcanzar los mismos objetivos. La medida de instalación de cámaras biométricas busca prevenir cualquier tipo de ilícito en los espacios públicos, refleja una desproporción en cuanto al fin perseguido a la vez que deja de lado del principio de una intervención mínima a través del aparato punitivo del Estado, propio de lo que se denomina "derecho penal mínimo"[18].

Regulaciones internacionales que limitan el tratamiento biométrico

El impacto de la vigilancia masiva en la privacidad no solo afecta a nivel individual, sino que también entra en conflicto con los estándares establecidos por las normas internacionales de derechos humanos. Instrumentos como la Declaración Universal de Derechos Humanos, el Pacto Internacional de Derechos Civiles y Políticos y la Convención Americana de los Derechos humanos que reconocen la privacidad como un derecho fundamental que protege a las personas contra injerencias arbitrarias y abusivas en su vida privada.

Estas normativas subrayan la importancia de limitar la vigilancia estatal y otras formas de recopilación masiva de datos, garantizando que estas prácticas no socaven el goce pleno de derechos esenciales como la libertad de expresión, la asociación y el derecho a la vida privada. La Declaración Universal de los Derechos Humanos (ONU, 1948) en sus artículos 7 sobre igualdad ante la ley, 11 sobre presunción de inocencia, 12 sobre el derecho a la honra y dignidad, 13 sobre la libre circulación, 20 sobre la libertad de reunión y 30 sobre la indivisibilidad de los derechos, garantizan derechos fundamentales inherentes a toda persona que pueden verse comprometidos con la implementación de tecnologías de video vigilancia. De manera similar, el Pacto Internacional de Derechos Civiles y Políticos (PIDCP, 1966) protege el derecho a la privacidad y a la libertad de expresión en sus artículos 17 y 19, respectivamente, destacando la necesidad de salvaguardar estos derechos ante el avance de tecnologías invasivas. También se encuentran los instrumentos regionales en materia de Derechos Humanos como la Convención Americana de Derechos Humanos de la OEA reconocen los derechos a la libertad de opinión y de expresión, a la reunión, a la honra y dignidad[19], y disponen normas relativas a privacidad y libertad de expresión[20](OEA, 1969).

Además de estas normativas vigentes y vinculantes para Paraguay, las relatorías especiales de la ONU y la OEA han recomendado la imposición de moratorias o incluso la prohibición del uso de tecnologías de reconocimiento facial. Estas recomendaciones se deben a la falta de medidas de protección eficaces que garanticen el respeto de los derechos de las personas titulares de los datos, asegurando que su privacidad y otros derechos fundamentales no sean vulnerados.

18 Rolon y Sequera. 2015. Vigilancia de las comunicaciones en Paraguay. TEDIC. Disponible en: https://www.tedic.org/wp-content/uploads/2018/12/Vigilancia-estatal-de-las-comunicaciones-y-derechos-fundamentales-en-Paraguay.pdf En esta investigación se desarrolla el apartado sobre el derecho penal mínimo significa la reducción al mínimo de las circunstancias penales y su codificación general mediante la despenalización de todas aquellas conducta que no ofendan bienes fundamentales y que saturan el trabajo judicial con un dispendio inútil e inocuo de aquel recurso escaso y costoso que es la pena y tienen el triple efecto del debilitamiento general de las garantías, de la ineficacia de la maquinaria judicial y de la devaluación de los bienes jurídicos merecedores de tutela penal." Ferrajoli, Luigi. Crisis del sistema político y jurisdicción: la naturaleza de la crisis italiana y el rol de la magistratura. Revista Pena y Estado año 1 número 1–Argentina 1995: Editores del Puerto s.r.l. p. 113

19 Convención Americana de Derechos Humanos, artículos 11, 13 y 15.

20 Pacto Internacional de Derechos Civiles y Políticos, artículos 17 y 19.

Relacionados a la implementación de biometría, organismos internacionales de derechos humanos han expresado su preocupación por el uso indiscriminado de tecnologías biométricas. El Alto Comisionado de las Naciones Unidas para los Derechos Humanos ha señalado[21] la implementación de proyectos basados en datos biométricos sin las garantías legales necesarias y que solicita a los Estados a demostrar la necesidad y proporcionalidad de estos sistemas para fines legítimos antes de su implementación.

Expertos como Frank La Rue[22] y Navi Pillay[23], en sus roles como Relator Especial de la ONU y Alto Comisionado de la ONU para los Derechos Humanos respectivamente, han manifestado inquietud por las posibles violaciones al derecho a la privacidad debido al uso inadecuado de tecnologías biométricas. Estas preocupaciones subrayan la necesidad de una regulación más estricta y una protección más robusta de los datos personales.

Martin Scheinin, ex Relator Especial de la ONU[24], ha advertido sobre los riesgos específicos asociados con el almacenamiento centralizado de datos biométricos. Según su análisis, esta práctica no solo aumenta la vulnerabilidad de los individuos y compromete la seguridad de la información, sino que también podría llevar a un aumento significativo en las tasas de error a medida que se acumula más información biométrica en estas bases de datos centralizadas.

> "Los casos en que la biometría no se almacena en un documento de identidad, sino en una base de datos centralizada, incrementando los riesgos para la seguridad de la información y dejando a los individuos vulnerables. A medida que aumenta la información biométrica, las tasas de error pueden aumentar significativamente".

> "El incremento en las tasas de error puede llevar a la criminalización ilícita de individuos o a la exclusión social. A la vez, el Relator destaca un aspecto que mencionamos anteriormente, la irrevocabilidad de los datos biométricos".

> "(…) Una vez copiados y/o utilizados fraudulentamente por un actor malicioso, no es posible emitirle a un individuo una nueva firma [identidad] biométrica".

En junio de 2019, David Kaye, ex Relator Especial de la ONU[25] presentó ante el Consejo de Derechos Humanos la urgente necesidad de que los Estados impongan moratorias inmediatas al uso de tecnologías de vigilancia, incluido el reconocimiento facial, hasta que se establezcan regulaciones que respeten los derechos humanos y cuenten con amplias salvaguardas.

---

21 Asamblea General (ONU). 2018. El derecho a la privacidad en la era digital. Informe del Alto Comisionado de las Naciones Unidas para los Derechos Humanos. A/HRC/39/29. 2018. Disponible en: https://documents.un.org/doc/undoc/gen/g18/239/61/pdf/g1823961.pdf

22 ONU. 2013. Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue* A/HRC/23/40. ONU. Abril, 2013.

23 UN News Centre, 2013. UN rights chief urges protection for individuals revealing human rights violations. Disponible en: https://news.un.org/en/story/2013/07/444512

24 ONU. 2019. Informe del Relator Especial sobre la promoción y protección de los derechos humanos y las libertades fundamentales en la lucha contra el terrorismo, Martin Scheinin, 2009, P.10-11. Disponible en: http://www2.ohchr.org/english/bodies/hrcouncil/docs/13session/A-HRC-13-37.pdf

25 ONU. 2019. UN expert calls for immediate moratorium on the sale, transfer and use of surveillance tools. Disponible en: https://www.ohchr.org/en/press-releases/2019/06/un-expert-calls-immediate-moratorium-sale-transfer-and-use-surveillance?LangID=E&NewsID=24736

La Relatoría Especial para la Libertad de Expresión, en su informe anual correspondiente al año 2022, menciona el caso del metro de la ciudad de Sao Paulo, en el cual la Corte de Justicia del Estado de Sao Paulo rechazó la ejecución del sistema de captación y procesamiento de datos biométricos de los usuarios del metro de la ciudad para utilización en sistemas de reconocimiento facial dada su "potencialidad de afectar derechos fundamentales de los ciudadanos"[26].

El Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y expresión, en su informe sobre Vigilancia y Derechos Humanos, insistió en que los Estados debían adoptar medidas para impedir la comercialización de las tecnologías de vigilancia, haciendo especial énfasis en la atención a la investigación, el desarrollo, el comercio, la exportación y el uso de esas tecnologías, teniendo en cuenta su capacidad para facilitar la violación sistemática de los Derechos Humanos[27].

Por su parte, el Comité Jurídico Interamericano (CJI) de la Organización de Estados Americanos (OEA) redactó los Principios Actualizados de Privacidad y Protección de Datos Personales[28], los cuales en su totalidad deberían regir la utilización de estos equipos.

Entre los principios más importantes en materia de protección de datos personales, destacan los siguientes:

- **Finalidades legítimas y lealtad:** las imágenes captadas por los equipos de videovigilancia deben ser recolectadas únicamente para los fines debidamente establecidos en la ley, y por medios legales y legítimos, los cuales resulten de mínima intervención, proporcionales y no excedan los límites de la estricta necesidad.
- **Pertinencia y necesidad:** las imágenes recolectadas deben ser únicamente las que resulten pertinentes y adecuadas para los fines específicos de su recolección y tratamiento posterior, así como deben estar limitadas al mínimo necesario para ello.
- **Limitación del tratamiento y su conservación:** las imágenes recolectadas deberán ser tratadas y conservadas de acuerdo con su finalidad específica y por el tiempo necesario para el cumplimiento de dichos fines.
- **Seguridad de los datos:** los datos recolectados deben ser protegidos bajo criterios de confidencialidad, integridad y disponibilidad, mediante salvaguardias de seguridad a niveles técnico, administrativo e institucional razonables y adecuados contra tratamientos no autorizados o ilegítimos, incluyendo el acceso, pérdida, destrucción, daños o divulgación, aún cuando ocurran de manera accidental. Dichas medidas deben ser plenamente auditables en todos sus niveles y actualizadas permanentemente.

  Asimismo, los datos recolectados no deberán ser divulgados, puestos a disposición de terceros, ni emplearse para fines distintos a los que motivaron la recolección, salvo que la persona afectada preste su consentimiento para ello.

26 OEA, 2022. Informe anual de la Relatoría Especial para la Libertad de Expresión: Informe anual de la Comisión Interamericana de Derechos Humanos. Disponible en: https://www.oas.org/es/cidh/expresion/informes/IA2022ESP.pdf

27 ONU, 2019. La vigilancia y los derechos humanos. Informe del Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y de expresión. Disponible en: https://documents.un.org/doc/undoc/gen/g19/148/79/pdf/g1914879.pdf

28 OEA. 2021. Principios actualizados sobre la privacidad y protección de datos personales. Disponible en: https://www.oas.org/es/sla/cji/docs/Publicacion_Proteccion_Datos_Personales_Principios_Actualizados_2021.pdf

- Disponibilidad: los responsables del tratamiento de los datos deben disponer métodos razonables, ágiles, sencillos y eficaces para permitir que los titulares de los datos recolectados puedan solicitar el acceso a ellos, así como su rectificación y cancelación.

Se evidencia un esfuerzo creciente por establecer marcos legales que regulen el tratamiento de datos biométricos, especialmente en lo que respecta a la implementación del reconocimiento facial en espacios públicos y privados. No obstante, expertos en la materia advierten que las regulaciones centradas únicamente en la protección de datos personales son insuficientes para abordar los desafíos específicos que plantea la biometría. En el ámbito de la privacidad, aún faltan marcos teóricos y legislativos robustos que comprendan integralmente los riesgos asociados a estas tecnologías, tales como la vulnerabilidad a los abusos, la falta de consentimiento informado, y la posibilidad de vigilancia masiva y discriminación. La carencia de un enfoque normativo adecuado y especializado deja un vacío crítico que expone a las personas a riesgos significativos, subrayando la necesidad urgente de desarrollar regulaciones más detalladas y con salvaguardas efectivas para proteger los derechos fundamentales. (Díaz, 2018)

MARCHA ATRÁS EN EL USO DEL RECONOCIMIENTO FACIAL EN EL MUNDO

La tendencia de implementación de reconocimiento facial en los espacios públicos es mundial. A continuación compartiremos algunos antecedentes de países de occidente y los argumentos y discusiones que se están dando a nivel global para dar marcha atrás a la implementación del reconocimiento facial.

Buenos Aires, Argentina

Durante el 2023, un sistema de reconocimiento facial, ideado inicialmente para rastrear y capturar prófugos en la Ciudad Autónoma de Buenos Aires, fue centro de una gran controversia tras descubrirse que fue utilizado para monitorear a miles de personas que no figuraban en el listado oficial de prófugos, incluyendo a jueces, figuras públicas y líderes de derechos humanos, generando acusaciones de espionaje y abuso de poder[29]. Tras numerosas medidas judiciales desde la sociedad civil, su implementación se declaró inconstitucional y se abrieron investigaciones judiciales[30].

Además, la imprecisión del sistema condujo a detenciones irregulares y potencialmente injustas por parte de la Policía de la Ciudad. Los falsos positivos y la falta de controles adecuados sobre el uso del sistema plantearon serias dudas sobre la protección de los derechos civiles y la seguridad jurídica en Argentina que hasta hoy siguen siendo ejemplo de las amenazas que pudieran suscitar a la democracia.

El uso de datos biométricos en cámaras de video vigilancia, particularmente por el avance del reconocimiento facial, se encuentra en la mira ante la creciente preocupación de poblaciones, gobiernos y organismos especializados.

29 R3D: Red en Defensa de los Derechos Digitales. 2023. Gobierno de Buenos Aires solicitó datos biométricos de más de 200 jueces y fiscales sin justificación. Disponible https://r3d.mx/2023/05/22/gobierno-de-buenos-aires-solicito-datos-biometricos-de-mas-de-200-jueces-y-fiscales-sin-justificacion/

30 CELS. 2022. Uso ilegal del sistema de reconocimiento facial en CABA: A pedido del gobierno de la Ciudad, el TSJ sacó al juez de la causa. Disponible en: https://www.cels.or$ar/web/2022/07/uso-ilegal-del-sistema-de-reconocimiento-facial-en-caba-a-pedido-del-gobierno-de-la-ciudad-el-tsj-saco-al-juez-de-la-causa/

Otros casos se vienen documentando a nivel global como se puede ver en el Informe “Te están mirando, publicado por organizaciones que pertenecen a la International Network of Civil Liberties Organizations (INCLO), quienes analizaron como de diversas maneras, el uso de Sistemas de Reconocimiento Facial (SRF) afectaron las vidas de la población en 13 países de las Américas, África, Europa, Asia y Australia. (International Network of Civil Liberties Organizations, 2021).

Las evidencias sobre la gravedad de implementar tecnologías de vigilancia sin evaluaciones de impacto de derechos humanos o con implementaciones entre lagunas legales, impulsan una industria inhumana, oscura y con cuestionables aplicaciones, que reproducen discriminaciones, sesgos e incluso, prácticas antidemocráticas y corruptas de forma masiva.

La cadena de corrupción ligada a la expansión de esta industria se entreteje con varios componentes: las compras públicas dirigidas o manipuladas, el avance de vulneraciones al sistema garantista penal, la tecnificación de instrumentos de persecución ideológica-política y el uso abusivo de datos personales, incluso considerables sensibles.

Incluso su posible regulación hoy está en la mira global a consecuencias de las dificultades que generaría, siendo una descripción interesante la ofrecida por Carmen-Nicole Cox, directora de asuntos gubernamentales de ACLU California Action: “Regular la vigilancia facial es como tratar de bloquear una bala de cañón con cartón” en pleno contexto de disolución en pos de avanzar en la regulación del asunto en California, Estados Unidos (Holden, 2023).

La discusión está cada día más presente. A continuación hacemos un recuento de hechos relevantes ocurridos alrededor del globo entre el 2022 y 2023:

San Paulo, Brasil

El 18 de mayo de 2023, el Tribunal de Justicia de São Paulo suspendió un llamado a licitación de 20.000 cámaras con reconocimiento facial, tras una acción civil impulsada por la Concejal Silvia Ferraro de la Bancada Feminista del PSOL, integrante de la Cámara Municipal del ayuntamiento[31].

En la sentencia el juez Luis Manuel Fonseca Pires señaló serias preocupaciones de violación masiva a derechos fundamentales, destacando particularmente el riesgo de reproducir discriminación social y racismo estructural sin que existan mecanismos de revisión de estos comportamientos[32]. En la sentencia citó a la Red de Observatorios de Seguridad, la cual indica que “el 90 por ciento de los arrestos realizados en Brasil mediante esta tecnología (datos recopilados en 2019) fueron de personas negras, y entre ellos hubo errores de identificación que llevaron a la detención de inocentes”.

Aún así, el falló fue apelado por la prefectura del Estado consiguiendo una revocación en Cámara, programando la subasta[33].

31 Agencia Brasil. 2023. TJ suspende compra de cámaras con reconocimiento facial en SP. Disponible en: https://agenciabrasil.ebc.com.br/saude/noticia/2023-05/tj-suspende-compra-de-cameras-com-reconhecimento-facial-em-sp

32 Tribunal de Justicia Do Estado de Sao Paulo. 2023 Decisión – Mandado. Disponible en: https://www.migalhas.com.br/arquivos/2023/5/02F4930DEF8E75_decisao-smart-sampa.pdf

33 Agencia Brasil. 2023. Sao Paulo tendrá cámaras de conocimiento facial. Disponible en: https://agenciabrasil.ebc.com.br/es/justica/noticia/2023-05/justicia-lanza-edicto-de-camaras-con-reconocimiento-facial-en-sp

Este caso se suma a muchos otros sucesos recientes, cómo la suspensión de un llamado desde el Concejo Municipal, la prohibición judicial del sistema de reconocimiento facial en el metro de Sao Paulo tras una acción legal impulsada por Defensoría Pública del Estado de São Paulo, la Defensoría Pública Federal, el Instituto Brasileño de Protección al Consumidor (Idec), Intervozes – Colectivo Brasil de Comunicação, y Artigo 19 Brasil[34].

Estrasburgo, Francia

En julio del 2023 el Tribunal Europeo de Derechos Humanos (ECHR) determinó que Rusia violó los derechos a la privacidad, vida familiar y libertad de expresión del manifestante Nikolay Glukhin[35] al utilizar tecnología de reconocimiento facial para identificarlo tras una protesta pacífica en solitario en Moscú[36].

Según Glukhin, la policía usó videos y fotos de su protesta en redes sociales, junto con imágenes del sistema de video vigilancia del metro de Moscú, para identificarlo y arrestarlo. Fue multado por protestar sin notificar a las autoridades previamente.

Aunque Rusia aseguró que Glukhin violó leyes sobre protestas, el ECHR encontró que el uso de reconocimiento facial fue desproporcionado e incompatible con una sociedad democrática, dado que la protesta fue pacífica y no representó peligro. El Tribunal señaló que no había otra forma en que la policía hubiera podido identificarlo tan rápidamente.

