



ESTADO DE VIGILANCIA

LA EXPANSIÓN DEL USO DE TECNOLOGÍAS DE VIGILANCIA MASIVA POR
EL GOBIERNO DE ARGENTINA

AMNESTY
INTERNATIONAL



Amnistía Internacional es un movimiento integrado por 10 millones de personas que activa el sentido de humanidad dentro de cada una de ellas y que hace campaña en favor de cambios que permitan que todo el mundo disfrute de sus derechos humanos. Nuestra visión es la de un mundo donde quienes están en el poder cumplen sus promesas, respetan el derecho internacional y rinden cuentas. Somos independientes de todo gobierno, ideología política, interés económico y credo religioso, y nuestro trabajo se financia principalmente con las contribuciones de nuestra membresía y con donativos. Creemos que actuar movidos por la solidaridad y la compasión hacia nuestros semejantes en todo el mundo puede hacer mejorar nuestras sociedades.

Agradecimientos

Amnistía Internacional agradece a los socios, incluidas las organizaciones de la sociedad civil y los activistas, que han contribuido a esta investigación.

© Amnesty International 2026

Salvo cuando se indique lo contrario, el contenido de este documento está protegido por una licencia 4.0 de Creative Commons (atribución, no comercial, sin obra derivada, internacional).

<https://creativecommons.org/licenses/by-nc-nd/4.0/legalcode.es>

Para más información, visiten la página *Permisos* de nuestro sitio web:

<https://www.amnesty.org/es/permissions/>.

El material atribuido a titulares de derechos de autor distintos de Amnistía Internacional no está protegido por la licencia Creative Commons.

Publicado por primera vez en 2026

por Amnesty International Ltd.

Peter Benenson House, 1 Easton Street

London WC1X 0DW, Reino Unido



Ilustración de portada: Amnesty International / Celina Hilbert

Índice: AMR 13/1104/2026 Spanish

Idioma original: Inglés

amnesty.org

**AMNISTÍA
INTERNACIONAL**



ÍNDICE

1.RESUMEN EJECUTIVO	10
CONTEXTO: POLÍTICAS DE RECORTE Y REPRESIÓN DE LA PROTESTA SOCIAL	10
REFORMAS ESTRUCTURALES Y OPERATIVAS Y ADQUISICIÓN DE TECNOLOGÍAS DE VIGILANCIA	10
ADQUISICIÓN DE TECNOLOGÍAS DE VIGILANCIA	11
EL EFECTO INHIBIDOR DE LA VIGILANCIA	12
RESPONSABILIDADES CORPORATIVAS DE CLEARVIEW AI	12
RECOMENDACIONES PRINCIPALES	13
2.METODOLOGÍA	15
2.1 CONTEXTO, MÉTODOS Y ALCANCE DE ESTE ESTUDIO	15
2.2 HISTORIA DE LA VIGILANCIA EN ARGENTINA Y LA REGIÓN	18
2.3 VIGILANCIA MASIVA SIN CONTROL: RECONOCIMIENTO FACIAL DE PRÓFUGOS EN LA CIUDAD DE BUENOS AIRES	19
2.4 EXPERIENCIAS REGIONALES: AMÉRICA LATINA FRENTE A LA EXPANSIÓN DE LA VIGILANCIA MASIVA	20
3. ESTÁNDARES LEGALES APLICABLES AL USO DE TECNOLOGÍAS DE VIGILANCIA EN ARGENTINA	22
3.1 DERECHO A LA PRIVACIDAD Y PROTECCIÓN DE DATOS PERSONALES	23
3.3 LIBERTAD DE REUNIÓN PACÍFICA Y ASOCIACIÓN	24
3.4 DERECHO A LA IGUALDAD Y NO DISCRIMINACIÓN	24
3.5 TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PÚBLICA	26
3.6 ESTÁNDARES INTERNACIONALES NO PRESCRIPTIVOS Y DESARROLLOS RECIENTES	26
4. IMPACTOS EN LOS DERECHOS HUMANOS DE LAS TECNOLOGÍAS DE VIGILANCIA	27
4.1 RECONOCIMIENTO DE IMÁGENES Y BIOMETRÍA	27
4.2 PREDICCIÓN DE DELITOS Y DELIMITACIÓN DE ÁREAS DE VIGILANCIA	29
4.3 REVISIÓN DE REDES SOCIALES E INVESTIGACIÓN DE FUENTES ABIERTAS (OSINT)	30
5.POLÍTICAS Y TECNOLOGÍAS DE VIGILANCIA: UN NUEVO PARADIGMA	31