Organizaciones celebraron el fallo, advirtiendo que el reconocimiento facial amenaza derechos como la libertad de expresión y protesta pacífica.

Unión Europea

La Unión Europea aprobó el Reglamento Europeo sobre Inteligencia Artificial (IA)[37], que entró en vigor el 1 de agosto de 2024. Este reglamento busca establecer un marco normativo para el uso de esta tecnología, reconociendo algunos de sus riesgos[38]. Sin embargo, permite que gobiernos y empresas privadas utilicen sistemas de reconocimiento facial de forma masiva, tanto en tiempo real (captura e identificación inmediata de rostros) como de manera retrospectiva (identificación de rostros en grabaciones previas).

En 2023, Amnistía Internacional advirtió que la Unión Europea subestima los riesgos del reconocimiento facial retrospectivo al argumentar que su uso diferido permite mitigar problemas potenciales. Esta postura, según la organización, ignora aspectos críticos como la desanonimización y la supresión de derechos fundamentales. Además, el mero conocimiento de que estas tecnologías

34 DPL News. 2022. Metro de Sao Paulo tiene prohibido utilizar sistema de reconocimiento facial. Disponible en: https://dplnews.com/metro-de-sao-paulo-tiene-prohibido-utilizar-sistema-de-reconocimiento-facial/

35 HUDOC- European Court of Human Rights. 2023. Use of facial-recongnition technology breached rights of Moscow underground protestor. Disponible en: https://hudoc.echr.coe.int/app/conversion/pdf/?library=ECHR&id=003-7694109-10618091&filename=Judgment%20Glukhin%20v.%20Russia%20-%20use%20of%20facial-recognition%20technology%20against%20Moscow%20underground%20protestor.pdf

36 R3D. 2023 Tribunal europea de Derechos humanos falla contra el uso de reconocimiento facial para identificar manifestante ruso. Disponible en: https://r3d.mx/2023/07/05/tribunal-europeo-de-derechos-humanos-falla-contra-el-uso-de-reconocimiento-facial-para-identificar-manifestante-ruso/

37 Europarl. 2024. La Eurocámara aprueba una ley histórica para regular la inteligencia artificial. Disponible en: https://www.europarl.europa.eu/news/es/press-room/20240308IPR19015/la-eurocamara-aprueba-una-ley-historica-para-regular-la-inteligencia-artificial

38 Comisión Europea. 2024. El reglamento de AI entra en vigor. Disponible en: https://commission.europa.eu/news/ai-act-enters-force-2024-08-01_es

pueden aplicarse en cualquier momento genera un efecto amedrentador[39] sobre las personas, limitando su libertad de expresión y movimiento.

Ante los abusos y desigualdades que implica el uso de estas tecnologías, Amnistía Internacional ha instado a la prohibición total de la vigilancia biométrica masiva. La Ley de IA representa una oportunidad clave para garantizar la protección de los derechos humanos y evitar que estas herramientas se conviertan en mecanismos de control y opresión.

Cambridge, Reino Unido

Un nuevo informe del Centro Minderoo para Tecnología y Democracia de la Universidad de Cambridge califica de "poco ético" y posiblemente ilegal el uso policial del reconocimiento facial en vivo en el Reino Unido[40]. Esta tecnología compara rostros vistos en cámaras de CCTV en tiempo real con listas de vigilancia de delincuentes buscados. Cuando hay coincidencia, se alerta a la policía.

El informe creó estándares éticos mínimos que debería cumplir esta tecnología. Ningún caso de uso policial en el Reino Unido pasó la prueba. No demostraron que sea efectiva ni segura, y no cumplen con requisitos de privacidad, derechos humanos y supervisión.

Los investigadores pidieron detener el uso policial de esta tecnología hasta no demostrar beneficios y minimizar riesgos. La Policía Metropolitana defendió la legalidad de su uso, pero expertos advierten que las leyes actuales no alcanzan para regular y limitar estos sistemas invasivos.

Estados Unidos

La presión existente en el país norteamericano llevó a que lugares como Massachusetts[41], Austin y San Francisco[42], el uso de reconocimiento facial haya sido prohibido[43] por las fuerzas policiales y entidades gubernamentales. Por otro lado, Nueva York y Portland, Oregon, son algunas de las ciudades en el país que han establecido restricciones sobre el uso de tecnología de reconocimiento facial en el sector privado[44]. Sin embargo, se profundizaron las discusiones con prósperos avances en la garantización de libertades civiles, tal como veremos a continuación.

En el 2023, varios senadores y representantes de Estados Unidos, incluyendo a figuras destacadas como Edward J. Markey, Bernie Sanders y Elizabeth Warren, han reintroducido la "Ley de Moratoria de Reconocimiento Facial y Tecnología Biométrica"[45]. Esta legislación busca prohibir que el gobierno utilice tecnologías de reconocimiento facial y otras soluciones biométricas, argumentando que

39 Amnistía Internacional. 2023. La vigilancia mediante reconocmiento facial restrospectivo oculta abusos contra los derechos humanos. Disponible en: https://www.es.amnesty.org/en-que-estamos/blog/historia/articulo/la-vigilancia-mediante-reconocimiento-facial-retrospectivo-oculta-abusos-contra-los-derechos-humanos/

40 Tech Monitor30. 2022. Police use of live facial recognition "unethical" and possibly illegal. Disponible en: https://techmonitor.ai/technology/ai-and-automation/police-facial-recognition-live-unethical

41 R3D. 2023. Massachusetts discute ley para restringir el uso policial de reconocimiento facial. Disponible en: https://r3d.mx/2023/08/04/massachusetts-discute-ley-para-restringir-el-uso-policial-del-reconocimiento-facial/

42 Washington Post. 2024. San Francisco become first city us ban facial recognition software. Disponible en: https://www.washingtonpost.com/technology/2019/05/14/san-francisco-becomes-first-city-us-ban-facial-recognition-software/

43 Washington Post. 2024. These cities bar facial recognition tech. Police still found ways to access it. Disponible en: https://www.washingtonpost.com/business/2024/05/18/facial-recognition-law-enforcement-austin-san-francisco/

44 Washington, Oregon, California, Colorado, and Alabama all have limited government actor or police use. Up to date information about state regulation of facial recognition technology can be found at. Disponible en: www.banfacialrecognition.com/map/.

45 Congress. GOV. 2023. H.R.1404 - Facial Recognition and Biometric Technology Moratorium Act of 2023. Disponible en: https://www.congress.gov/bill/118th-congress/house-bill/1404

estas herramientas presentan serios problemas de privacidad, libertades civiles y afectan desproporcionadamente a comunidades marginadas. Estas preocupaciones se han intensificado tras informes de que el reconocimiento facial ha llevado a arrestos injustos, especialmente de hombres negros, y que casi la mitad de los rostros de adultos en EE.UU. están en bases de datos de este tipo[46].

Las declaraciones de los legisladores enfatizan el peligro que estas tecnologías representan para la democracia y la privacidad de la ciudadanía. El senador Markey destacó que "la recopilación de datos biométricos plantea graves riesgos de invasión de la privacidad y discriminación". Por su parte, el representante Jayapal señaló que la tecnología de reconocimiento facial no solo es invasiva y errónea, sino que ha sido usada en contra de comunidades de color. La propuesta legislativa establece, entre otros puntos, una prohibición sobre el uso de tecnología de reconocimiento facial y otras tecnologías biométricas por parte de entidades federales, y condiciones para la entrega de fondos federales a entidades estatales y locales. Además, busca prohibir el uso de información recopilada por tecnología biométrica en procedimientos judiciales y otorga derechos de acción privada para personas afectadas[47].

La "Ley de Moratoria de Reconocimiento Facial y Tecnología Biométrica" ha recibido el respaldo de diversas organizaciones, entre las que se encuentran la ACLU, EPIC y la Electronic Frontier Foundation[48]. Estas entidades han destacado la importancia de proteger los derechos civiles y garantizar la privacidad de los ciudadanos frente a la creciente adopción de tecnologías de vigilancia.

Por otro lado, las organizaciones defensoras de los derechos de los migrantes han expresado preocupación ante las deficiencias de la nueva aplicación móvil lanzada por el gobierno de EE.UU. para procesar solicitudes de asilo en la frontera con México. Esta herramienta, denominada CBP One, utiliza tecnología de reconocimiento facial que ha demostrado tener sesgos, especialmente al intentar identificar a personas de piel oscura. El impacto ha sido particularmente notable entre los migrantes de Haití y países africanos, quienes enfrentan constantes errores al intentar ingresar sus datos y fotografías en la aplicación.

Además del evidente sesgo racial en la tecnología de reconocimiento facial, muchos solicitantes de asilo enfrentan otros obstáculos, como la falta de dispositivos móviles compatibles o un acceso limitado a Internet. En respuesta a estos desafíos, algunas organizaciones sin fines de lucro han implementado soluciones creativas, como usar luces brillantes al tomar fotografías para la aplicación, con el objetivo de mejorar el registro de las características faciales. Sin embargo, estas soluciones no son universales y, en particular, no han sido efectivas para niños menores de seis años. A pesar de las constantes consultas y preocupaciones presentadas, la Oficina de Aduanas y Protección Fronteriza (CBP) ha permanecido en silencio sin ofrecer soluciones o comentarios al respecto[49].

46 NextGov. Fcw. 2023. Lawmakers Intro Bill to Ban Government Use of Facial Recognition. Disponible en: https://www.nextgov.com/digital-government/2023/03/lawmakers-intro-bill-ban-government-use-facial-recognition/383691/

47 ED Marley. 2022. Senators Markey and Merkley, and Reps. Jayapal, Pressley to Introduce Legislation to Ban Government Use of Facial Recognition, Other Biometric Technology Disponible en: https://www.markey.senate.gov/news/press-releases/senators-markey-and-merkley-and-reps-jayapal-pressley-to-introduce-legislation-to-ban-government-use-of-facial-recognition-other-biometric-technology

48 EFF. 2020. Facial Recognition and Biometric Technology Moratorium Act of 2020. Disponible en: https://www.eff.org/my/document/facial-recognition-and-biometric-technology-moratorium-act-2020

49 The Guardian. 2023. Facial recognition bias frustrates Black asylum applicants to US, advocates say. Disponible: https://www.theguardian.com/us-news/2023/feb/08/us-immigration-cbp-one-app-facial-recognition-bias

Dos proyectos de ley han sido propuestos por miembros del Consejo Municipal de Nueva York para restringir el uso de tecnología de reconocimiento facial por parte de empresas y edificios residenciales, evitando su uso para identificar a clientes o inquilinos sin su consentimiento[50].

El primer proyecto, patrocinado por los concejales Shahana K. Hanif y Jennifer Gutiérrez, busca prohibir a negocios privados, incluidos estadios y auditorios públicos, el uso de información biométrica para identificar o verificar a un cliente. Si deciden recopilar esta información, deberán notificar y obtener el consentimiento escrito del cliente, y se les prohibirá compartir o almacenar dicha información.

Por otro lado, un segundo proyecto, se centra en edificios residenciales, buscando prohibir a los propietarios el uso de tecnologías de reconocimiento biométrico que identifiquen a inquilinos o sus invitados. Estas medidas surgen en un contexto en el que se descubrió que Madison Square Garden, bajo el propietario James Dolan, usaba esta tecnología, lo que generó controversia y posibles sanciones legales.

En una reciente discusión en el concejo municipal, el concejal Kristerfer Burnett, conocido por su compromiso con los derechos civiles y la privacidad, presentó dos proyectos de ley relacionados con la tecnología de reconocimiento facial[51]. Su propuesta surge en respuesta a las presiones tanto a nivel nacional como regional de organizaciones de la sociedad civil preocupadas por la privacidad y las libertades civiles.

El primer proyecto de Burnett busca establecer una comisión asesora comunitaria sobre vigilancia. Esta comisión requeriría la aprobación del concejo municipal antes que el Departamento de Policía de Baltimore pueda adquirir equipos de vigilancia. El segundo proyecto se centra en establecer regulaciones claras sobre el uso de la tecnología de reconocimiento facial, así como en la recuperación, retención y destrucción de datos.

Burnett muestra especial preocupación por las libertades civiles y la privacidad, particularmente en lo que respecta a las comunidades marginadas, que han enfrentado históricamente prácticas policiales y de vigilancia discriminatorias. El concejal enfatiza la necesidad de equilibrar la seguridad pública con la protección de la privacidad[52].

En ese contexto, en relación a los casos que se dan a nivel global, también se puede hacer referencia a las empresas de vigilancia, marcas de equipos y derechos humanos, para analizar si existen cuestionamientos a los productos que ofrecen o sus métodos de trabajo. Aquí compartimos una lista de nombres de empresas que ofrecen a los países este tipo de tecnología.

50 BiometricUpdate. 2024. Bills to ban facial recognition spark lively debate in New York council. Disponible en: https://www.biometricupdate.com/202406/bills-to-ban-facial-recognition-spark-lively-debate-in-new-york-council

51 The Baltimor Banner. 2023. Proposals to regulate facial recognition could be 'test case' for Baltimore's authority over its police. Disponible en: https://www.thebaltimorebanner.com/politics-power/local-government/proposals-to-curb-facial-recognition-could-test-baltimore-authority-over-police-WMHCJLZFNBC55J7BFY2G2GGWFI/

52 WYPR. 2021. Burnett Seeks Regulation Of Facial Recognition Technology In Baltimore. Disponible en: https://www.wypr.org/wypr-news/2021-02-25/burnett-seeks-regulation-of-facial-recognition-technology-in-baltimore

TABLA 4. Lista de empresas proveedoras de cámaras de reconocimiento facial en el mundo[53,54]

Hikvision
Senken
QNAP
Avigilon
Sony
Intelligent Security Systems (ISS)
Cellebrite
ZTE
NEC
Dahua
Huawei
Verint

Al respecto cabe señalar que existen cuestionamientos hacia algunas empresas, como Hikvision, según un artículo escrito[55] por el especialista en sistemas de seguridad Felipe Arguello. El nombre de esta empresa se puede observar reiteradamente entre las compras hechas por el Estado norteamericano en relación a cámaras de circuito cerrado.

La marca Hikvision, fue incluida en la lista negra del gobierno norteamericano, bajo el argumento de que incurrió en violaciones de derechos humanos en la provincia de Xinjiang, China, dirigidas contra minorías musulmanas, según el especialista Arguello y el medio internacional El Tiempo[56].

Un hecho similar ocurrió con la marca Intelligent Security Systems (ISS) en Brasil, que presenta sesgos raciales, según Investigadores[57] de la Universidad Federal de Paraná y la Pontificia Universidad Católica (PUC-PR) que realizaron un estudio sobre el uso de reconocimiento facial en escuelas de Paraná[58].

El informe destaca debilidades en la vigilancia, incumplimientos de la Ley de Protección de Datos

53 En el marco del análisis de las empresas que se encuentran en la lista de compras hechas por las instituciones estatales en Paraguay, podemos encontrar una serie de nombres, como señala la Tabla 4.

54 Esta lista se encuentran identificadas en las siguientes investigaciones:

1. Access. 2021. Disponible en:https://www.accessnow.org/wp-content/uploads/2021/09/vigilancia-latam-espa.pdf

2. AL SUR. 2021. Reconocimiento facial en América Latina. https://www.alsur.lat/sites/default/files/2021-11/ALSUR_Reconocimiento_facial_en_Latam_ES.pdf

55 Infotecnico. 2018 Disponible en: https://www.infoteknico.com/mas-sanciones-contra-dahua-y-hikvision/

56 El tiempo. 2019. EE. UU. pone en su lista negra a Hikvision por violación de derechos Disponible en: https://www.eltiempo.com/tecnosfera/novedades-tecnologia/administracion-trump-pone-a-hikvision-en-la-lista-negra-de-estados-unidos-420674

57 APP Sindicato. 2023. Distopia: pesquisadores(as) da UFPR e da PUC denunciam “monitoramento de emoções” nas escolas estaduais. Disponible en: https://appsindicato.orģbr/distopia-pesquisadoresas-da-ufpr-e-da-puc-denunciam-monitoramento-de-emocoes-nas-escolas-estaduais/

58 La ISS es uno de los software que usa la Policía Nacional paraguaya y que lo documentamos más abajo.

y cuestiona la eficacia de la inteligencia artificial para monitorear el comportamiento estudiantil. Celepar, empresa pública de tecnologías de la información de Brasil, en colaboración con la PUC-PR, realizó pruebas de biometría facial y monitoreo externo con el software de ISS y concluyó acerca de la existencia de sesgos étnicos en los sistemas de reconocimiento facial, por lo que destacó el riesgo de reproducir discriminación social.

LOS DERECHOS HUMANOS Y LA VIGILANCIA A TRAVÉS DE CÁMARAS DE RECONOCIMIENTO FACIAL EN PARAGUAY

Como se destacó en la sección sobre derechos humanos a nivel internacional, Paraguay está comprometido con la protección de estos derechos, y los instrumentos internacionales son vinculantes en su territorio. Aunque no existen normativas específicas que regulen el tratamiento sobre biometría a nivel local, estas obligaciones internacionales deben considerarse al implementar o debatir sobre el uso de tecnologías biométricas. Es fundamental que cualquier discusión o implementación de tales tecnologías se alinee con los estándares de protección de derechos humanos establecidos en estos marcos legales, para asegurar que se respeten los derechos fundamentales de las personas.

La vigilancia estatal es una potestad limitada que debe estar justificada por razones específicas, como la prevención de delitos graves o la protección de la seguridad nacional. Para ser legítima, debe cumplir con principios de necesidad, proporcionalidad y legalidad, y la limitación del derecho a la privacidad debe ser estricta y proporcional al objetivo perseguido. Esta vigilancia requiere una base legal clara, supervisión judicial y transparencia para evitar abusos y proteger los derechos individuales. (EFF, s.f)

A continuación se describen las normas que aplican para limitar la vigilancia de las comunicaciones que se complementan con las normativas internacionales. En primer lugar se encuentra la Constitución Nacional reconoce en su artículo Nº 33 al Derecho a la Intimidad, el cual dispone:

> "La intimidad personal y familiar, así como el respeto a la vida privada, son inviolables. La conducta de las personas, en tanto no afecte al orden público establecido en la ley o a los derechos de terceros, estará exenta de la autoridad pública. Se garantizan el derecho a la protección de la intimidad, de la dignidad y de la imagen privada de las personas".

Asimismo, el mismo cuerpo legal reconoce en su artículo Nº 25 el Derecho a la Expresión de la Personalidad, y establece:

> "Toda persona tiene el derecho a la libre expresión de su personalidad, a la creatividad y a la formación de su propia identidad. Se garantiza el pluralismo ideológico".

En materia de protección de datos, la Constitución Nacional establece la figura del Habeas Data como la institución jurídica correspondiente para el acceso a la información[59] y a los datos relativos a sí mismo o a sus bienes que obren en registros oficiales o privados de carácter público, el

59 Paciello y Guerrero. 2022. Habeas data y afiliaciones fraudulentas por uso indebido de datos. TEDIC. Disponible en: https://www.tedic.org/wp-content/uploads/2022/10/Habeas-data-y-afiliaciones-fraudulentas-WEB.pdf

conocimiento del uso que se haga de los mismos y la finalidad de su tratamiento. De igual manera, establece el mecanismo jurisdiccional correspondiente para solicitar la actualización, rectificación o destrucción de dichos datos en caso de que fueran erróneos o afectaran ilegítimamente sus derechos[60].

En Paraguay, aunque no existen normas específicas que establezcan estándares mínimos para la protección de datos personales, incluyendo su recolección, tratamiento y procesos de anonimización o eliminación, el ordenamiento jurídico vigente contempla disposiciones generales de protección.

Por su parte, la Ley Nº 4868/2013 de Comercio Electrónico establece en su artículo Nº 6 que:

> "En ningún caso la actividad comercial de los Proveedores podrá vulnerar: (...) e) la protección de los datos personales y los derechos a la intimidad personal y familiar de las partes o los terceros intervinientes; y, f) la confidencialidad de los registros y cuentas bancarias".

No obstante, es importante mencionar el proyecto de ley de Protección Integral de Datos Personales presentado por varios diputados nacionales[61], con apoyo de la Coalición de Datos Personales de Paraguay[62]. Esta propuesta tiene por objeto establecer disposiciones precisas y detalladas, modernas, que garanticen el respeto a los derechos y garantías reconocidos y garantizados por la Constitución Nacional, alineados con los estándares globales que rigen la materia, que brinden seguridad jurídica tanto a los ciudadanos como a los responsables del tratamiento de los datos.

Este proyecto de ley busca crear una agencia estatal de protección de datos, la cual estaría a cargo de la supervisión y ejecución de las disposiciones legales establecidas en el proyecto mencionado, así como la asistencia técnica a los responsables del tratamiento de los datos y a la ciudadanía en general acerca de su aplicación.

El vacío normativo existente en el ordenamiento jurídico local se configura a partir de la falta de especificación de los parámetros de razonabilidad y proporcionalidad en la captación, procesamiento y almacenamiento de las imágenes captadas por los equipos con tecnología de reconocimiento facial.

---

60 Acuña, Alonzo y Sequera. 2017. La protección de datos personales en bases de datos públicas en Paraguay. TEDIC Disponible en: https://www.tedic.org/la-proteccion-de-datos-personales-en-bases-de-datos-publicas-en-paraguay/

61 Congreso Nacional. 2021. Proyecto de ley de protección integral de datos personales. Disponible en: https://silpy.congreso.gov.py/web/expediente/115707

62 Coalición de datos personales. 2024. Última versión del proyecto de ley de datos personales en Paraguay: Un trabajo colectivo y participativo. Disponible en: https://www.datospersonales.orǧpy/ultima-version-del-proyecto-de-ley-de-datos-personales-en-paraguay-un-trabajo-colectivo-y-participativo/

Esta versión es la tercera versión y última entregada por los miembros de la Coalición. Link del SILPY https://silpy.congreso.gov.py/web/descarga/dictamencomision-440780?preview

Por otro lado, la ley 6534/20 de protección de datos personales crediticios, normativa que solo aborda cuando se trata para los fines de créditos de las personas, define en su artículo 3 (Inc a y b) lo que entiende por datos personales y datos personales sensibles:

- **Datos Personales:** Información de cualquier tipo, referida a personas jurídicas o personas físicas determinadas o determinables. Se entenderá por determinable la persona que pueda ser identificada mediante algún identificador o por uno o varios elementos característicos de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona. Los derechos y garantías de protección de datos personales serán extendidos a personas jurídicas en cuanto le sean aplicables.
- **Datos personales sensibles:** Aquellos que se refieran a la esfera íntima de su titular, o cuya utilización indebida puedan dar origen a discriminación o conlleve un riesgo grave para éste. Se consideran sensibles los datos personales que puedan revelar aspectos como origen racial o étnico; creencias o convicciones religiosas, filosóficas y morales; afiliación sindical; opiniones políticas; datos relativos a la salud, a la vida, preferencia u orientación sexual, datos genéticos o datos biométricos dirigidos a identificar de manera unívoca a una persona física.

Sin embargo esta ley no ofrece garantías ni orientaciones para su tratamiento, solo lo define y luego se enfoca exclusivamente a los tratamientos crediticios. Esto se espera subsanar con la futura ley que se encuentra en el Congreso Nacional sobre la protección integral de los datos personales.

Como podemos observar, en las disposiciones normativas vigentes está ausente la determinación de la responsabilidad relativa al funcionamiento de los equipos con tecnología de reconocimiento facial. Estos incluyen: el funcionamiento de los equipos, su operación, mantenimiento, reparación en caso de fallas o daños, el tratamiento de los datos recolectados, la seguridad de los datos y la integridad tanto de los funcionarios intervinientes como de la institución ante la mala utilización de los equipos y los datos personales recolectados.

Este aspecto es crucial, ya que los equipos son adquiridos con fondos provenientes de municipalidades, gobernaciones y otras instituciones estatales ajenas a la Policía Nacional. Esto plantea interrogantes clave sobre la titularidad de dichos equipos y la legalidad del uso de estos fondos para los fines mencionados.

La experiencia a nivel mundial demuestra que aún con disposiciones legales y jurídicas claras, los abusos son cometidos con frecuencia, lo cual permite suponer que el vacío normativo no sólo propiciaría los abusos sino que llevaría inclusive a una normalización de los abusos bajo el argumento de “seguridad nacional”.

La vigilancia masiva cómo amenaza al orden democrático

Durante las manifestaciones ocurridas en marzo del 2021, cuando miles de manifestantes salieron a las calles desesperados por la crisis sanitaria sufrida a causa de la pandemia del COVID-19, desde la Policía Nacional se reconoció que estaban realizando perfilamientos de personas por medio de cámaras de video vigilancia en vía pública, con discrecionalidad y presuntamente, sin orden judicial:

- La jefa de Relaciones Públicas de la Policía, María Elena Andrada, informó que se ha hecho un recorrido con las grabaciones de las cámaras del Sistema 911 en cada día de protestas y se ha logrado identificar a “un mismo grupo de personas que participa en todos los días con incidentes.

- Nota en IP Paraguay (IP 2021). “Policía tiene identificadas a personas que cometieron desmanes mediante el Sistema 911”. 9 de marzo de 2021.
- Esta situación quedó aún más expuesta cuando el ministro del Interior de ese periodo, Arnaldo Giuzzio, solicitó en las mismas fechas implementar más cámaras de vigilancia masiva en vía pública con recursos del FSU (CONATEL, 2021).

Paraguay no es un país en el que la Policía Nacional se caracterice por ser la institución que más respeta los Derechos Humanos sino que su funcionamiento sigue muy marcado por prácticas heredadas de la dictadura de Stroessner (CODEHUPY, 2022). Son numerosas las denuncias ciudadanas contra la Policía Nacional por los excesos en los que incurrieron contra manifestantes, las cuales fueron difundidas por los medios de prensa locales, tanto de los efectivos comunes como de los pertenecientes al denominado Grupo Lince.

Llevando estos abusos materiales al plano de los datos biométricos y el uso de tecnología con reconocimiento facial, no sería una sorpresa que éstos sean utilizados con fines de espionaje y/o seguimiento a la ciudadanía pertenecientes a partidos y organizaciones políticas de oposición, activistas sociales, o simples ciudadanos comunes que manifiestan abiertamente su descontento con el Gobierno o algún funcionario específico de él.

Esta situación, además de vulnerar los derechos antes mencionados, generaría una criminalización de la lucha social y del derecho a la manifestación, lo cual podría verse traducido en una vigilancia masiva y clandestina de la ciudadanía, cuya calificación de su comportamiento estaría sometida a la mera voluntad de un operador, sin las más mínimas garantías jurídicas ni legales que permitan hacer efectivos los derechos que le asisten.

Ahora bien, el vacío legal y la insuficiencia jurídica, conceptual y normativa de la cual adolecen las normas mencionadas no se ve limitada solo a la cuestión operativa y tecnológica, sino también en lo relativo a la naturaleza propiamente dicha del Sistema 911.

Por otra parte, en cuanto al manejo de los datos personales y privados, la policía Policía Nacional utiliza reiteradamente refiere que no puede otorgar la información, solicitada a través de la Ley de Acceso a la Información Pública, sobre las cámaras de reconocimiento facial, argumentando que se tratan de información sensible (TEDIC, 2019).

No obstante, contradictoriamente a dichas afirmaciones de la fuerza de seguridad estatal, la falta de una ley de protección de datos personales y una mejor gestión de la información personal de la ciudadanía, se puso en evidencia justamente luego de que se filtre ese tipo de información, lo cual también fue documentado por TEDIC a través del artículo “La filtración de datos policiales en Paraguay y una imperante urgencia de respuestas” (TEDIC, 2023).

El artículo detalló que esta filtración de datos no solo consistió en números de documentos de identidad, sino además, de datos biométricos, con más de cuatro millones de recortes de imágenes faciales captadas por cámaras.

El hecho de que esto haya ocurrido, genera cuestionamientos sobre cómo se puede estar utilizando este tipo de tecnología. En ese contexto, para Amnistía Internacional España[63]:

> "La identificación biométrica remota 'en diferido' es posiblemente la medida de vigilancia más peligrosa de la que hayamos oído hablar".

Ante la posibilidad de que situaciones similares, como la mencionada filtración de datos vuelvan a ocurrir, deja entrever la necesidad de que haya normativas claras y mayor apertura del Estado Paraguayo a la transparencia en la materia. Los archivos filtrados, documentados por TEDIC, contenían información relacionada con niños, niñas y adolescentes, personas con identidad de género disidentes y datos personales sensibles, que deberían tener un tratamiento especial.

La implementación de ésta tecnología, sin evaluaciones de necesidad y proporcionalidad, hoy está exponiendo los datos biométricos y sensibles de la población a merced de posibles cruzamiento con otros datos expuestos en la misma base, relacionados a actividades vinculadas al crimen organizado, investigaciones internas del cuerpo de seguridad, sumarios y procesos llevados a cabo por las fuerzas públicas y otras entidades que han colaborado con la institución policial.

El daño exponencial es significativo, por tanto merece una auditoría profunda y una interrupción inmediata de las prácticas en curso lesivas a los derechos humanos, cómo la implementación de tecnologías de reconocimiento facial en cámaras en vía pública.

SISTEMA 911: PRINCIPAL INSTITUCIÓN QUE ADMINISTRA LAS CÁMARAS DE RECONOCIMIENTO FACIAL

El sistema fue creado por la Ley 4739/12 durante el Gobierno del ex-presidente Federico Franco, y es gestionado por la Dirección del Centro de Seguridad y Emergencias (CSE), dependiente de la Dirección General de Orden y Seguridad de la Policía Nacional.

Las facultades operativas del CSE consisten en el desarrollo y la operación del Sistema 911, la recepción y el procesamiento de las solicitudes de auxilio, así como el seguimiento de las solicitudes recibidas hasta su conclusión, entre otras de carácter netamente organizacional (Congreso Nacional, 2012). Esta dirección está dirigida por un Comisario General Inspector de Orden y Seguridad, conforme lo establece la misma ley.

El 5 de mayo de 2014, la Comandancia de la Policía Nacional emitió la Resolución 452, que establece de manera detallada las funciones y aspectos operativos del Sistema 911. Esta resolución creó y reguló la División de Cámaras y Monitoreo, responsable del monitoreo constante a través de cámaras de seguridad instaladas en distintas áreas bajo la jurisdicción del Sistema 911 (Policía Nacional, 2014). Entre sus funciones, la División se encarga de la vigilancia permanente, la detección de situaciones sospechosas de personas y vehículos, y el control de placas en lugares de alta afluencia.

Algunas de estas actividades tienen un alto potencial para vulnerar las normativas internacionales de derechos humanos previamente mencionadas. Además, tanto la ley que establece el Sistema 911 como las normativas internas de la Policía Nacional omiten definir criterios jurídicos claros sobre lo que constituye una 'situación sospechosa'. No se especifica quién califica dichas

63 Amnistía Internacional España. 2023. La vigilancia mediante reconocimiento facial retrospectivo oculta abusos contra los derechos humanos. Disponible en: https://www.es.amnesty.org/en-que-estamos/blog/historia/articulo/la-vigilancia-mediante-reconocimiento-facial-retrospectivo-oculta-abusos-contra-los-derechos-humanos/

actividades, ni el procedimiento a seguir para confirmarlas o descartarlas. Tampoco se contempla un mecanismo adecuado para la anonimización, destrucción o almacenamiento de las imágenes capturadas. (TEDIC, 2015)

La ley del Sistema 911 define su objetivo principal como la gestión integral de emergencias, desde la recepción del llamado hasta el reporte final, posicionando al sistema 911 como un canal de atención de emergencias ofrecido a la ciudadanía por la Policía Nacional y otras instituciones participantes (Congreso Nacional, 2012). Sin embargo, la adquisición de equipos con tecnología de reconocimiento facial, financiada con los Fondos de Servicios Universales (FSU) de la Comisión Nacional de Telecomunicaciones (CONATEL), plantea serias dudas sobre su legalidad y alineación con el propósito original del Sistema.

EVOLUCIÓN DE LA INCORPORACIÓN DE CÁMARAS EN PARAGUAY

La Policía Nacional, en 2018, anunció la incorporación de 154 cámaras de circuito cerrado, de las cuales 44 contaban con tecnología de reconocimiento facial, según informes del diario ABC Color (ABC. 2022).

Ese mismo año, el informe realizado por TEDIC concluía que la recolección masiva de datos biométricos "es innecesaria y desproporcionada" (TEDIC, 2018). En este informe hacía referencia a que la invasión se da al involucrar la recopilación de datos personales de individuos que transitan por espacios públicos, sin importar si han estado involucrados en actividades sospechosas o no, y sin ofrecer aparentes garantías de protección. También hablaba de la necesidad de transparencia del software de datos biométricos, su uso y alcance.

Sin embargo, a pesar de las diversas publicaciones de los medios de comunicación como Última Hora, La Nación y ABC Color, que se vamos a desglosar a continuación, y las solicitudes de información a través de los pedidos de acceso a la información pública entre agosto y setiembre de 2023 por TEDIC, cuyas respuestas por parte de varias instituciones fueron reiteradamente negadas, es prácticamente imposible determinar cuántas cámaras con reconocimiento facial fueron adquiridas desde aquel anuncio hasta la fecha de la elaboración de esta investigación.

Se puede observar que no existe un criterio unificado al proporcionar información sobre la cantidad de cámaras de circuito cerrado instaladas. Es decir, no existe una fuente única que ayude a transparentar estas cifras. Esta situación es evidenciada por las publicaciones hechas por distintos medios de comunicación.

En enero de 2021, había 1.444 cámaras a nivel país, según un informe publicado en julio de 2021[64] por la Dirección del Centro de Seguridad y Emergencias del departamento del Sistema 911 de la Policía Nacional. En septiembre del 2021, el diario Última Hora (UH) refiere que el Sistema 911 contaba con un total de 1.458 equipos[65], es decir, 14 cámaras más, después de ocho meses de la publicación anterior.

64 Policía Nacional del Paraguay. 2021. Tercer Informe Semestral de Rendición de Cuentas al ciudadano 2020. Policía Nacional del Paraguay. Disponible en: https://www.policianacional.gov.py/wp-content/uploads/2021/01/NOTA-07-2021-DIRECCION-CENTRO-DE-SEGURIDAD-Y-EMERGENCIAS.pdf

65 Ultima hora. 2021. Policía Nacional: solo el 60% de las cámaras del 911 funcionan. Disponible en: https://www.ultimahora.com/policia-nacional-solo-el-60-las-camaras-del-911-funcionan-n2960069

En dicha oportunidad, la fuente de la noticia fue el oficial Germán Rodríguez, del Sistema de Emergencia 911 de la Policía Nacional y no un informe, como el primero. Posteriormente, en octubre de 2022, La Nación publicó que el Sistema 911 de la Policía Nacional tenía 1.447 cámaras[66]. Esta publicación se basó en un nuevo informe de la Dirección del Centro de Seguridad y Emergencias, departamento del Sistema 911. El mismo habla de solo tres cámaras más de las que se tenían en enero de 2021, pero, si se hace una comparación con lo expresado por el oficial Rodríguez en septiembre de 2021 hay 11 cámaras menos.

Asimismo, para noviembre de 2022 según el diario ABC Color, el sistema de 911 ya contaba con un total de 1500 cámaras de circuito cerrado, aunque aclaraba que entonces funcionaban solo 800 por falta de mantenimiento[67]. Esta información se basó en la entrevista realizada al comisario Rafael González, jefe del Sistema 911 de la Policía Nacional.

Los informes oficiales del Sistema 911 revelan discrepancias en el número de cámaras reportadas. Además, la Policía Nacional no ha respondido a las solicitudes de información realizadas por TEDIC en 2023[68]. Estos hechos sugieren una falta de documentación transparente sobre cámaras robadas o extraviadas, incluyendo la ausencia de informes de seguimiento, actas de robo, sumarios internos y resoluciones correspondientes. Esta carencia de trazabilidad crea un ambiente propicio para la corrupción interna.

La gravedad del problema en la gestión y mantenimiento de esta tecnología se evidencia en su funcionamiento deficiente. Casos concretos ilustran esta situación[69]:

- En Remansito, distrito de Villa Hayes, las seis cámaras destinadas a la detección de placas vehiculares no operan a plena capacidad.
- En Yby Yaú, departamento de Concepción, las cámaras Panorámica, Inclinación y Zoom (PTZ) se encuentran completamente inoperativas.

Estos ejemplos demuestran que la infraestructura de vigilancia, una vez instalada, no mantiene su funcionalidad al 100%, lo cual compromete significativamente su eficacia y el propósito para el cual fue implementada.

Siguiendo esta línea de publicaciones de la Policía Nacional y medios de comunicaciones. Hemos elaborado una tabla descriptiva sobre la cantidad de adquisiciones de cámaras, el tipo, la marca y las que están en uso o fuera de uso.