5.1 AMPLIACIÓN DEL ALCANCE DE INVESTIGACIÓN DEL SISTEMA DE INTELIGENCIA Y DE LAS FUERZAS FEDERALES	31
5.1.1 REFORMA DEL SISTEMA DE INTELIGENCIA NACIONAL	32
5.1.2 REFORMA DEL ESTATUTO DE LA POLICÍA FEDERAL	32
5.2 ELEMENTOS OPERATIVOS PARA IMPLEMENTAR LAS TAREAS DE VIGILANCIA INTERNA	33
5.2.2 LA UNIDAD DE INTELIGENCIA ARTIFICIAL APLICADA A LA SEGURIDAD (UIAAS)	34
5.2.3 EL PROTOCOLO DE “CIBERPATRULLAJE”	34
5.2.4 RECONOCIMIENTO FACIAL <i>EX POST</i> : EL PROTOCOLO DE RECONOCIMIENTO Y COMPARACIÓN FACIAL	35
6. ANÁLISIS DE COMPRAS Y CONTRATACIONES DE TECNOLOGÍAS DE VIGILANCIA	36
6.1 TECNOLOGÍAS ADQUIRIDAS POR EL GOBIERNO NACIONAL	37
6.1.1 VIGILANCIA DE FUENTES ABIERTAS Y DE REDES SOCIALES	37
6.2.2 PROCESAMIENTO DE IMÁGENES CON TECNOLOGÍAS DE RECONOCIMIENTO FACIAL	38
6.1.3 DRONES, ROBOTS Y VIGILANCIA AÉREA	40
6.1.4 ALGORITMOS PREDICTIVOS: HERRAMIENTAS DE REFUERZO DE ESTEREOTIPOS	41
6.2 TECNOLOGÍAS DE VIGILANCIA ADQUIRIDAS POR LA CIUDAD DE BUENOS AIRES: AUMENTO DE COBERTURA DE VIDEOVIGILANCIA Y NUEVAS TECNOLOGÍAS DE RECONOCIMIENTO FACIAL	42
6.2.1 ¿CÓMO SE TRADUCE ESTO EN UN ESCENARIO REAL DE PROTESTA EN LA CIUDAD DE BUENOS AIRES?	44
7. EL EFECTO INHIBIDOR: CUANDO LA PERCEPCIÓN DE LAS TECNOLOGÍAS DE VIGILANCIA AFECTA LOS DERECHOS DE LAS PERSONAS	48
7.1 EFECTO INHIBIDOR Y AJUSTES DEL COMPORTAMIENTO COMO RESULTADO DE LA VIGILANCIA	49
7.2 LA CONTRACCIÓN DEL ESPACIO DE REUNIÓN	50
7.3 AUTOCENSURA Y FALTA DE GARANTÍAS PARA LA LIBERTAD DE EXPRESIÓN	52
8. CONCLUSIONES Y RECOMENDACIONES INICIALES	55
8.1 AL GOBIERNO NACIONAL Y DE LA CIUDAD DE BUENOS AIRES:	56
8.2 AL GOBIERNO NACIONAL Y ESPECIALMENTE AL MINISTERIO DE SEGURIDAD:	58
8.3 AL CONGRESO DE LA NACIÓN:	58
8.4 A LOS ORGANISMOS REGIONALES E INTERNACIONALES DE DERECHOS HUMANOS	58
ANEXO 1 – DETALLE DE COMPRAS Y CONTRATACIONES	59
COMPRAS Y CONTRATACIONES DEL GOBIERNO NACIONAL	59
COMPRAS Y CONTRATACIONES DEL GOBIERNO DE LA CIUDAD DE BUENOS AIRES	60
MONTOS ADQUISICIÓN DE PUNTOS DE CAPTURA BAJO RESOLUCIONES DE AMPLIACIÓN CABA	63

ÍNDICE DE TABLAS

TABLA 1: PEDIDOS DE ACCESO A LA INFORMACIÓN PÚBLICA SOBRE TECNOLOGÍAS DE VIGILANCIA	16
TABLA 2: COMPRAS Y CONTRATACIONES DE TECNOLOGÍA POR PARTE DEL MINISTERIO DE SEGURIDAD NACIONAL.	36
TABLA 3: CONTRATACIÓN DE INFRAESTRUCTURA PARA LA VIGILANCIA POR EL GOBIERNO DE LA CABA.	42
TABLA 4: REQUERIMIENTOS PARA LAS CÁMARAS DE VIDEOVIGILANCIA DEL GOBIERNO DE LA CIUDAD DE BUENOS AIRES 2024-2025, SEGÚN REQUERIMIENTOS TÉCNICOS DEL PROCESO DE COMPRA 3202-0540-LPU24	43