66 La Nación. 2022. De 1.447 cámaras instaladas que tenía la Policía se redujeron a 640. Disponible en: https://www.lanacion.com.py/investigacion/2022/10/18/de-1447-camaras-instaladas-que-tenia-la-policia-se-redujeron-a-640/

67 ABC Color. 2022. De 1.500 cámaras del 911 en Paraguay, unas 800 no funcionan. Disponible en: https://www.abc.com.py/policiales/2022/11/11/de-1500-camaras-del-911-en-paraguay-unas-700-no-funcionan/

68 TEDIC. 2023. Amparos judiciales sobre reconocimiento facial en Paraguay realizadas por miembros de TEDIC: https://www.tedic.org/con-mi-cara-no-la-vigilancia-masiva-a-traves-del-reconocimiento-facial-en-paraguay/

69 La Nación. 2022. De 1.447 cámaras instaladas que tenía la Policía se redujeron a 640. Disponible en: https://www.lanacion.com.py/investigacion/2022/10/18/de-1447-camaras-instaladas-que-tenia-la-policia-se-redujeron-a-640/

TABLA 5. Evolución de la implementación de cámaras de la Policía Nacional durante el 2021.

DPTO	CIUDAD	CANTIDAD										ESTADO	
		Enero 2021					Diciembre 2021					En línea	Fuera de línea
		RF	PTZ	Fijas	LPR	Total	RF	PTZ	Fijas	LPR	Total		
Capital	Asunción	12	390	239	26	667	10	397	231	24	662	**234**	**428**
Central	San Lorenzo	3	155	4	26	188	6	178	4	26	188	**89**	**125**
	Luque												
	Capiatá												
	Ñemby												
Cordillera	Caacupé	0	10	0	4	34	0	10	0	4	34	**22**	**12**
	San Bernardino	2	18	0			2	18	0				
Alto Paraná	Ciudad del Este	10	110	0	12	132	10	104	0	12	126	**58**	**68**
Itapúa	Encarnación	10	88	56	10	164	10	87	56	10	163	**117**	**46**
Caaguazú	Coronel Oviedo	0	35	0	35	35	0	33	0	0	33	**24**	**9**
Amambay	Pedro Juan Caballero	8	76	0	12	96	8	76	0	12	96	**48**	**48**
Misiones	San Ignacio	0	30	0	6	66	0	30	0	6	61	**17**	**8**
	San Juan Bautista	0	30	0	0		0	25	0	0		**32**	**4**
Concepción	Concepción	0	38	0	0	48	0	38	0	0	48	**20**	**15**
	Yby Yau	0	10	0	0		0	10	0	0		**0**	**10**

Estos datos obtenidos en el marco de esta investigación confirman que evidentemente hubo un aumento de la adquisición de cámaras y software con reconocimiento facial por parte de la Policía Nacional. A esto se suma que, hay proyecciones de que este número siga en incremento considerando los proyectos legislativos existentes.

En ese contexto, se puede citar por ejemplo, el anuncio hecho por el Viceministerio de Transporte de Paraguay en julio de 2022[70], respecto a la búsqueda de implementar el Sistema Nacional de Arribo de Buses, una iniciativa de modernización del transporte público en el área metropolitana con una inversión de USD 12 millones.

Este proyecto prevé la construcción de 130 paradas de autobús equipadas con cámaras de seguridad, botones de emergencia conectados a la Policía Nacional y tecnología de reconocimiento facial y de placas. Las especificaciones del proyecto incluyen la instalación de 8.000 cámaras[71] en paradas y dentro de los autobuses, 130 cámaras con reconocimiento facial en paradas y 130 cámaras de reconocimiento de placas en paradas.

Adicionalmente, en junio de 2024 el Congreso Nacional aprobó la ley 7269 "De prevención, control y erradicación de la violencia en el deporte"[72], propuesto por los diputados los diputados Basilio Núñez, Juan Carlos Galaverna, Fernando Ortellado, David Rivas y la diputada Rocío Abed. El objetivo de esta legislación es establecer mecanismos de control y prevención de la violencia en eventos deportivos.

La iniciativa contempla la creación del Registro Nacional de Espectadores (RENAES) para recopilar información sobre incidentes violentos. Además, la ley establece sanciones tanto para los espectadores como para los organizadores en caso de incumplimiento, y enfatiza la instalación de sistemas de circuito cerrado de televisión y tecnología de grabación en las áreas cercanas a los recintos deportivos.

A pesar del cambio de gobierno, no existen señales que el cambio en la política integre perspectivas de derechos humanos, acceso a la información pública y mayor transparencia en la materia[73].

Paraguay aún no cuenta con una ley integral de protección de datos personales. Esta ausencia, combinada con una comprensión deficiente de los principios garantistas penales y las normativas de derechos humanos, plantea serias amenazas. Existe el riesgo de que se flexibilicen los controles y se avance en la implementación de tecnologías que degradan la calidad democrática y, contrariamente a lo que muchos piensan, afectan negativamente la seguridad de la población en el ejercicio de sus libertades civiles. Esta situación pone de manifiesto la urgente necesidad de establecer un marco legal robusto que proteja los derechos individuales y regule adecuadamente el uso de tecnologías de vigilancia.

70 Última Hora (2022). Paradas inteligentes sumarán 8.000 cámaras de seguridad. https://www.ultimahora.com/paradas-inteligentes-sumaran-8000-camaras-seguridad-n3013537

71 ídem nota al pie número 69.

72 Congreso Nacional – Ley 7269/2024 https://silpy.congreso.gov.py/web/expediente/128240

73 CODEHUPY. 2023. Informe de Derechos Humanos en Paraguay -2023. Bloque derechos digitales. Deudas y desafíos para un pleno disfrute de los derechos humanos en el entorno digital. Ley de registro único de espectadores. Pag 5. Disponible en: https://www.tedic.org/wp-content/uploads/2023/12/LIBERTAD-Digitales___Pdf-1.pdf

Donaciones y adquisiciones de cámaras de reconocimiento facial

En Paraguay, la adquisición de cámaras de reconocimiento facial se lleva a cabo principalmente a través de dos mecanismos: donaciones de los Fondos de Servicios Universales (FSU) y adquisiciones mediante licitaciones a través de la Dirección Nacional de Contrataciones Públicas (DNCP). En este apartado se describirán cada uno de los procesos, así como su legalidad de los mismos.

FONDOS DE SERVICIOS UNIVERSALES (FSU)

Los Fondos de Servicio Universal (FSU) son mecanismos diseñados para abordar las brechas de conectividad generadas por las características sociales, económicas, geográficas y demográficas del país. El concepto de servicios universales en telecomunicaciones se popularizó a nivel mundial durante la Conferencia Mundial de Telecomunicaciones (WTDC) organizada por la Unión Internacional de Telecomunicaciones (UIT). Surgieron en América Latina y el Caribe en respuesta a las privatizaciones de las décadas de 1980 y 1990, con el objetivo de mejorar el acceso a las tecnologías de la información y comunicación (TIC) en áreas menos atendidas. A pesar de su papel crucial en el desarrollo regional, la conectividad sigue siendo un desafío, con una brecha significativa entre zonas urbanas y rurales y un acceso a Internet de banda ancha aún limitado en comparación con otras regiones. Los FSU buscan cerrar estas brechas proporcionando recursos para inversiones en infraestructura y subsidios para proyectos en áreas rurales y desfavorecidas, promoviendo así la igualdad de acceso a servicios esenciales como la educación, la salud y el empleo. (Alliance for affordable Internet, 2021).

Como se observa se enfatiza que la finalidad del FSU consiste en subsidiar a los prestadores de servicios públicos de telecomunicaciones en las áreas que así lo justifiquen, refiere el estudio "Cerrando la brecha de conectividad digital: Políticas públicas para el servicio universal en América Latina y el Caribe", del BID (García Zaballos et al, 2021)

En América Latina, los fondos para estos servicios son financiados a través de contribuciones de los operadores de telecomunicaciones. El FSU se nutre generalmente de los aportes obligatorios de los prestadores de servicios de telecomunicaciones. Cada operador contribuye con el 1% de sus ingresos totales obtenidos por la prestación de servicios, descontando impuestos y tasas aplicables. (Alliance for affordable Internet, 2021).

En Paraguay aparece el FSU en el año 1995. La Ley 642/1995, en su Capítulo II, Artículo 97, estableció la creación del Fondo de Servicios Universales. El texto de la ley especifica:

> "Crea el Fondo de Servicios Universales que será administrado por la Comisión Nacional de Telecomunicaciones, con la finalidad de subsidiar a los prestadores de servicios públicos de telecomunicaciones en áreas que así lo justifiquen. La reglamentación de la presente Ley establecerá los sujetos y condiciones de contribución a dicho Fondo y definirá dichas áreas".

La ley determina así cuál es la finalidad de este Fondo, a la vez que supedita las condiciones específicas de su funcionamiento, como ser los sujetos contribuyentes y las condiciones de contribución, a la reglamentación de la ley por Decreto.

En ese orden, el Decreto Nº14135/96 que reglamenta la Ley 642, en virtud al artículo 129, delega esta facultad reglamentaria a la propia CONATEL, estableciendo que será la Comisión la que aprobará en un Reglamento específico, las normas que regulen el funcionamiento del Fondo de los Servicios Universales fijando los sujetos, condiciones de contribución y definición de las áreas de aplicación, de acuerdo a las políticas que señale el Gobierno. El mismo artículo del Decreto Nº14135/96 dispone además una restricción específica sobre el ámbito de aplicación del Fondo de Servicios Universales, estableciendo que la CONATEL no podrá usar los recursos provenientes del mismo, para gastos propios ni para su financiamiento.

En cumplimiento a esta delegación de la facultad reglamentaria, la CONATEL elabora y aprueba el Reglamento del Fondo de Servicios Universales, cuya primera versión no se encuentra a disposición por parte de CONATEL, para su visualización. Luego, por Resolución Nº312[74] del año 1999, el Directorio de CONATEL resuelve modificar por primera vez este Reglamento del Fondo de Servicios Universales.

Desde aquel primer Reglamento específico dictado por la CONATEL en el año 1999, hasta la fecha, han tenido lugar numerosas versiones[75] que han modificado tanto los objetivos del Fondo de Servicios Universales (FSU) como la forma de composición de sus recursos. En el siguiente resumen presentamos brevemente la evolución de estas modificaciones a lo largo del tiempo

Resolución Nº312/99 – Se establece la composición de los recursos del FSU por un mínimo de 20% del pago por derecho de explotación, el cual equivale al 1% da los Ingresos brutos del prestador que son recaudados por la CONATEL;

Resolución Nº495/2000 – Se mantiene la composición de los recursos del FSU. Se incorpora un artículo 47 al Reglamento del FSU que modifica los objetivos de este Fondo, ampliando su ámbito de alcance. El artículo incorporado es el siguiente:

> "Artículo 47.- El Fondo de Servicios Universales podrá subsidiar, además del Servicio Universal, programas sociales para promoción de la Educación, Cultura, Salud y Servicios de Emergencia, a través de los prestadores de servicios públicos de telecomunicaciones".

Resolución Nº34/2002 – Se mantiene la composición de los recursos del FSU con el 20% del pago por derecho a explotación. Se introduce una importante modificación sobre los objetivos del Fondo que no solamente amplia su ámbito de alcance, sino que además modifica la naturaleza de las contribuciones que este Fondo podrá efectuar.

El FSU consiste, tal como se ha dispuesto desde la primera versión de su Reglamento y hasta la fecha, en "un fondo creado con la finalidad de subsidiar a los operadores de servicios públicos de telecomunicaciones en áreas que así lo justifiquen, ya sea por porque no exista disponibilidad de servicios públicos de telecomunicaciones eficientes o imperen razones de interés público o social" (artículo 2 del Reglamento).

A través de esta Resolución Nº34/2002, motivados en la firma de un Convenio de Cooperación entre el Ministerio del Interior y la CONATEL, se incluye dentro del ámbito de alcance de este Fondo, a los "servicios de telecomunicaciones reservados al Estado, por gestión directa o por sus entes públicos", que se determinan en el artículo 60 de la Ley 642/95.

74 https://www.conatel.gov.py/conatel/wp-content/uploads/2019/10/go-000626-120bis-rd312-1999.pdf

75 https://www.conatel.gov.py/conatel/regimen-tarifario-y-fondo-de-servicios-universales/

Pero además de extender el ámbito de alcance para poder abarcar específicamente estos servicios reservados al Estado, se introduce una modificación en la naturaleza de la modalidad de financiamiento a ser realizado a través del Fondo, que de acuerdo con su finalidad es la de subsidiar a los operadores de servicios públicos de telecomunicaciones. Para ello, el artículo 9 del Reglamento dispone que "el financiamiento con cargo a los recursos del FSU podrá ser reembolsable o no reembolsable, y el financiamiento podrá cubrir hasta el 100 % de la inversión Inicial, en ambos casos será determinado en cada proyecto por la CONATEL, tomando en consideración la evaluación económica del proyecto realizada por ella". De la disposición claramente se comprende que la modalidad de financiamiento consiste en el otorgamiento de un subsidio para el financiamiento de proyectos previamente acordados con la CONATEL.

Sin embargo, para hacer factible el compromiso convenido con el Ministerio del Interior, se resolvió hacer lugar a la modificación de esta modalidad de financiamiento, en relación con los servicios listados en el art. 60 de la Ley 642[76], conforme a los siguientes argumentos:

> "CONSIDERANDO: Que se ha firmado el Convenio de Cooperación entre el Ministerio del Interior y la Comisión Nacional de Telecomunicaciones CONATEL, cuyo objeto es "Dotar a la Policía Nacional de un sistema de atención y despacho de llamadas de emergencias, a través de la provisión limitada y por única vez de los bienes y servicios necesarios como la ingeniería, el equipamiento, el software, la capacitación y garantía de funcionamiento en condiciones de operación normal por el periodo de dos (2) años para lo cual la CONATEL utilizará el Fondo de Servicios Universales. Que para que la CONATEL pueda otorgar subsidios en bienes y servicios, resulta necesario modificar el Reglamento del Fondo de Servicios Universales y: […]"

En consecuencia, la Resolución Nº34/2002 modifica el Reglamento del FSU incluyendo la siguiente disposición de autorización de uso de sus recursos:

> "Articulo 11. La CONATEL podrá realizar el subsidio para los servicios comprendidos por el Art. 60 de la Ley 642/95, por medio de la provisión de bienes y servicios a ser especificados por ella en cada proyecto. Los bienes y servicios mencionados deberán ser proveídos a través de licitación pública de ofertas."

De esta forma, el FSU queda autorizado a financiar como forma de subsidio de los servicios allí establecidos, directamente por medio de la provisión de bienes y servicios por parte de CONATEL, introduciendo esta importante modificación en la naturaleza de la modalidad de financiamiento que puede efectuarse a través del Fondo.

---

76 "Artículo 60.- Los servicios de telecomunicaciones reservados al Estado, por gestión directa o por sus entes públicos, son los siguientes:
- servicios radioeléctricos de aywuda a la meteorología;
- servicios radioeléctricos de ayuda a la navegación aérea;
- servicios radioeléctricos de ayuda a la navegación fluvial y marítima;
- servicios radioeléctricos de navegación aéro-espacial;
- servicios radioeléctricos de radio astronomía;
- servicios de socorro y seguridad de la vida humana en los ríos de la República y en alta mar;
- servicios de telecomunicaciones, información y auxilio en carretera; y,
- aquellos servicios que afecten la seguridad de la vida humana, o cuando por razones de interés público así lo establezca el Poder Ejecutivo.

El Estado podrá otorgar en concesión la prestación temporaria de estos servicios a particulares en las condiciones que se determine en las respectivas normas legales, reglamentarias y contractuales."

Resolución Nº795/2004 – Se modifica la composición de los recursos del FSU, incrementado el porcentaje que estaba fijado en un 20 % de los aportes abonados por las empresas operadoras bajo el concepto de Tasa por explotación comercial, al 40 %.

Es interesante notar cuáles fueron los argumentos sostenidos para fundamentar este incremento, que conforme lo señalado en la Resolución podemos resumir en "la notoria disminución en las recaudaciones previstas en concepto de Tasa de Explotación Comercial, que actualmente es la única fuente de financiación del fondo de referencia", afirmando que "la adopción de la medida sugerida no afectaría el normal funcionamiento de la CONATEL". Asimismo, se argumenta "que actualmente y en el futuro normalmente será muy difícil contar como fuente de recursos para el Fondo de Servicios Universales provenientes de asignaciones, donaciones, legados, transferencias u otros aportes establecidos en el inciso b del artículo 6 del Reglamento mencionado".

Los argumentos sostenidos ponen de resalto el alto grado de discrecionalidad que dispone la CONATEL para tomar decisiones sobre cómo se debe integrar la composición de los recursos del Fondo, y una muy débil argumentación fáctica que acompañe estas decisiones. En este caso, no se verifica que la decisión esté respaldada al menos por estudios técnicos concretos que demuestren comprobadamente la necesidad de los cambios sostenidos por la Comisión.

Resolución 1499/2006 – Se modifica nuevamente la composición de los recursos del FSU, esta vez dismuniyendo el porcentaje que estaba fijado en un 40 % de los aportes abonados por las empresas operadoras bajo el concepto de Tasa por explotación comercial, al 20 %.

En línea con lo mencionado anteriormente, de nuevo se exponen débiles argumentos para fundamentar la decisión adoptada, la cual implica una medida de gran trascendencia al disponer la reducción en un 50% de los recursos destinados al Fondo, a tan solo 2 años de haberse resuelto su aumento en igual proporción. El argumento expresado en la Resolución refiere a los montos presupuestados para al FSU en el ejercicio fiscal 2007, comparado con el 2007 y el saldo disponible para el Fondo a esa fecha, al que se lo considera un "monto muy superior a las previsiones presupuestarias, tanto del ejercicio 2006 como el ejercicio 2007", por lo cual "la Gerencia Administrativa Financiera concluye que la reducción del porcentaje de aporte al Fondo de Servicios Universales está totalmente justificado".

Resolución 196/2014 – Se mantiene la composición de los recursos del FSU con el 20% de los aportes abonados por las empresas operadoras por el concepto de Tasa por Explotación Comercial.

Resolución 2474/2018 – Se modifica la composición de los recursos del FSU, incrementado el porcentaje que estaba fijado en un 20 % de los aportes abonados por las empresas operadoras bajo el concepto de Tasa por explotación comercial, al 30 %. A más de ello, la modificación también dispone incorporar un nuevo recurso a integrar el FSU, constituido por "el 50% de todos los ingresos percibidos en concepto de MULTAS por sanciones aplicadas a prestadores de servicios de telecomunicaciones".

Para esta decisión, la Gerencia Administrativa Financiera argumenta que considerando que el aumento implicaría un importe que dejará de estar disponible para gastos corrientes de la CONATEL, "considerando la totalidad de los ingresos de la CONATEL, no tendría mayor incidencia en el cumplimiento de los compromisos asumidos". Asimismo, se manifiesta que "los ingresos percibidos en concepto de MULTAS, puede considerarse una fuente de financiamiento que ayudará a fortalecer las disponibilidades financieras del Fondo de Servicios Universales, en ese sentido, podría considerarse la posibilidad de derivar el 50% de todos los ingresos percibidos por MULTAS al Fondo de Servicios Universales, decisión que no afectará el cumplimiento de las obligaciones

de la CONATEL". Y, por último, la Gerencia de Planificación y Desarrollo indica "que a fin de lograr los objetivos del Plan Nacional de Telecomunicaciones - PNT, es necesaria la intervención del regulador, en lo que se refiere a las zonas poco rentables para las empresas prestadoras de servicios, utilizando los recursos del FSU, para lo cual sería necesario modificar el Reglamento del FSU, con una propuesta de ampliación del porcentaje de la Tasa de Explotación Comercial destinada para constituir los recursos del FSU".

Actualmente, las fuentes de recursos del Fondo de Servicios Universales, según el Art. 6 del Reglamento, están fijadas en: El 30% (treinta por ciento) del pago por derecho de explotación que equivale al 1% (uno por ciento) de los ingresos brutos del prestador que son recaudados por la Comisión Nacional de Telecomunicaciones; el 50% de todos los ingresos percibidos en concepto de MULTAS por sanciones aplicadas a prestadores de servicio de Telecomunicaciones, y; las asignaciones, donaciones, legados, trasferencias u otros aportes por cualquier título proveniente de personas naturales o jurídicas.

El artículo 3 del Reglamento del Fondo de Servicios Universales , detalla los objetivos principales del fondo, que son: (a) financiar la expansión de los servicios públicos de telecomunicaciones en áreas rurales y lugares de interés público y social; (b) facilitar el acceso eficiente y asequible a los servicios de telecomunicaciones para un mayor número de paraguayos, ajustando las tarifas a los niveles de ingresos de los beneficiarios; y (c) maximizar el beneficio económico de los servicios de telecomunicaciones, reduciendo costos en sectores clave como la salud y la educación (CONATEL, 2000). Además, el Reglamento incluye un glosario que define los servicios universales como el acceso a teléfonos públicos o cabinas con capacidad para transmitir voz y datos en localidades, ya sean rurales o urbanas, que carecen de servicios de telecomunicaciones y que son consideradas de interés nacional. Esta definición es provisional y puede ser modificada por CONATEL, aunque hasta la fecha no se han realizado cambios (CONATEL, 2000).

De las situaciones evidenciadas en la evolución de este marco normativo y regulatorio del Fondo de Servicios Universales, se desprenden los siguientes aspectos que merecen una especial atención:

- La ley 642/95 en su artículo 97 dispuso que la reglamentación (que, conforme al artículo 238 de la Constitución, corresponde a quien ejerce la Presidencia de la República) sería la instancia normativa a través de la cual se establezcan los sujetos y las condiciones de contribución del Fondo de Servicios Universales. Sin embargo, el Decreto №14135/96 obvia abordar estas definiciones en su cuerpo normativo, y delega a la CONATEL la atribución de aprobarlas por medio de un Reglamento específico.

  La discrecionalidad que ha caracterizado a los actos de reglamentación del Fondo de Servicios Universales por parte de la CONATEL, da cuenta de la necesidad de promover un nuevo encuadre normativo para la definición de la composición del Fondo de Servicios Universales, que respete la jerarquización normativa que la ley estableció en primer orden. El Decreto reglamentario delegó esta facultad a la CONATEL para que la ejerza a través de sus Reglamentos, aprobados por Resolución del Directorio, los que constituyen actos administrativos que por su categoría normativa revisten menor estabilidad jurídica y menor control, a la vez que excluyen la participación del Poder Ejecutivo en la toma de decisiones.

- Actualización de definiciones, objetivos y otras condiciones relativas al FSU “de acuerdo a las políticas que señale el Gobierno”: El Decreto reglamentario de la Ley 642/95 dispuso que las definiciones que se hagan sobre el FSU deberán ser “de acuerdo a las políticas que señale el Gobierno”. Actualmente, en virtud a la Ley 6207/18 que crea el MITIC, ésta institución es titular del 50% por del Fondo de Servicios Universales administrado por la CONATEL, conforme lo dispone el artículo 18, inciso 3.

  Sin embargo, a pesar de esta importante modificación de incidencia en la política de gobierno, no se ha visto que esté reflejada en la reglamentación del Fondo, y además, como consecuencia del encuadre normativo actual, se excluye asimismo la partipación del MITIC en las decisiones que afecten la composición de este fondo.

  Además, existen numerosas condiciones del contexto actual de los servicios de telecomunicaciones y convergencia con servicios TIC, entre otras muchas que sin duda se han evidenciado a lo largo de estos casi 25 años de vigencia de este Fondo, que ameritan una profusa revisión y actualización de su Reglamento y las condiciones establecidas en el mismo.

CONECTIVIDAD Y EL USO REAL DEL FSU

Según los informes de subsidios otorgados del FSU por CONATEL, durante los últimos 6 años[77] efectuó millonarias compras para donar cámaras de reconocimiento facial y otros insumos de seguridad para el sistema 911. Como se puede observar en sus informes, escasamente fue destinado a la expansión de los servicios públicos de telecomunicaciones en áreas rurales y lugares de interés público y social, como por ejemplo, los centros educativos. Por ejemplo, en julio de este año, una publicación periodística señaló que los directores de instituciones educativas denunciaron baja conectividad en las instituciones educativas (Última Hora, 2023).

La nota periodística indicó además que de 8.900 casas de estudio, solo 2.055 tenían conectividad a internet gracias al Ministerio de Educación y Ciencias (MEC) o el Ministerio de Tecnologías de la Información y Comunicación (MITIC).

Por otra parte, en cuanto al acceso a internet desde los hogares, según el Instituto Nacional de Estadísticas (2023), las brechas en la conexión son mayores al hacer la comparación entre las zonas urbanas (83,2%) y las zonas rurales (63,7%), a través de los diferentes tipos de conexión.

Si bien, esta encuesta apunta a que el porcentaje de acceso al internet es elevado (98,8%), cuando hablamos de una conexión desde el teléfono celular y a servicios de mensajería o redes sociales, esto no garantiza una conexión eficiente para trabajar o estudiar, como se pudo observar en la pandemia con los problemas que presentó la mala calidad de la conexión.

Según la Encuesta Permanente de Hogares (EPH: 2023), la población paraguaya que utiliza internet es de 76.3%, lo que representa aproximadamente 4.556.000 personas. El crecimiento porcentual del año 2015 al 2022 ha sido de 26.6% (De 49.7% a 76.3%). Por otro lado, el acceso a internet está marcado por área de residencia, presentando una importante preeminencia la zona urbana vs la rural, pues las personas que viven en zonas urbanas alcanzan el 83.2% y las que viven en áreas rurales el 63.7%. Es importante señalar, que, 9 de cada 10 hogares en el país cuentan con el acceso a por lo menos una tecnología de información y comunicación (teléfono, televisor, radio, computadora, TV cable, Tablet, entre otros).

77 CONATEL. Subsidios otorgados por año. Disponible en https://www.conatel.gov.py/conatel/subsidios-otorgados/

En cuanto a las características de uso, según criterios etarios, se observa que el grupo comprendido de 20 a 34 años es el que utiliza mayormente internet, pues se pudo identificar que el uso en esta franja es superior al 90%, mientras que el bloque de más de 35 años alcanza el 69.3%, el de 15 a 19 años el 87% y el de 10 a 14 años muestra un 51.6%. El uso de internet según sexo muestra que el 77.6% corresponde a mujeres y el 74.9% a hombres.

Un aspecto interesante a resaltar es que existe una correspondencia de mayor cantidad de uso de internet según mayor sea la cantidad de años de estudio, en este sentido, las personas con más de 13 años de estudios utilizan en un porcentaje superior al 90%.

Es por tanto que la utilización de recursos públicos del FSU de forma discrecional y con poca transparencia, no solo es un hecho que puede dar lugar a la corrupción pública sino que también contribuye a profundizar desigualdades estructurales históricas, perpetuando un modelo de desarrollo económico y social excluyente.

Los altos costos de inversión en tecnologías de seguridad ineficientes y críticas en asuntos de derechos humanos se contraponen a proyectos posibles cómo fortalecer conectividad en zonas remotas para abordar la seguridad más allá de una mirada persecutoria.

A partir de lo expuesto sobre el Sistema 911 y el FSU, se observa que el canal de gestión de emergencias administrado por la Policía Nacional no se ajusta completamente a los objetivos del FSU ni cumple con la definición oficial de servicio universal establecida por la CONATEL. No obstante, el FSU sigue siendo utilizado, junto con gobernaciones y otras entidades gubernamentales, para la adquisición de equipos con tecnología de reconocimiento facial, lo que plantea preguntas sobre su alineación con el propósito original del fondo.

DONACIONES DEL FSU AL SISTEMA 911 Y MUNICIPIOS

El FSU, creado para fin de cerrar la brecha de conectividad digital y conectar a grupos vulnerables, se dedica a hacer compras para la Policía Nacional, específicamente de tecnología de reconocimiento facial. Esta cuestión fue criticada internacionalmente por la Alliance for Affordable Internet, en colaboración con Internet Society. En su análisis de diversos casos de ejecución de FSU en América Latina, la Alliance for Affordable Internet identificó un uso excepcional de estos fondos para la adquisición de cámaras de video vigilancia por Paraguay. Según su informe, “algunos usos, como la compra de equipos TIC, por ejemplo cámaras de vigilancia, pueden no contribuir necesariamente al objetivo de universalidad para el que se crearon los FSU” (Alliance for Affordable Internet, 2021, p. 29). Esta crítica utilizan las investigaciones previas realizadas por TEDIC en 2018[78], que ya habían señalado preocupaciones similares sobre la alineación de los fondos con sus objetivos originales.

CONATEL adjudicó un total de 27 Licitaciones, desde 2011 hasta 2022, a través del FSU[79]. En este punto, cabe destacar que desde 2011 hasta 2016, CONATEL adquirió equipos para la conexión y expansión de la conexión de internet.

78 TEDIC. 2018. Biometría y vigilancia: la enajenación continua de nuestros derechos. Disponible en: https://www.tedic.org/wp-content/uploads/2018/12/La-enajenaci%C3%B3n-continua-de-nuestros-derechos_TEDIC_2018-2.pdf

79 CONATEL s.f. Contratos otrogados a través del FSU. Disponible en: https://www.conatel.gov.py/conatel/contratos-fsu/

A partir de 2017, CONATEL empieza a realizar compras destinadas a la Policía Nacional y de tecnología con reconocimiento facial. En esta serie de licitaciones es posible hallar un total de siete compras que incluyen cámaras de circuito y softwares de reconocimiento facial. Desde ese total, la empresa TSV del Paraguay se alzó con seis licitaciones.

Un dato importante de mencionar es que ninguna de estas licitaciones se encuentran en la Dirección Nacional de Contrataciones Públicas, sino en la página de CONATEL, en la sección de contratos otorgados a través del FSU. Estas licitaciones adjudicadas a TSV suman en cinco años, de 2018 a 2022, un total de ₲ 57.550.880.000 (USD 7.831.117 al cambio actual)[80].

A continuación, brindamos un análisis sintético de las principales cuestiones observadas en las licitaciones ejecutadas por CONATEL y brindada al Sistema 911, a cargo del Ministerio del Interior y la Policía Nacional de Paraguay:

- **FSU № 2/2018**

En el año 2018, CONATEL continuó con su compra destinada al Sistema de Emergencias 911 de la Policía Nacional, dependiente del Ministerio del Interior. En esta ocasión, la compra fue para expandir el SADLE 911 de la Policía Nacional en las ciudades de Coronel Oviedo, Caaguazú, San Ignacio, Ciudad Del Este y Encarnación. (CONATEL, 2018).

La empresa adjudicada fue nuevamente TSV del Paraguay por ₲ 18.700.000.000 (USD 2.544) entre los varios íntems requeridos, CONATEL adquirió, sitios (cámara PTZ IP) de video vigilancia con todos sus accesorios: 15 para Coronel Oviedo; ocho para Caaguazú, 30 para San Ignacio, 60 para Ciudad del Este y 60 para Encarnación. Además para Encarnación se adquirieron 10 cámaras de reconocimiento de placas y 10 cámaras de reconocimiento de rostro.

- **FSU № 2/2019**

Esta licitación del FSU se basó en subsidiar la implementación de la ampliación del SADLE de la Policía Nacional "mediante un sistema complementario para la comunicación de datos críticos de todas las llamadas que acceden, mediante la marcación de la numeración 911, a los Centros de Seguridad y Emergencias (CSE) ubicados en las ciudades de Asunción, Ciudad del Este, Encarnación, Concepción, Coronel Oviedo y San Juan Bautista" (CONATEL, 2019).

Entre los detalles solicitados, el documento señala que plataforma a ser provista deberá contar con una serie de características y prestaciones, entre las cuales se mencionan algunas de las más llamativas.

El sistema deberá permitir la integración de sistemas de terceros como sistemas de CCTV, sistemas de reconocimiento facial, sistema de alarmas, sistemas de reconocimiento de placas etc., la cual permitirá al módulo de gestión de incidentes enviar notificaciones masivas a usuarios y/o a la fuerza de respuesta en caso de que exista algún incidente detectado por alguno de estos sistemas. La empresa adjudicada fue una vez más la empresa TSV del Paraguay por un monto total de ₲ 7.970.000.000 (USD 1.084.501).

80 Banco central del Paraguay. Cotización Moneda. Cambio calculado al realizar esta investigación: 7349 Gs x dólar americano. https://www.bcp.gov.py/webapps/web/cotizacion/monedas

- **FSU № 01/2020**

  Esta convocatoria sirvió para subsidiar la expansión del SADLE del Sistema 911 de la Policía Nacional que fue realizada e Implementado en el departamento Central y Asunción". (CONATEL, 2020).

  Entre una serie de ítems, se destacan la adquisición de 50 cámaras IP PTZ. El contrato señala que el presente llamado requiere la provisión, instalación y puesta en funcionamiento de cámaras IP tipo PTZ y detalla la distribución de las mismas por ciudad y comisarías:

  - Asunción (20 cámaras): Comisaría №3, Comisaría №12, Comisaría №13 Cantidad: Veinte
  - Área Metropolitana (30 cámaras):Comisaría №8 (Capiatá), Comisaría №53 (Fernando De La Mora), Comisaría №7 (Ñemby) y la Comisaría №15 (San Lorenzo).

  Por otra parte, también habla de la provisión de tres cámaras para reconocimiento facial a ser distribuidas en el área Central: Comisaría №8, Comisaría №53 y la Comisaría №7. Esta es la única licitación de esta serie que fue adjudicada a la empresa Proseco S.A, por el monto de ₲ 7.899.900.000 (USD 1.074.962).

  La implementación de cámaras en el marco de esta licitación expone una preocupación particular, atendiendo a una presunta intención de monitorear espacios públicos de protesta social, tal cómo se puede ver en el reporte de instalación de cámaras firmado en abril del 2021, a pocos días de grandes manifestaciones ocurridas en el Centro de Asunción tras la crisis sanitaria-económica a causa del COVID-19 (CONATEL, 2021).

  El documento, firmado por Juan Carlos Duarte, presidente de CONATEL[81], da cuenta que a pedido del ex-ministro Arnaldo Giuzzio en notas del 16 y 30 de marzo, se solicitó la instalación de cámaras, por ejemplo, frente al partido de gobierno, la Asociación Nacional Republicana (ANR), tras las manifestaciones ocurridas durante marzo del 2021 en Asunción por la crisis sanitaria. (CONATEL, 2021)

81 Fue presidente de CONATEL en el periodo (2019-2023) y actualmente se le renueva el puesto en CONATEL. Según la publicación de ABC, durante la administración de Duarte hubo malversaciones de fondos de la institución por valores de más de 4 millones de USD. https://www.abc.com.py/politica/2023/08/18/pena-coloca-en-conatel-al-que-la-cgr-lo-descubrio-con-manejo-discrecional-de-recaudacion/

El documento da cuenta de una buena práctica de transparencia pública. Estas serían las ubicaciones exactas donde se instalaron las mismas:

COMISARÍA 3° ASUNCIÓN		
Nº	Dirección/Ubicación	Tipo
1	Independencia Nacional c/ Presidente Franco	PTZ
2	Independencia Nacional c/ Paraguayo Independiente	PTZ
3	Paraguayo Independiente y Nuestra Señora de la Asunción	PTZ
4	Nuestra Señora de la Asunción y Presidente Franco	PTZ
5	Presidente Franco y Alberdi	PTZ
6	25 de Mayo y Tacuarí	PTZ
7	Chile y Manduvirá	PTZ
6	Lorenza Martínez y Cmte. Pedro Caballero	PTZ
7	Cañadón Chaqueño y Sto. 1ro. Eladio Galeano	PTZ
COMISARÍA 13° ASUNCIÓN		
1	Choferes del Chaco y Cap. Aparicio Figari	PTZ
2	Eucalipto y Carmen del Paraná	PTZ
3	Eucalipto y Mons. Hermenegildo Roa	PTZ
4	Carmen del Paraná y Defensa Nacional	PTZ
5	Boquerón y Cap. Aparicio Figari	PTZ
6	Guaraní y Chivato	PTZ
COMISARÍA 7° CENTRAL - ÑEMBY		
1	Plaza Fulgencio Yegros	PTZ
2	Acceso Sur c/ Bernardino Caballero	PTZ
3	Acceso Sur e Independencia Nacional	PTZ
4	Acceso Sur y Sargento Simeón Gómez	PTZ
5	Acceso Sur y Avda. Emiliano Vasconcellos	PTZ
6	Avda. Emiliano R. Fernández y Avda. Pratt Gill	PTZ
7	Avda. Pratt Gill c/ Santa Librada	PTZ
8	Santa Rosa y Presidente Franco	PTZ
COMISARÍA 15° CENTRAL - B° BARCEQUILLO		
1	Andrés Barbero y Zavalas Cué	PTZ

COMISARÍA 53° CENTRAL - B° SAN MIGUEL		
1	Avda. Mcal. López y Libertad	PTZ
2	Avda. Mcal. López y Cnel. Ayala	PTZ
3	Libertad c/ Antonio Ruiz Montoya	PTZ
4	Cnel. Machuca y Laguna Grande	PTZ
5	Avda. Laguna Grande y Manuel Britez Borges	PTZ
6	Avda. Mcal. López y Libertad	RF

- **FSU № 01/2021**

En 2021, aún durante la pandemia, CONATEL convocó a una licitación para el "otorgamiento de subsidio a través del fondo de servicios universales para la creación del centro de seguridad y emergencias del sistema 911 – CSE 911 de la Policía Nacional a ser implementado en la sede Villarrica, para los departamentos Guairá y Caazapá" (Contrato 03/21, 2021).