ABREVIATURAS

PALABRA	DEFINICIÓN
AAIP	Acceso a la Información Pública
AFC	Agencia Federal de Ciberinteligencia
AGCBA	Auditoría General de la Ciudad de Buenos Aires
APN	Administración Pública Nacional
CCPR	Comité de Derechos Humanos de las Naciones Unidas
CIDH	Comisión Interamericana de Derechos Humanos
CNC	Centro Nacional de Ciberseguridad
Co.Na.R.C.	Consulta Nacional de Rebeldías y Capturas
Corte IDH	Corte Interamericana de Derechos Humanos
CS5	Centro de Sinergia Cibernética de las Fuerzas Policiales y de Seguridad Federales
CSIRT-MINSEG	Equipo de Respuesta ante Incidentes de Seguridad Informática del MINSEG
EIPD	Evaluación de Impacto en la Protección de Datos
FIP	Federación Internacional de Prensa
GCABA	Gobierno de la Ciudad Autónoma de Buenos Aires
IA	Inteligencia Artificial
LPDP	Ley de Protección de Datos Personales
MINSEG	Ministerio de Seguridad
O.D.I.A.	Observatorio de Derecho Informático Argentino
PIDCP	Pacto Internacional de Derechos Civiles y Políticos
Re.Na.Per.	Registro Nacional de las Personas de la Nación
SiPreBa	Sindicato de Prensa de Buenos Aires
SRFP	Sistema de Reconocimiento Facial de Prófugos

PALABRA	DEFINICIÓN
TRF	Tecnologías de Reconocimiento Facial
UIAAS	Unidad de Inteligencia Artificial Aplicada a la Seguridad

GLOSARIO

PALABRA	DEFINICIÓN
ALGORITMO	Conjunto de instrucciones que se dan a una computadora para realizar una tarea o resolver un problema.
DATOS DE ENTRENAMIENTO DE FRT	Imágenes utilizadas para entrenar un algoritmo de reconocimiento facial, con el fin de permitir la comparación e identificación de futuras imágenes faciales.
EFFECTO INHIBIDOR (<i>CHILLING EFFECT</i>)	Fenómeno por el cual las personas limitan o modifican su comportamiento, especialmente el ejercicio de derechos como la libertad de expresión, por temor a posibles consecuencias negativas, como vigilancia, sanciones o represalias.
ENFOQUE SOCIOTÉCNICO	Estrategia de análisis de la tecnología que considere el contexto en el que se implementa, así como los factores políticos y estructurales que la atraviesan. En este caso, el análisis incluye las políticas que habilitan su uso, el marco normativo aplicable, los mecanismos de protección frente a abusos, el entramado de actores públicos y privados involucrados, y los grupos y derechos afectados por su despliegue.
PERFILAMIENTO	Práctica de recopilar y analizar datos sobre personas o grupos para identificar características, patrones de comportamiento o niveles de riesgo, con el fin de clasificarlos o tomar decisiones sobre ellos.
PLIEGOS DE ESPECIFICACIONES TÉCNICAS (PET)	Documento que forma parte de un proceso de compra y que describe de manera clara y detallada las características técnicas, requisitos, normas y condiciones que deben cumplir los bienes o servicios a adquirir. Su objetivo es asegurar que los proveedores comprendan exactamente lo que se necesita.
POLICIAMIENTO PREDICTIVO	Término utilizado para describir sistemas policiales basados en datos, perfiles y evaluaciones de riesgo, cuyo carácter verdaderamente predictivo es altamente cuestionable. Refiere a la utilización de algoritmos y análisis de datos históricos, con el propósito de anticipar dónde podrían ocurrir delitos. El policiamiento predictivo incluye técnicas con capacidad de analizar grandes volúmenes de datos heterogéneos mediante algoritmos de aprendizaje automático para identificar patrones, anomalías y tendencias, construir perfiles de riesgo, establecer vínculos entre eventos o individuos y generar predicciones sobre posibles conductas futuras o escenarios de riesgo.
RECONOCIMIENTO DE IMÁGENES Y BIOMETRÍA	Capacidad de procesar imágenes y datos biométricos para identificar o verificar personas, mediante técnicas como reconocimiento facial, comparación de imágenes, detección de rasgos y análisis en tiempo real de video, facilitando la identificación y validación de identidades.