El pliego de bases y condiciones exige un sistema de videovigilancia con 20 cámaras IP PTZ, distribuidas en toda la ciudad de Villarrica, conectadas al CSE 911, mediante fibra óptica como red de acceso. Entre otros ítems, el monto adjudicado en el marco de esta compra fue de ₲ 7.990.000.000 (USD 1.087.222) y una vez más fue adjudicada a la empresa TSV del Paraguay.

- **FSU № 02/2021**

En 2021, CONATEL realizó una convocatoria para el otorgamiento de subsidio a través del Fondo de Servicios Universales para "la expansión del Sistema de Atención y Despacho De Llamadas De Emergencia SADLE 911- de la Policía Nacional a ser implementado en la ciudad de Horqueta, departamento de Concepción"[82].

En la ocasión, la institución adquirió 15 unidades de cámara IP PTZ y un software. El pliego de bases y condiciones señala que:

> "Además de un software VMS se debe considerar la provisión, instalación y configuración del software a ser provisto, el mismo deberá contar con las licencias necesarias para la gestión y grabación de quince (15) canales de video, y adicionalmente una (1) licencia para analítica de reconocimiento facial".

Dicho software estaba destinado a la Comisaría 3.°, ubicada sobre Avda. Mcal. López, Entre Brasil y Ypané. Nuevamente la empresa TSV del Paraguay S.R.L es la adjudicada y en esta adjudicación no se puede determinar el monto adjudicado, considerando que en la página no se encuentra o no se puede descargar el documento.

Este software además contiene exigencias como la capacidad de registrar y almacenar en la base de datos: imagen del rostro, fecha, hora, y cámara; además de mostrar en la interfaz gráfica la tasa de reconocimiento (%) y el nombre de cada persona reconocida.

82 CONATEL. Licitación pública FSU. 02.2021. Disponible en: https://www.conatel.gov.py/conatel/wp-content/uploads/2023/03/4.-pbc-lp-fsu-n-02-2021.pdf

También refiere que debe almacenar un número ilimitado de listas de vigilancia de reconocimiento facial y perfiles de personas en ellas. Asimismo deberá contar con campos de: primer nombre, segundo nombre y apellido. Incluso requiere la posibilidad de que cada perfil de persona pueda ser agregado a una "lista negra".

- **FSU № 02/2022**

  Con esta licitación, la CONATEL subsidió la implementación de un CSE del Sistema 911 en la sede regional del departamento Central (CONATEL, 2202a). Esta adquisición también fue adjudicada a la empresa TSV del Paraguay por ₲ 13.000.000.000 (USD 1.768.948) para un total de 82 ítems, entre los cuales se encuentran los siguientes pedidos:

  - Un software de reconocimiento facial con módulo forense.
  - Un soporte y mantenimiento garantizado de buen funcionamiento software de reconocimiento facial con módulo forense por 730 días
  - Un servidor para módulo de análisis facial forense.
  - Un servicio de implementación servidor para módulo de análisis facial forense.

- **FSU № 03/2022**

  Esta licitación se denomina "Otorgamiento De Subsidio A Través Del Fondo De Servicios Universales Para La Expansión Del Sistema de Atención y Despacho de Llamadas de Emergencia -SADLE 911- De La Policía Nacional, a ser Implementado en la Ciudad De San Lorenzo, Departamento Central". (CONATEL, 2022b).

  Entre los 18 ítems adjudicados, se describe la compra de un servidor de analítica de reconocimiento facial y software de reconocimiento facial por suscripción de 24 meses (por canal de video) por un monto de ₲ 1.990.980.000 (USD 2.700.918) a la empresa TSV Del Paraguay S.R.L.

  En efecto, las compras realizadas por la Comisión Nacional de Telecomunicaciones (Conatel), mediante el Fondo de Servicios Universales, revelan un desvío significativo respecto al propósito original de estos fondos, que estaban destinados a cerrar brechas de conectividad en el país, las cuales persisten de manera considerable.

  También esta investigación revela un incremento en la compra de cámaras con tecnología de reconocimiento facial, financiadas a través de una serie de inversiones multimillonarias. Este incremento en adquisiciones contrasta con la limitada efectividad de dicha tecnología para prevenir delitos o identificar a los responsables, tal como se ha destacado previamente en esta investigación. Estos procesos, además, exponen una preocupante falta de diversificación en la selección de proveedores, dado que la empresa TSV Del Paraguay S.R.L. ha sido elegida en múltiples ocasiones. Asimismo, llaman la atención las especificaciones con las que cuentan algunas compras de software de reconocimiento facial con capacidad no sólo de reconocimiento facial, sino de generar una base de datos y la consecuente posibilidad de eventualmente incluir nombres en una "lista negra". A esto se suma la preocupación por la efectiva vigilancia masiva que se busca ejercer con la instalación de estas cámaras, principalmente en espacios de protesta social, lo cual pone en riesgo la democracia y la libertad de ejercer el derecho a manifestarse, como lo señala el pedido realizado en 2021 por el entonces ministro del Interior, Arnaldo Giuzzio, de poner cámaras en puntos claves.

- **FSU № 02/2024**

  La licitación Pública FSU 02/2024[83] "Para el otorgamiento de subsidio a través del fondo de servicios universales para la implementación de un centro de seguridad y emergencias del sistema 911 – CSE 911 de la Policía Nacional en la ciudad de Pilar, departamento de Ñeembucu y la provisión de equipos terminales móviles fue lanzada en setiembre del 2024. Al cierre de esta investigación, según la base de pliegos y condiciones de la licitación FSU 02/2024[84], se encuentra en la fase final sin que se haya adjudicado un oferente ni definido un monto máximo para el proyecto.

  Esta licitación tiene como objetivo proveer equipamiento informático, software de vigilancia y cámaras de videovigilancia. Específicamente, se detalla la adquisición de 20 cámaras de videovigilancia PTZ y 10 cámaras tipo *bullet*.

ADQUISICIONES DE CÁMARAS DE RECONOCIMIENTO POR LICITACIONES EN LA DNCP

Investigar sobre las licitaciones convocadas por diversas instituciones públicas para adquirir cámaras y software de reconocimiento facial resultó ser una tarea compleja. El acceso a estos datos se dificultó porque, al publicar la información sobre estas compras, las instituciones no incluyeron palabras clave en los títulos ni las clasificaron en las categorías correspondientes de la Dirección Nacional de Contrataciones Públicas (DNCP)

Al indagar sobre la adquisición de tecnología con reconocimiento facial en la página de la DNCP, únicamente se identifica una licitación convocada por CONATEL en diciembre de 2022. Este proceso fue convocado por CONATEL, en diciembre de 2022, con el título de: "Licitación Pública Nacional para la Adquisición De Equipos De Seguridad y Sistemas De Circuito Cerrado CCTV", por un monto de ₲ 3.459.800.000. (USD 470.785). (Dirección Nacional de Contrataciones Públicas, 2022c).

En esta convocatoria, se presentaron dos firmas, Blue Ocean Company S.A. y TSV del Paraguay S.R.L., proceso en el cual fue adjudicada la firma TSV. En un total de cinco ítems, fueron adquiridas 58 cámaras y un software de reconocimiento facial de la marca CORSIGHT, procedente de Israel.

En este proceso no se hallaron protestas. Sin embargo, se encontraron varias consultas y verificaciones de la Dirección Nacional de Contrataciones Públicas. Es relevante destacar que esta adquisición fue categorizada como Categoría 24, que abarca: equipos, accesorios y programas computacionales, de oficina, educativos, de imprenta, de comunicación y señalamiento.

Como se puede observar, la cantidad de cámaras que aparentemente tiene la Policía Nacional para el sistema de 911 difiere de la cantidad de compras que aparecen en estos resultados.

Por ende, para hallar esta información, el equipo de investigación debió dejar de lado las palabras claves y reemplazarlas por otras. También fue necesario cambiar la categoría de la búsqueda específica en la página web de la DNCP, considerando que la web cuenta con distintos filtros para la búsqueda de información sobre las licitaciones.

---

83 La licitación 01/2024 fue cancelada según los datos públicos de CONATEL. Disponible en https://www.conatel.gov.py/conatel/licitacion-publica-fsu-n-01-2024/

84 CONATEL. Licitación pública FSU. 02.2024. Disponible en: https://www.conatel.gov.py/conatel/wp-content/uploads/2024/09/anexo-rd-2580-2024-pbc-lp-fsu-n-02-2024_2.pdf

Ese fue el caso de la licitación № 419935, de octubre de 2022 denominada "Actualización y Adquisición de Equipos para el Centro de Seguridad y Emergencias del Sistema 911 de la Policía Nacional". (Dirección Nacional de Contrataciones Públicas, 2022a).

La Policía Nacional, a través del Ministerio del Interior, fue la institución convocante para esta compra, la cual resultó difícil de localizar debido a dos razones principales. Primero, el título de la licitación no incluye palabras clave como "cámara", "monitoreo" o "reconocimiento facial". Segundo, la licitación no está catalogada en la Categoría 25, que corresponde a "equipos militares de seguridad y servicios de seguridad y vigilancia". En contraste, el nombre de la licitación hace referencia a un "Centro de Seguridad", pero está clasificada en la Categoría 24, que abarca "equipos, accesorios y programas computacionales, de oficina, educativos, de imprenta, de comunicación y señalamiento". Este hallazgo sugiere una falta de criterios estatales o institucionales unificados para la adquisición de cámaras y software de reconocimiento facial. Es decir, esta compra se realizó para el centro de seguridad, pero no estaba en la categoría de seguridad. Además contemplaba la compra de tecnología de reconocimiento facial, información que no aparece en el título.

En una millonaria compra de la Policía Nacional, por un total de ₲ 22.463.000.000 (USD 3.056.606), se adquirieron dos lotes: uno con 72 ítems y otro con 10 ítems, que incluye un software de reconocimiento facial de la marca CORSIGHT, procedente de Israel. Aunque la licitación fue impugnada, no se suspendió. Es relevante destacar que no todas las cámaras utilizadas por la Policía Nacional fueron compradas directamente por el Ministerio del Interior. Según las solicitudes de acceso a la información pública realizadas por TEDIC entre agosto y septiembre de 2023[85], otras entidades públicas, como municipalidades, gobernaciones y diversas direcciones, confirmaron que también han adquirido cámaras que están conectadas al sistema del 911.

Las instituciones que respondieron afirmativamente a la consulta respecto al uso de la tecnología de reconocimiento facial se encuentran en la Tabla 5.

TABLA 6. Instituciones que reconocieron tener tecnología de reconocimiento facial

Administración Nacional de Navegación y Puertos (ANNP)
Dirección Nacional de Migraciones
Gobernación de Itapúa
Municipalidad de Paraguarí
Cámara de Senadores
Dirección Nacional de Aeronáutica Civil (DINAC)

Asimismo, varias administraciones departamentales, además de entidades binacionales, afirmaron que adquirieron cámaras que fueron conectadas al sistema de 911. Estas instituciones son las gobernaciones de Presidente Hayes, Boquerón y Caaguazú, así como la Entidad Binacional Yacyretá, el Ministerio de Hacienda, Secretaría Nacional Antidrogas (SENAD) y el Ministerio de Justicia, totalizando 13.

85 Portal Unificado de Acceso a la Información Pública. (n.d.). Solicitudes de información pública. Recuperado de https://informacionpublica.paraguay.gov.py/portal/

Las compras de cámaras de circuito cerrado o de vigilancia, con o sin reconocimiento facial, no se hicieron solamente a través de los Fondos de Servicios Universales (FSU) sino también a través de las mismas instituciones y fueron publicadas en la Página Nacional de Contrataciones Públicas.

Para analizar en mayor detalle cómo evolucionaron las compras hechas por estas instituciones estatales, a continuación se encuentra el desglose de cada uno de los procesos realizados y las observaciones o inquietudes que parten de ellas.

En abril de 2012, la Policía Nacional realizó una contratación directa, a través de la convocatoria Nº 240169, en el cual fue adjudicada la empresa Visual Soluciones Informáticas SRL, sin embargo, en la Dirección Nacional de Contrataciones Públicas no aparece la lista de oferentes. (Dirección Nacional de Contrataciones Públicas, 2012a).

El monto adjudicado es de ₲ 110.000.000 (USD 14.968), para la adquisición de 32 cámaras de circuito cerrado, de tres tipos diferentes. Esta compra se hizo a través de la Categoría 24 de Equipos, accesorios y programas computacionales, de oficina, educativos, de imprenta, de comunicación y señalamiento.

En noviembre de 2014, CONATEL llevó a cabo un concurso de ofertas para la modernización del circuito cerrado a través de la licitación Nº 271004. En este proceso participaron seis empresas: Bullers Sociedad Anónima, Cellular SA, Central Inalámbrica de Monitoreo de Alarmas Sociedad Anónima, Data Lab SA, Diego Joaquín Rodríguez Barrios y Progress Fábrica de Software S.R.L (Dirección Nacional de Contrataciones Públicas, 2014). La empresa seleccionada fue TSV Del Paraguay S.R.L. CONATEL adquirió 44 cámaras de circuito cerrado, correspondientes a tres ítems, por un total de ₲ 164.020.083 (USD 22.318).

En noviembre de 2015, la Policía Nacional realizó una compra directa para un Sistema de Circuito Cerrado de Video Vigilancia mediante la licitación Nº 287860. En este proceso se presentaron Hugo Félix Benítez Peralta y Jorge Eduardo Colnago Barrios, siendo la adjudicación otorgada a Colnago Barrios. La compra incluyó 16 cámaras, por un total de ₲ 117.990.000 (USD 16.055) (Dirección Nacional de Contrataciones Públicas, 2015).

En diciembre de 2015, la Policía Nacional adquirió cámaras de circuito cerrado para el Departamento de Identificaciones mediante la licitación Nº 231138 (Dirección Nacional de Contrataciones Públicas, 2012b). La compra directa, adjudicada a Comtel Sociedad Anónima por ₲ 129.340.000 (USD 17.599), no incluyó una lista de oferentes.

En abril de 2021, la Policía Nacional llevó a cabo una contratación directa para la compra de un circuito cerrado mediante la licitación Nº 392828. Se adquirieron 16 cámaras por un total de ₲ 18.882.000 (USD 2.569). Cuatro firmas presentaron ofertas: José Antonio Duarte Santa Cruz, Online Paraguay S.A., Security Systems Paraguay S.A. y Tes Ingeniería S.A., siendo adjudicada esta última (Dirección Nacional de Contrataciones Públicas, 2021). Curiosamente, esta compra se realizó bajo la Categoría 22 - Maquinarias, Equipos y herramientas mayores - Equipos de transporte.

En esta investigación llama la atención que esta compra se hizo a través de la Categoría 22 - Maquinarias, Equipos y herramientas mayores - Equipos de transporte. Hasta ese momento, las compras de cámaras a través de la DNCP eran sin explicitar que sean con tecnología especializada de reconocimiento facial, lo cual no significa que no puedan ser integradas a un sistema de monitoreo con procesamiento de rostros a pesar de contar con menor resolución y por tanto, mayores obstáculos en la detección.

Desde noviembre de 2022, las instituciones del Estado comenzaron a realizar compras de tecnología con reconocimiento facial a través de la DNCP. El Ministerio del Interior llevó a cabo una Licitación Nº 419935, y en diciembre de 2022, CONATEL convocó a una Licitación Pública Nacional Nº 419105 (Dirección Nacional de Contrataciones Públicas, 2022b, 2022c).

Ambas licitaciones se orientaron a adquirir tecnología con capacidad de reconocimiento facial, como se detalla en la siguiente sección sobre litigios estratégicos. Esto permite resaltar que los llamados y las compras hechas por las distintas instituciones intervinientes, presentan una dificultad en el acceso a la información, considerando que las instituciones públicas no categorizan ni titulan correctamente las licitaciones relacionadas con la adquisición de cámaras de reconocimiento facial, lo que torna compleja su búsqueda en la base de datos pública de la Dirección Nacional de Contrataciones Públicas (DNCP). Es decir, la información existe, pero es de difícil acceso. Esta dificultad genera inquietudes en relación a la transparencia en la información proveída en estos procesos.

Además, es posible destacar incoherencias en la clasificación de licitaciones, ya que la compra de equipos de seguridad y cámaras no se clasifican adecuadamente en las categorías correspondientes. Por ejemplo, licitaciones que incluyen tecnología de seguridad se colocan en categorías relacionadas con equipos de oficina o programas computacionales.

La incorrecta clasificación de las licitaciones no sólo dificulta el acceso a los datos, sino que también sugiere una falta de criterios unificados en el uso de tecnología de seguridad, lo que podría llevar a una gestión desorganizada y opaca de los recursos.

Asimismo, entre los hallazgos resalta la interconexión de las cámaras entre distintas instituciones, lo cual demuestra que no sólo el Ministerio del Interior realiza compras en materia de equipos de seguridad para el sistema 911. Es posible confirmar que otras instituciones como municipalidades, gobernaciones y entidades públicas también han adquirido cámaras que son conectadas al sistema 911, con lo cual no sólo amplían el uso del reconocimiento facial a lo largo y ancho del país, sino que también generan deliberadamente un mayor obstáculo rastrear la compra e instalación de este tipo de tecnologías.

Análisis de informes oficiales

En el marco de la investigación, que además de monitorear las compras y donaciones descritas más arriba, busca evaluar la efectividad de la tecnología de reconocimiento facial en la mejora de la seguridad ciudadana. Para eso, TEDIC solicitó a la Policía Nacional, a través del portal unificado de acceso a la información pública, detalles sobre los resultados de la inversión multimillonaria en esta tecnología. La solicitud se centró en obtener datos sobre las detenciones realizadas gracias al uso de esta tecnología. Aunque la información proporcionada no especifica directamente el número de detenciones, sí incluye cifras de las alertas generadas anualmente desde la implementación de las cámaras y el software de reconocimiento facial, que se presentan a continuación:

TABLA 7. Alertas arrojada por cámaras de Reconocimiento facial

Mes	2019	2020	2021	2022	2023
Enero	0	20	1	0	0
Febrero	0	11	0	1	1
Marzo	0	13	1	0	0
Abril	0	0	0	1	0
Mayo	0	0	1	0	0
Junio	0	0	2	0	0
Julio	0	1	0	1	0
Agosto	0	0	1	0	0
Septiembre	0	1	4	1	-
Octubre	0	0	1	1	-
Noviembre	26	1	5	0	-
Diciembre	40	1	1	0	-
Total	**66**	**48**	**17**	**5**	**1**

Fuente: Policía Nacional del Paraguay, 2023.

En ese contexto, es necesario recordar que en el período comprendido entre 2018 y 2022, la CONATEL realizó adjudicaciones que ascienden a un monto de ₲ 28.590.880.000 para comprar infraestructura, cámaras y software de reconocimiento facial al servicio del 911.

Sin embargo, es importante destacar que, a pesar de la inversión sustancial realizada en esta tecnología, los resultados obtenidos, en materia de alertas para detener a sospechosos o criminales, hasta agosto de 2023, son modestos. Según las cifras proporcionadas por la dirección de Prevención y Seguridad del Centro de Seguridad y Emergencias, durante un periodo de cinco años, apenas se generaron 137 alertas mediante el uso de cámaras de reconocimiento facial. (Policía Nacional del Paraguay, 2023)

Este dato nos lleva a realizar un cálculo significativo: el costo de cada alerta generada a través de esta tecnología asciende en promedio a la cifra de ₲ 208.692.554 para el Estado. Es innegable que este costo por alerta es considerablemente elevado y plantea interrogantes sobre la eficacia de este tipo de inversiones en términos de seguridad pública y si permite realmente lograr el objetivo expresado. Adicionalmente, cabe mencionar que durante el mismo período, se realizaron un total de 7.590 solicitudes de acceso a grabaciones de cámaras de seguridad. (Policía Nacional del Paraguay, 2023)

Es importante destacar que, ya en 2019, una nota publicada por el diario ABC Color señalaba que la empresa TSV SRL se había consolidado como la "eterna proveedora" de cámaras de reconocimiento facial para la Policía Nacional a través de CONATEL. (ABC Color, 2019). Además, la publicación cuestionaba el funcionamiento de estos dispositivos y subrayaba su nula efectividad para detener personas hasta ese momento:

> "Existen dudas del funcionamiento óptimo de las cámaras pues ante el alto índice de robos y asaltos, no se ven muchas capturas de sospechosos. Además, ni una sola detención se produjo el año pasado por influencia de la nueva tecnología. En varias oportunidades ABC solicitó visitar la central de monitoreo para ver su operatividad, pero le negaron con el argumento del "riesgo de seguridad pública".

Entre noviembre de 2019 y marzo de 2020, los sistemas de reconocimiento facial emitieron 110 alertas. Sin embargo, desde abril de 2020 hasta agosto de 2023, solo se registraron 27 alertas, de las cuales apenas una corresponde a 2023.

Aunque la tecnología de reconocimiento facial puede ser útil en situaciones específicas, como la identificación de criminales peligrosos buscados por autoridades nacionales e internacionales, las estadísticas de la Policía Nacional revelan que, a nivel local, los resultados son mínimos y casi insignificantes. Además, estas cifras no consideran los problemas de discriminación y sesgos inherentes a esta tecnología, los cuales fueron abordados en los apartados de otros países, evidenciando aún más las limitaciones y riesgos de su implementación en contextos de seguridad ciudadana.

Estos resultados cuestionan la necesidad de continuidad del uso de tecnologías de reconocimiento facial en el ámbito de la seguridad pública, dado que los beneficios obtenidos son escasos y no justifican el riesgo de comprometer el cumplimiento de las convenciones internacionales ratificadas por Paraguay, como se mencionó anteriormente.

LITIGIOS ESTRATÉGICOS SOBRE RECONOCIMIENTO FACIAL

TEDIC realiza litigios estratégicos[86] en temas de tecnología y derechos humanos a menudo ante el Poder Judicial paraguayo y Sistema Interamericano de los Derechos Humanos (SIDH). Actualmente se encuentra realizando litigios sobre el reconocimiento facial a nivel nacional, para cuestionar el uso desproporcionado e invasivo de esta tecnología en Paraguay, y proteger los derechos a la privacidad, la no discriminación y la libertad de expresión de la ciudadanía, promoviendo marcos regulatorios más justos y respetuosos de los derechos humanos.

TEDIC ha realizado tres litigios estratégicos sobre el objeto de estudio, uno en 2018 y otros dos en 2023, ambos a través de amparos de acceso a la información. En los tres casos, las instituciones públicas se negaron a proporcionar la información solicitada sobre la implementación y uso de estos sistemas, lo que motivó las acciones legales para exigir transparencia y rendición de cuentas.

Primer litigio: Año 2018

En julio de 2018, el Ministerio del Interior y la Policía Nacional iniciaron un proceso de modernización del Sistema 911 en Asunción y el Área Metropolitana como se explica en los apartados correspondientes a las donaciones y adquisiciones de la implementación de cámaras de reconocimiento facial. En 2019, Maricarmen Sequera, abogada y representante de TEDIC, solicitó información al Ministerio del Interior sobre este proyecto a través del Portal Unificado de Acceso a la Información Pública. La respuesta del Ministerio, el 26 de abril de 2019, fue parcial, negándose a brindar información clave alegando confidencialidad[87].

Ante esta negativa, Sequera presentó un amparo invocando la Ley 5282/2014 y la Acordada 1005/2015 de la Corte Suprema de Justicia, con el fin de exigir la entrega de los datos solicitados. El caso fue llevado al IX Juzgado Penal de Garantías de la Capital, donde la solicitud fue desestimada en primera instancia, decisión que luego fue confirmada por el Tribunal de Apelación Penal.

La resolución judicial[88] refleja una preocupante realidad: los órganos estatales aplican las normas legales de manera selectiva, cumpliendo unas y omitiendo otras según su conveniencia, afectando gravemente los derechos humanos. Lo más alarmante es que los jueces, quienes deberían velar por el respeto a las leyes, terminan legitimando estas prácticas. Un ejemplo es la sentencia Nro. 70 del 25 de agosto de 2019, en la que se admite que no se especificó la ley que declara secreta la resolución 238, pero se justifica la negativa bajo el argumento de que la Policía Nacional, como órgano de seguridad interna del Estado, puede considerar su información como reservada según el artículo 175 de la Constitución Nacional.

Este razonamiento permite que cualquier acción de la Policía Nacional sea calificada como de seguridad nacional, sin un sustento normativo claro, replicando prácticas de la época dictatorial que la Constitución Nacional buscó erradicar. Así, se abre una peligrosa ventana que amenaza el estado de derecho y revive lógicas autoritarias que la sociedad paraguaya se ha comprometido a superar.

---

86 Los litigios estratégicos son herramientas legales que buscan provocar cambios sociales y normativos más amplios a través de casos específicos presentados en tribunales. No se trata solo de ganar un juicio, sino de desafiar leyes, políticas o prácticas que vulneran derechos fundamentales, buscando influir en la legislación y en la percepción pública.

87 TEDIC. 2019. ¿Quién vigila al vigilante? Reconocimiento facial en Asunción. Disponible en: https://www.tedic.org/quien-vigila-al-vigilante-reconocimiento-facial-en-asuncion/

88 Sentencia 70 -2019 – Amparo constitucional promovido por Maricarmen Sequera Buzarquis bajo patrocinio de los abogados Federico Legal Aguilar y Ezequiel F. Santagada c/Ministerio del Interior 2019-609. Disponible en: https://www.tedic.org/wp-content/uploads/2019/09/Sentencia-de-la-camara_rechazo-a-amparo-MDI_-2019-09-02-09.01.10.pdf

Luego de la segunda apelación, Sequera y su defensa decidieron llevar el caso a la última instancia. En 2019, recurrieron a la Corte Suprema de Justicia para solicitar una revisión de la sentencia y reafirmar el derecho de acceso a la información pública, insistiendo en que la negativa injustificada de las instituciones estatales vulnera derechos fundamentales y sienta un peligroso precedente. Recién en el 2024, luego de 5 años, la Sala Constitucional de la Corte Suprema de Justicia (CSJ) ha resuelto por unanimidad, mediante el Acuerdo y Sentencia Nº 843 del 7 de agosto de 2024, declarar la inconstitucionalidad del Acuerdo y Sentencia Nº 70/2019 del Tribunal de Apelación en lo Penal de la Capital, Cuarta Sala[89].

En dicha resolución, la CSJ ratificó la constitucionalidad de la Acordada Nº 1005, dictada por ella misma, la cual regula el procedimiento del amparo en casos de denegación de acceso a la información pública. En la misma se resolvió que la decisión del Tribunal de Apelación fue arbitraria y que efectivamente es el amparo la vía procesal regulada para iniciar juicios en esta materia.

La resolución dictada por la CSJ establece un precedente relevante respecto de la Acordada Nº 1005 y genera una nueva oportunidad para que la justicia avance en el derecho fundamental de acceso a la información, sobre un tema sensible relacionado con cómo el Estado trata nuestra información personal para fines de seguridad nacional.

Segundo litigio: Ministerio del Interior (2023)

Nuevamente, en 2023, Leonardo Gómez, miembro de TEDIC realizó nuevos pedidos formales a varias instituciones estatales para obtener información acerca de las cámaras equipadas con reconocimiento facial, y entre ellas, al Ministerio del Interior, en el caso de esta última, la respuesta ha sido nuevamente negativa, amparándose en el único apartado de esta ley que se refiere a la información reservada.

En 2023, TEDIC realizó 41 solicitudes de acceso de información a instituciones públicas, que abarcan ministerios, secretarías, gobernaciones y municipalidades (Ver tabla 3). De estas, 30 respondieron a la consulta. Entre las que respondieron, 20 confirmaron la existencia de cámaras de seguridad en sus instalaciones. No obstante, sólo cinco de estas instituciones admitieron contar con sistemas de reconocimiento facial en dichas cámaras[90].

TEDIC, en un esfuerzo por obtener la información requerida, solicitó la reconsideración del pedido de acceso a información pública realizada al Ministerio del Interior, que fue respondida de manera negativa. La justificación que ofrecieron se basó en que estos datos podrían ser clasificados como información pública de carácter reservado y que su divulgación podría afectar el servicio y la protección de los datos personales de los ciudadanos.

Es crucial señalar que la solicitud de información no requería datos personales, sino más bien información pública relacionada con cámaras que almacenan datos personales de la ciudadanía y que operan en espacios públicos.

89 El documento se encuentra pasa su consulta en la web de la Corte Suprema de Justicia: https://www.csj.gov.py/jurisprudencia/home/DocumentoJurisprudencia?codigo=106501

90 Portal Unificado de Acceso a la Información Pública. (n.d.). Solicitudes de información pública. Recuperado de https://informacionpublica.paraguay.gov.py/portal/

Adicionalmente, cabe mencionar que, aunque no se dispone de una cifra precisa sobre la cantidad de cámaras con reconocimiento facial ubicadas en distintos puntos del territorio nacional, las mismas autoridades estatales han anunciado constantemente la incorporación de más cámaras equipadas con esta tecnología. Esto plantea preguntas significativas sobre la expansión de la vigilancia y la necesidad de una revisión exhaustiva de las políticas y prácticas relacionadas con la privacidad y la transparencia en este contexto.

Ante la nueva respuesta negativa recibida en el marco de la reconsideración solicitada, TEDIC promovió un amparo judicial de acceso a la información pública contra el Ministerio del Interior. Para entender en dicho juicio, resultó sorteado el Juzgado de Primera Instancia en lo Civil y Comercial del 3º turno, Secretaría 5.

En primera instancia, el Juzgado a cargo resolvió rechazar el amparo promovido. Ante esta situación, TEDIC interpuso un recurso de apelación el cual confirmó la sentencia dictada por el Juzgado de primera instancia[91].

Frente a la situación de negación del derecho a acceder a información pública, el caso fue promovido a la Corte Suprema de Justicia y se encuentra en estudio ante la sala Constitucional, debido a que se presentó una acción de inconstitucionalidad contra las resoluciones negatorias dictadas en ambas instancias.

Tercer litigio: Policía Nacional (2023)

Paralelamente, TEDIC presentó un amparo contra la Policía Nacional en diciembre de 2023 para obtener estadísticas sobre el uso de tecnologías de reconocimiento facial, las cuales ya habían sido publicadas en parte en 2021 y sobre la cual se han expuesto hallazgos en esta investigación. La Policía se negó a proporcionar la información argumentando razones de "seguridad nacional", lo que TEDIC calificó como una extralimitación en sus funciones, ya que en ocasiones anteriores la misma información había sido divulgada sin problemas, evidenciando además la relevancia de su publicación para la labor periodística y el ejercicio del control ciudadano.

Este amparo fue presentado ante el Juzgado de Primera Instancia en lo Civil y Comercial del 19º turno. TEDIC enfrentó dificultades técnicas al intentar presentar una apelación, pero finalmente, el 1 de enero de 2024, logró presentarla. El 15 de enero de 2024, el Tribunal de Apelación falló a favor de TEDIC, declarando que la negativa de la Policía Nacional no estaba justificada y que el derecho de acceso a la información pública debe ser respetado, incluso en casos que involucran tecnologías de vigilancia[92].

El fallo destacó que invocar la "seguridad nacional" no puede ser un argumento generalizado para ocultar información que debe ser pública, lo que representa un triunfo y precedente importante a invocar en casos similares que acontezcan en adelante.

91 Corte Suprema de Justicia (2024). Acuerdo y sentencia N.º 5. "Tribunal de Apelación Civil y Comercial de la Capital. Quinta Sala. Juicio "Leonardo Gómez Berniga c/ Ministerio del Interior s/ Amparo". Año 2023 №469". Disponible en: https://www.pj.gov.py/descargas/transparencia/ID217F2-65e85a3cd4366-a-y-s-n-05-de-fecha-21-de-febrero-de-2024.pdf

92 Corte Suprema de Justicia (2024). Acuerdo y sentencia N.º 2. Tribunal de Apelación de Feria. Juicio "Leonardo Gómez Berniga c/ Policía Nacional s/ Amparo". Año 2023 N.º 395". Disponible en: https://www.pj.gov.py/descargas/transparencia/ID214F2-65e8627302a1d-a-y-s-n-02-de-fecha-15-de-enero-de-2024.pdf

Tras esta situación, desde TEDIC hemos instado al Juzgado donde inició el expediente que haga cumplir la sentencia y, el 15 de abril del 2024, el Departamento del Sistema 911 proveyó un informe con la información solicitada, revelando la existencia de 1641 cámaras instaladas a nivel país bajo control de la Policia Nacional (ver cifras informadas en el Anexo I).

CONCLUSIÓN

La revisión metodológica realizada mediante diversos procedimientos ha permitido obtener una visión integral sobre la adquisición y uso de tecnología de reconocimiento facial por parte del Estado paraguayo. Se emplearon revisiones documentales de leyes e información tanto nacionales como internacionales, búsquedas en la página oficial de la Dirección Nacional de Contrataciones Públicas (DNCP) y la Comisión Nacional de Telecomunicaciones (CONATEL), así como solicitudes de acceso a la información, para recopilar datos relevantes y actualizados.

Los resultados de esta investigación revelan que las disposiciones normativas vigentes no determinan claramente la responsabilidad sobre el funcionamiento de los equipos de reconocimiento facial, incluyendo su operación, reparación, tratamiento de datos recolectados, seguridad de los datos y la integridad de los funcionarios y la institución ante el mal uso de los equipos y datos personales.

Este aspecto es crucial, ya que los equipos son adquiridos con fondos de municipalidades, gobernaciones y otras instituciones estatales ajenas a la Policía Nacional, lo que plantea interrogantes sobre la titularidad de los equipos y de sus respectivos mantenimientos.

La ausencia de una ley integral de protección de datos personales en Paraguay, combinada con una comprensión deficiente de los principios garantistas penales y normativas de derechos humanos, plantea serias amenazas a la protección de datos.

La implementación de tecnologías de reconocimiento facial representa un riesgo para la calidad democrática y la seguridad de la población, afectando negativamente el ejercicio de sus libertades civiles. En paralelo, las compras realizadas por CONATEL mediante el Fondo de Servicios Universales (FSU) muestran un desvío considerable de su propósito original, que era reducir las brechas de conectividad, las cuales aún persisten significativamente. Este desvío, justificado en su momento como excepcional, ha derivado en una práctica recurrente, sin que se presenten resoluciones especiales que respalden dichas adquisiciones.

Además, la investigación revela un incremento en la compra de cámaras con tecnología de reconocimiento facial, financiadas mediante grandes inversiones. Sin embargo, esto contrasta con la limitada efectividad de esta tecnología para prevenir delitos o identificar a los responsables, según lo expuesto en el informe.

Estos procesos también exponen una preocupante falta de diversificación en la selección de proveedores, dado que la empresa TSV Del Paraguay S.R.L. ha sido elegida en múltiples ocasiones. Las especificaciones de algunas compras de software de reconocimiento facial incluyen capacidades para no sólo reconocer rostros, sino también mantener una base de datos y permitir la inclusión de nombres en una “lista negra”. Esto, junto con la instalación de cámaras en espacios de protesta social, pone en riesgo la democracia y la libertad de ejercer el derecho a manifestarse.

Por otra parte, la incorrecta clasificación de las licitaciones dificulta el acceso a los datos y además sugiere una falta de criterios unificados en el uso de tecnología de seguridad, lo que podría llevar a una gestión desorganizada y opaca de los recursos. Además, la interconexión de las cámaras entre diversas instituciones, como municipalidades, gobernaciones y otras entidades públicas, amplía el uso del reconocimiento facial a lo largo y ancho del país, representando un mayor obstáculo para rastrear la compra e instalación de este tipo de tecnologías.

Aunque la tecnología de reconocimiento facial puede ser útil en situaciones específicas, como la identificación de criminales peligrosos buscados por autoridades nacionales e internacionales, las estadísticas de la Policía Nacional revelan que, a nivel local, los resultados son mínimos y casi insignificantes. Además, estas cifras no consideran los problemas de discriminación y sesgos inherentes a esta tecnología, los cuales fueron abordados en los apartados de otros países, evidenciando aún más las limitaciones y riesgos de su implementación en contextos de seguridad ciudadana.