PALABRA	DEFINICIÓN
RECONOCIMIENTO FACIAL	Técnica de visión por computadora utilizada para identificar rostros humanos a partir de imágenes empleadas previamente para entrenar un algoritmo.
REVISIÓN DE REDES SOCIALES E INVESTIGACIÓN / INTELIGENCIA DE FUENTES ABIERTAS (OSINT)	Capacidad de recolectar, integrar y analizar información proveniente de fuentes abiertas digitales (redes sociales, sitios web, foros, bases públicas), permitiendo mapear relaciones entre personas, identificar patrones de comportamiento, reconstruir actividades y generar inteligencia a partir de datos dispersos, mediante técnicas de correlación y visualización de vínculos.
TECNOLOGÍAS DE VIGILANCIA	Tecnologías, incluidos el hardware, el software y los servicios, diseñadas para permitir la vigilancia encubierta y no encubierta por parte de sistemas digitales y sobre estos, con el fin de supervisar, extraer, recopilar y/o analizar datos, incluidas las tecnologías de vigilancia biométrica.
TECNOLOGÍAS DE VIGILANCIA MASIVA	Tipo de tecnologías de vigilancia que, por su alcance y capacidad de procesamiento, permiten monitorear grandes volúmenes de personas y territorios con mayor precisión y automatización.
VIGILANCIA	Conjunto de prácticas mediante las cuales el Estado produce, organiza y utiliza información sobre las personas, para el fin declarado de la prevención e investigación de delitos.

1. RESUMEN EJECUTIVO

CONTEXTO: POLÍTICAS DE RECORTE Y REPRESIÓN DE LA PROTESTA SOCIAL

Entre diciembre de 2023 y diciembre de 2025, el Gobierno argentino implementó una gran cantidad de reformas en las áreas de seguridad e inteligencia y expandió el uso de tecnologías de vigilancia, en el marco de los primeros dos años de gestión de Javier Milei y la alianza La Libertad Avanza.

La vigilancia tiene un rol central en la agenda de gobierno: ya desde su plataforma electoral¹, el oficialismo planteaba el uso de herramientas como bases de datos vinculadas a reconocimiento facial y una mayor inversión en tecnologías para seguridad. Estos compromisos públicos se tradujeron en reformas del sistema de seguridad e inteligencia, junto con la implementación de nuevas prácticas como la creación de bases de datos de manifestantes, la vigilancia de redes sociales, el uso de reconocimiento facial, drones y cámaras móviles.

Estas reformas se dieron en el contexto de un fuerte ajuste económico en áreas sociales clave y a una reconfiguración institucional marcada por cambios normativos y medidas presupuestarias que ampliaron las capacidades punitivas, represivas y de vigilancia del Estado, sin un fortalecimiento equivalente de los mecanismos de control y rendición de cuentas.

A la vez, se intensificaron las narrativas polarizantes y del “enemigo interno”, expresado en represalias contra mujeres y comunidades LGBTI, las personas migrantes y otros grupos marginalizados, así como en la deslegitimación y el hostigamiento de actores de la sociedad civil, en particular periodistas y medios de comunicación, organizaciones sociales y de derechos humanos, sindicatos, espacios académicos y movimientos feministas y socioambientales.

En este marco, las tecnologías de vigilancia no operan como herramientas neutrales, sino como parte de una infraestructura orientada al control social, la persecución de la disidencia y la restricción del espacio cívico, amplificando prácticas de vigilancia, perfilamiento y represalias con efectos directos sobre derechos como la privacidad, la libertad de expresión, la asociación y la reunión pacífica.

REFORMAS ESTRUCTURALES Y OPERATIVAS Y ADQUISICIÓN DE TECNOLOGÍAS DE VIGILANCIA

En solo dos años, el Gobierno nacional impulsó un conjunto de reformas institucionales orientadas a ampliar sus capacidades de vigilancia e inteligencia, implementadas principalmente mediante decretos y resoluciones del Poder Ejecutivo, sin debate legislativo.