Estos resultados cuestionan la necesidad de continuidad del uso de tecnologías de reconocimiento facial en el ámbito de la seguridad pública, dado que los beneficios obtenidos son escasos y no justifican el riesgo de comprometer el cumplimiento de las convenciones internacionales ratificadas por Paraguay, como se mencionó anteriormente.

Esta investigación hizo evidente además la poca colaboración de algunas instituciones, como la Policía Nacional, para ofrecer información sobre la compra de cámaras y la instalación de las mismas. La justificación ofrecida se basó en que estos datos podrían ser clasificados como información pública de carácter reservado, y que su divulgación podría afectar el servicio y la protección de los datos personales de los ciudadanos. No obstante, es crucial señalar que la solicitud de información no requería datos personales, sino información pública relacionada con cámaras que almacenan datos personales de la ciudadanía y que operan en espacios públicos.

Adicionalmente, aunque no se dispone de una cifra precisa sobre la cantidad de cámaras con reconocimiento facial ubicadas en distintos puntos del territorio nacional, las autoridades estatales han anunciado constantemente la incorporación de más cámaras equipadas con esta tecnología. Esto plantea preguntas significativas sobre la expansión de la vigilancia y la necesidad de una revisión exhaustiva de las políticas y prácticas relacionadas con la privacidad y la transparencia en este contexto.

RECOMENDACIONES

1. **Desarrollar un marco legal integral para la protección de datos personales:**

   Paraguay debe establecer una ley de protección integral de datos personales que regule el uso de tecnologías de vigilancia, incluyendo el reconocimiento facial. Esta ley debe garantizar la privacidad y seguridad de los datos almacenados, así como establecer responsabilidades claras para las instituciones que manejan los mismos.

2. **Mejorar la transparencia y accesibilidad de la información:**

   Las instituciones públicas deben categorizar y titular correctamente las licitaciones relacionadas con la adquisición de cámaras de reconocimiento facial. Esto facilitará el acceso a la información y mejorará la transparencia en los procesos de compra y uso de estas tecnologías.

3. **Diversificar la selección de proveedores:**

   Es recomendable diversificar la selección de proveedores para evitar la concentración de contratos en una sola empresa. Esto promoverá la competencia y además educirá el riesgo de corrupción y mejorará la calidad de los equipos adquiridos.

4. **Realizar auditorías independientes:**

   El Estado debe convocar auditorías independientes y periódicas de los sistemas de reconocimiento facial para evaluar su efectividad y detectar posibles sesgos o problemas de discriminación. Los resultados de estas auditorías deben ser públicos y utilizados para mejorar las políticas y prácticas de vigilancia.

5. **Limitar el uso de tecnologías de videovigilancia a fines específicos y legítimos:**

   El Estado debe articular los mecanismos adecuados para limitar el uso de tecnologías de videovigilancia, incluyendo el reconocimiento facial, a fines específicos y determinados, de manera proporcional y bajo estricta supervisión.

6. **Implementar mecanismos de supervisión y rendición de cuentas:**

   Se debe determinar una autoridad administrativa encargada de supervisar el uso de la tecnología de videovigilancia y reconocimiento facial, a fin de que ésta disponga los mecanismos técnicos y documentales de rendición de cuentas por parte de los operadores, con capacidad de auditar el funcionamiento y facultad sancionatoria a quienes se aparten del marco regulador.

7. **Diseñar mecanismos que bloqueen el uso discriminatorio:**

   El Estado debe implementar mecanismos y salvaguardias que permitan asegurar las limitaciones en el uso de la tecnología de videovigilancia y reconocimiento facial, mediante revisiones periódicas y medidas de trazabilidad del uso, a fin de evitar que sean utilizados con fines distintos a los originales.

REFERENCIAS BIBLIOGRÁFICAS

1. Alliance for Affordable Internet. (2021). Fondo de Servicio Universal en América Latina y el Caribe. https://a4ai.org/wp-content/uploads/2022/01/2021-12-16-Universal-Service-and-Access-Funds-SPANISH-Report.pdf

2. Alonzo,L , Carrillo, E y Sequera, M . (2018). TEDIC. La enajenación continua de nuestros derechos. Sistemas de identidad: Biometría y cámaras de vigilancia no reguladas en Paraguay. TEDIC. https://www.tedic.org/la-enajenacion-continua-de-nuestros-derechos-sistemas-de-identidad-biometria-y-camaras-de-vigilancia-no-reguladas-en-paraguay/

3. Access Now. (2021). Hecha en el exterior, utilizada en casa. https://www.accessnow.org/wp-content/uploads/2021/09/vigilancia-latam-espa.pdf

4. Al Sur. (2021). Reconocimiento facial en América Latina. https://www.alsur.lat/sites/default/files/2021-11/ALSUR_Reconocimiento_facial_en_Latam_ES.pdf

5. EFF. (s.f). Necessary and proportionate on the application of human rights to commmunications surveillance. Disponible en: https://necessaryandproportionate.org/

6. García Zaballos, A., Huici, H., Puig Gabarró, P., & Iglesias Rodriguez, E. (2021). Cerrando la brecha de conectividad digital: Políticas públicas para el servicio universal en América Latina y el Caribe. Inter-American Development Bank. https://doi.org/10.18235/0003066

7. Holden, L. (2023). Divisions Grow Over Use of Facial Recognition in California. GovTech. https://www.govtech.com/policy/divisions-grow-over-use-of-facial-recognition-in-california

8. International Network of Civil Liberties Organizations. (2021). Te están mirando. Resistencias frente a las vulneraciones de derechos por sistemas de reconocimiento facial en el mundo. https://files.inclo.net/content/pdf/4/Spanish%20Report.pdf

9. Marianne Díaz. (2018). El cuerpo como dato. Derechos Digitales. https://www.derechosdigitales.org/wp-content/uploads/cuerpo_DATO.pdf

10. Privacy International. 2013. Biometrics: friend or foe of privacy. Disponible en: https://www.privacyinternational.org/news-analysis/1409/biometrics-friend-or-foe-privacy

11. Rolon, J y Sequera, M. (2015). TEDIC.Vigilancia estatal de las comunicaciones y derechos fundamentales en Paraguay

12. TEDIC. (2023). La filtración de datos policiales en Paraguay y una imperante urgencia de respuestas [Página institucional]. https://www.tedic.org/la-filtracion-de-datos-policiales-en-paraguay-y-una-imperante-urgencia-de-respuestas/

MEDIOS DE COMUNICACIÓN CONSULTADOS

13. ABC Color. (2019). TSV SRL es la eterna proveedora tecnológica del 911 de la Policía. https://www.abc.com.py/edicion-impresa/economia/2019/11/11/tsv-srl-es-la-eterna-proveedora-tecnologica-del-911-de-la-policia/

14. IP Paraguay. (2021, marzo 9). Policía tiene identificadas a personas que cometieron desmanes mediante Sistema 911. .::.::Agencia IP::. https://www.ip.gov.py/ip/policia-tiene-identificadas-a-personas-que-cometieron-desmanes-mediante-sistema-911/

15. La Nación. (2022). De 1.447 cámaras instaladas que tenía la Policía se redujeron a 640. https://www.lanacion.com.py/investigacion/2022/10/18/de-1447-camaras-instaladas-que-tenia-la-policia-se-redujeron-a-640/

16. Última Hora. (2023, julio 13). De 8.900 escuelas, apenas 2.055 tienen conexión a internet este año [Medio de Comunicación]. Última hora. https://www.ultimahora.com/de-8-900-escuelas-apenas-2-055-tienen-conexion-a-internet-este-ano

NORMATIVAS E INSTRUMENTOS INTERNACIONALES

17. Asamblea General (ONU). 2018. El derecho a la privacidad en la era digital. Informe del Alto Comisionado de las Naciones Unidas para los Derechos Humanos. A/HRC/39/29. 2018. https://documents.un.org/doc/undoc/gen/g18/239/61/pdf/g1823961.pdf

18. Convención Americana sobre Derechos Humanos – pacto de San José. (1969). https://www.oas.org/dil/esp/1969_Convenci%C3%B3n_Americana_sobre_Derechos_Humanos.pdf

19. Declaración Universal de los Derechos Humanos, (1948). http://www.ohchr.org/EN/UDHR/Documents/UDHR_Translations/spn.pdf

20. Pacto Internacional de los Derechos Civiles y Políticos, (1966). http://www.ohchr.org/SP/ProfessionalInterest/Pages/CCPR.aspx

21. OEA. Departamento de Derecho Internacional. Secretaría de Asuntos Jurídicos. (2023). Principios actualizados sobre la privacidad y la protección de datos personales. Secretaría de Asuntos Jurídicos de la Organización de los Estados Americanos.

22. ONU – CCPR. 1999. Comentario general 27. https://www.acnur.org/fileadmin/Documentos/BDL/2001/1400.pdf

23. ONU. 2013. Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue* A/HRC/23/40. ONU. Abril, 2013.

24. ONU. 2019. Informe del Relator Especial sobre la promoción y protección de los derechos humanos y las libertades fundamentales en la lucha contra el terrorismo, Martin Scheinin, 2009, P.10-11. Disponible en: http://www2.ohchr.org/english/bodies/hrcouncil/docs/13session/A-HRC-13-37.pdf

25. OEA, 2022. Informe anual de la Relatoría Especial para la Libertad de Expresión: Informe anual de la Comisión Interamericana de Derechos Humanos. Disponible en: https://www.oas.org/es/cidh/expresion/informes/IA2022ESP.pdf

26. ONU, 2019. La vigilancia y los derechos humanos. Informe del Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y de expresión. Disponible en: https://documents.un.org/doc/undoc/gen/g19/148/79/pdf/g1914879.pdf

NORMATIVAS, LEYES, RESOLUCIONES Y DOCUMENTOS OFICIALES

27. CONATEL. (2000). Resolución No 495.

28. CONATEL. (2018). Contrato No 27/2018. https://contrataciones.gov.py/licitaciones/convocatoria/328038-adquisicion-sistemas-camaras-vigilancia-lpn-07-sbe-2017-1.html

29. CONATEL. (2019). Contrato No 50/2019. https://www.conatel.gov.py/conatel/wp-content/uploads/2020/03/contrato-n-0050-2019-para-el-otorgamiento-de-subsidio-a-traves-del-fsu-para-la-implementacion-del-servicio-de-atencion-y-despacho-de-llamadas.pdf

30. CONATEL. (2020). Contrato No 7/2020. https://www.conatel.gov.py/conatel/wp-content/uploads/2021/11/contrato-n-07-2020-proseco.pdf

31. CONATEL. (2021). Nota PR 315/2021. https://www.conatel.gov.py/conatel/wp-content/uploads/2021/09/pr-315-2021-ministerio-del-interior.pdf

32. CONATEL. Contrato № 03/21. (2021). [Página oficial]. //www.conatel.gov.py/conatel/wp-content/uploads/2021/11/contrato_n3_2021_tsv_cse_villarrica.pdf

33. CONATEL. (2022a). Contrato No 13/2022. https://www.conatel.gov.py/conatel/wp-content/uploads/2022/08/contrato_13-2022_consorcio_voxingenieria_chaco2022_1.pdf

34. CONATEL. (2022b). Contrato No 37/2022. https://www.conatel.gov.py/conatel/wp-content/uploads/2023/01/contrato-n-37-2022-sanlo.pdf

35. Congreso Nacional (1995) Ley 642 /1995 De Telecomunicaciones

36. https://www.bacn.gov.py/leyes-paraguayas/2452/ley-n-642-telecomunicaciones

37. Congreso Nacional. (2012). Ley 4739/12—Que crea El Sistema 911 de Atención, Despacho y Seguimiento de Comunicaciones de Emergencias. http://digesto.senado.gov.py/detalles&id=7947

38. Congreso Nacional (2020) Ley 6534/21 De protección de datos personales crediticios. https://www.bacn.gov.py/leyes-paraguayas/9417/ley-n-6534-de-proteccion-de-datos-personales-crediticios

39. Dirección Nacional de Contrataciones Públicas. (2012a, julio). Contrato de la Licitación 240169—Adquisición de Circuito Cerrado. https://contrataciones.gov.py/licitaciones/adjudicacion/contrato/240169-visual-soluciones-informaticas-s-r-l-1.html

40. Dirección Nacional de Contrataciones Públicas. (2012b, diciembre 7). Adjudicación de la Licitación 231138—ADQUISICIÓN DE EQUIPO DE CIRCUITO CERRADO PARA EL DEPARTAMENTO DE IDENTIFICACIONES. https://www.contrataciones.gov.py/licitaciones/adjudicacion/231138-adquisicion-equipo-circuito-cerrado-departamento-identifiaciones/resumen-adjudicacion.html

41. Dirección Nacional de Contrataciones Públicas. (2014, noviembre 22). Adjudicación de la Licitación 271004—MODERNIZACIÓN DEL CIRCUITO CERRADO. https://www.contrataciones.gov.py/licitaciones/adjudicacion/271004-modernizacion-circuito-cerrado/resumen-adjudicacion.html

42. Dirección Nacional de Contrataciones Públicas. (2015, diciembre 23). Adjudicación de la Licitación 287860—Sistema de circuito cerrado de video vigilancia. https://www.contrataciones.gov.py/licitaciones/adjudicacion/287860-sistema-circuito-cerrado-video-vigilancia-1/resumen-adjudicacion.html

43. Dirección Nacional de Contrataciones Públicas. (2021, junio 16). Adjudicación de la Licitación 392828—ADQUISICIÓN DE CIRCUITO CERRADO. https://www.contrataciones.gov.py/licitaciones/adjudicacion/392828-adquisicion-circuito-cerrado-1/resumen-adjudicacion.html

44. Dirección Nacional de Contrataciones Públicas. (2022a, octubre 4). Planificación de la Licitación 419935—Actualización y Adquisición de Equipos para el Centro de Seguridad y Emergencias del Sistema 911 de la Policía Nacional para Asunción y Regionales Ad Referendum Plurianual. https://www.contrataciones.gov.py/licitaciones/planificacion/419935-actualizacion-adquisicion-equipos-centro-seguridad-emergencias-sistema-911-policia-1.html

45. Dirección Nacional de Contrataciones Públicas. (2022b, noviembre 28). Adjudicación de la Licitación 419935—Actualización y Adquisición de Equipos para el Centro de Seguridad y Emergencias del Sistema 911 de la Policía Nacional para Asunción y Regionales Ad Referendum Plurianual. https://www.contrataciones.gov.py/licitaciones/adjudicacion/419935-actualizacion-adquisicion-equipos-centro-seguridad-emergencias-sistema-911-policia-1/resumen-adjudicacion.html

46. Dirección Nacional de Contrataciones Públicas. (2022c, diciembre 12). Adjudicación de la Licitación 419105—ADQUISICIÓN DE EQUIPOS DE SEGURIDAD Y SISTEMAS DE CIRCUITO CERRADO CCTV. https://www.contrataciones.gov.py/licitaciones/adjudicacion/419105-adquisicion-equipos-seguridad-sistemas-circuito-cerrado-cctv-1/resumen-adjudicacion.html

47. Instituto Nacional de Estadística. (2023). Tecnología de la Información y Comunicación en el Paraguay (TIC). EPH 2015-2022. Instituto Nacional de Estadística. https://www.ine.gov.py/Publicaciones/Biblioteca/documento/226/Tecnolog%C3%ADa%20de%20la%20Informaci%C3%B3n%20y%20Comunicaci%C3%B3n%20EPH%202015_2022.pdf

48. Instituto Nacional de Estadística. (2023) Resultados preliminares del Censo de Población y Vivienda 2022. Disponible en https://www.ine.gov.py/censo2022/documentos/Revista_Censo_2022.pdf

49. Policía Nacional del Paraguay. (2014). Resolución CPN № 452. https://www.policianacional.gov.py/wp-content/uploads/2018/03/RESOLUCI%C3%93N-N%C2%B0-452-POR-LA-QUE-SE-APRUEBA-EL-NUEVO-REGLAMENTO-ORGANICO-FUNCIONAL-SISTEMA-911.pdf

50. Policía Nacional del Paraguay. (2023, octubre 16). Memorandum O.E.G No 10/2023. Respuesta de pedido de acceso a la información pública. https://informacionpublica.paraguay.gov.py/portal/#!/ciudadano/solicitud/74291

ANEXO

RESUMEN DE CÁMARAS A NIVEL PAÍS – ABRIL 2024

Capital

Ciudad	PTZ	Fijas	LPR	FR	Total
Asunción	448	261	28	12	749

Departamento Central

Ciudad	PTZ	Fijas	LPR	FR	Total
San Lorenzo	86	0	6	1	93
Fernando de la Mora	20	2	0	0	22
Luque	32	1	4	3	40
Lambaré	20	2	4	0	26
Ñemby	14	0	0	1	15
Capiatá	12	0	0	1	13
Mariano Roque Alonso	11	0	4	0	15
Itá	16	0	0	0	16
Villa Elisa	17	0	0	0	17
Total	228	5	18	6	257

Departamento de Cordillera

Ciudad	PTZ	Fijas	LPR	FR	Total
Caacupé	13	0	0	0	13
San Bernardino	18	0	4	2	24
Total	31	0	4	2	37

Departamento de Alto Paraná

Ciudad	PTZ	Fijas	LPR	FR	Total
Ciudad del Este	110	0	12	10	132

Departamento de Itapúa

Ciudad	PTZ	Fijas	LPR	FR	Total
Encarnación	88	56	10	10	164

Departamento de Caaguazú

Ciudad	PTZ	Fijas	LPR	FR	Total
Coronel Oviedo	35	0	0	0	35
Caaguazú	8	0	0	0	8
Total	43	0	0	0	43

Departamento de Misiones

Ciudad	PTZ	Fijas	LPR	FR	Total
San Juan Bautista	30	0	0	0	30
San Ignacio	30	0	6	0	36
Total	60	0	0	0	66

Departamento de Concepción

Ciudad	PTZ	Fijas	LPR	FR	Total
Concepción	38	0	0	0	38
Horqueta	15	0	0	0	15
Yby Yaú	10	0	0	0	10
Total	53	0	0	0	63

Departamento de Guairá

Ciudad	PTZ	Fijas	LPR	FR	Total
Villarrica	20	0	0	0	20

Departamento de Amambay

Ciudad	PTZ	Fijas	LPR	FR	Total
Pedro Juan Caballero	76	0	12	8	96

Departamento de Presidente Hayes

Ciudad	PTZ	Fijas	LPR	FR	Total
Villa Hayes - Peaje Remanso	0	0	6	0	6
Peaje Nueva Asunción - Chacoí	0	0	8	0	8
Total	0	0	14	0	14


Tecnología
& Derechos
Humanos