En el plano institucional, el Gobierno llevó adelante dos reformas del Sistema de Inteligencia Nacional, que ampliaron las funciones de inteligencia y contrainteligencia mediante definiciones amplias de “amenaza”, reforzaron la lógica de secreto, habilitaron un mayor acceso e intercambio de información entre organismos

¹ La agenda de seguridad llevó 47 ítems, superando ampliamente temas como Salud, Reforma Económica, Reforma Laboral, entre otras. La plataforma presentada en 2023 está disponible en: <https://www.electoral.gob.ar/nuevo/paginas/pdf/plataformas/2023/PASO/JUJUY%2079%20PARTIDO%20RENOVADOR%20FEDERAL%20-PLATAFORMA%20LA%20LIBERTAD%20AVANZA.pdf> Consultado en marzo 2026.

y crearon una nueva agencia especializada en ciberinteligencia. Estas modificaciones incrementaron la capacidad estatal de recolectar y centralizar grandes volúmenes de datos en un contexto de débiles mecanismos de control y supervisión.

En paralelo, la reforma del estatuto de la Policía Federal creó nuevas estructuras de investigación y formalizó prácticas como el monitoreo de redes sociales sin autorización judicial, estableciendo el “ciberpatrullaje” como función oficial. A ello se sumó la adopción de protocolos específicos para el uso de identidades digitales ficticias en investigaciones y la actuación de agentes encubiertos en entornos digitales.

En el plano operativo, el Gobierno, a través del Ministerio de Seguridad, estableció instrumentos clave como el “Protocolo Antipiquetes”, que habilita la intervención de fuerzas federales en protestas sin orden judicial y promueve la identificación, registro y sistematización de información sobre manifestantes, organizaciones y vehículos. Asimismo, creó la Unidad de Inteligencia Artificial Aplicada a la Seguridad (UIAAS), con amplias funciones vinculadas al análisis de datos, monitoreo digital, reconocimiento facial y predicción del delito, sin mecanismos específicos de control externo.

Finalmente, se adoptaron protocolos que regulan el uso de tecnologías específicas, como el ciberpatrullaje y el reconocimiento facial ex post, ampliando el marco operativo para la vigilancia en entornos digitales. En conjunto, estas medidas configuran la expansión de capacidades estatales de monitoreo, la incorporación de tecnologías avanzadas y la ausencia de mecanismos de control y rendición de cuentas robustos, en un contexto de crecientes acciones estatales autoritarias orientadas al control y la disuasión de la protesta.

ADQUISICIÓN DE TECNOLOGÍAS DE VIGILANCIA

Entre 2024 y 2025, el Ministerio de Seguridad Nacional avanzó en la adquisición de tecnologías de vigilancia por un monto de, al menos, 1,2 millones de dólares. Las contrataciones relevadas muestran una inversión sostenida en herramientas orientadas al monitoreo de fuentes abiertas, el reconocimiento facial y la vigilancia aérea, en un contexto de ajuste económico y sin información suficiente sobre controles, evaluaciones de impacto o salvaguardas para los derechos humanos, más allá de información mínima sobre contrataciones públicas.

Entre las adquisiciones analizadas en este informe se destacan:

- una licencia de la plataforma de investigación en fuentes abiertas Maltego, destinada a la recolección, cruce y visualización de grandes volúmenes de datos provenientes de redes sociales, sitios web, dark web, datos personales, infraestructura técnica y otras fuentes abiertas;
- la compra de una licencia de reconocimiento facial Clearview AI, una empresa conocida ampliamente por su historial de explotación masiva de datos biométricos sin base legal suficiente en múltiples contextos a nivel global;
- y la adquisición de drones y estaciones terrestres de operación, con capacidades de seguimiento automatizado, cámaras térmicas y transmisión en tiempo real de imágenes.

Estas compras se articulan con las nuevas reformas institucionales y protocolos y dotan de medios concretos a nuevas funciones de vigilancia a ser llevadas a cabo en entornos digitales y físicos. En particular, amplían la capacidad estatal para recolectar y procesar información sobre personas, identificar rostros, rastrear movimientos y reforzar tareas de monitoreo en el espacio público, incluso en contextos de protesta.

Además, estas adquisiciones deben analizarse de manera complementaria con la expansión de la infraestructura de videovigilancia llevada adelante por el Gobierno de la Ciudad Autónoma de Buenos Aires, que ha incrementado significativamente la cobertura territorial mediante la instalación de cámaras, sistemas de procesamiento de imágenes y servicios asociados. Mientras el gobierno nacional está reforzando sus capacidades de análisis, identificación y tratamiento de datos, la Ciudad de Buenos Aires incrementa simultáneamente su capacidad para recopilar información en los espacios públicos, impulsando la instalación de una amplia infraestructura de vigilancia y la celebración de contratos para adquirir nuevas herramientas que amplían aún más sus facultades de vigilancia. Esta combinación configura un aparato de vigilancia más integrado, que incrementa la capacidad estatal de monitoreo y vigilancia a escala urbana.

EL EFECTO INHIBIDOR DE LA VIGILANCIA

El informe identifica que el despliegue de políticas y tecnologías de vigilancia en Argentina tiene impactos directos en derechos humanos, y también produce efectos indirectos significativos sobre el ejercicio de derechos humanos, a través de lo que es conocido como “efecto inhibidor” o *chilling effect*. Este fenómeno se manifiesta cuando la mera percepción de estar siendo vigilado modifica las conductas de las personas, limitando su participación en el ejercicio de sus derechos humanos, incluyendo los derechos de libertad de expresión, asociación y reunión pacífica.

A partir de entrevistas a 21 personas de distintos perfiles, incluyendo periodistas, activistas, personas jubiladas, jóvenes y defensores de derechos humanos, el informe concluye que hay una percepción generalizada de vigilancia estatal, tanto en el espacio físico como en el entorno digital. Esta percepción se vincula con la presencia visible de tecnologías (como drones y cámaras), el monitoreo de redes sociales, la recopilación de información en contextos de protesta y antecedentes previos de vigilancia estatal.

Sustantivamente, esta percepción se traduce en cambios concretos de comportamiento, que afectan el ejercicio de derechos fundamentales. Entre ellos se destacan:

- La reducción o selectividad en la participación en manifestaciones, en algunos casos directamente vinculada al temor a la represión o a la identificación posterior.
- La modificación de estrategias organizativas de activistas, personas que protestan y la sociedad civil a gran escala, incluyendo menor exposición pública, mayor cautela en la planificación de actividades y reducción de la capacidad operativa de los grupos.
- La adaptación de prácticas comunicacionales, como el uso de plataformas más seguras o el abandono de canales considerados vulnerables.
- La autocensura en redes sociales y espacios públicos, mediante la moderación del discurso o la disminución de la participación.
- En el caso del periodismo, limitaciones en la cobertura y en la protección de fuentes, debido al riesgo de identificación y seguimiento.

Esto incluye impactos diferenciados en grupos específicos, particularmente en trabajadores de prensa, activistas y personas migrantes. Analiza también las consecuencias en la población joven. En estos casos, la vigilancia se combina con otras medidas, como la represión en el espacio público o disposiciones específicas como el reporte a autoridades migratorias, lo que intensifica los efectos disuasorios y genera mayores niveles de retraimiento.

Asimismo, esta investigación encuentra que la vigilancia no actúa de manera aislada, sino en articulación con otras políticas de seguridad, configurando un entorno en el que la percepción de control estatal constante debilita la confianza entre personas y organizaciones, dificulta la articulación colectiva y reduce la disposición a participar en actividades políticas o sociales. Estos hallazgos muestran que la vigilancia, incluso cuando no deriva en represalias directas, puede generar restricciones indirectas pero sustantivas sobre los derechos a la libertad de expresión, reunión y asociación, en línea con lo advertido previamente por organismos internacionales de derechos humanos. De este modo, el impacto de estas tecnologías excede su uso operativo, incidiendo en la configuración misma del espacio cívico.

Aunque las tecnologías y las políticas de vigilancia se han introducido como herramientas para, supuestamente, abordar determinadas formas de actividad delictiva, las conclusiones de Amnistía Internacional demuestran que las disposiciones legales redactadas de manera amplia, junto con el historial documentado de abusos y uso indebido de estas tecnologías en Argentina, vulneran los derechos a la privacidad, a la igualdad y la no discriminación, a la libertad de expresión y de reunión pacífica, al tiempo que socavan la transparencia y el acceso a la información.

RESPONSABILIDADES CORPORATIVAS DE CLEARVIEW AI

Amnistía Internacional ha concluido que Clearview AI debería haber sido consciente de los riesgos para los derechos humanos derivados de sus operaciones empresariales en general, incluso en Argentina. En virtud

de los Principios Rectores de la ONU sobre las Empresas y los Derechos Humanos (Principios Rectores de la ONU), las empresas deben hacer frente con prontitud a las consecuencias negativas sobre los derechos humanos en las que tengan alguna participación, independientemente del lugar en el que operen. Esta responsabilidad de las empresas de respetar los derechos humanos existe con independencia de la capacidad o voluntad de los Estados de cumplir sus propias obligaciones de derechos humanos y está por encima del cumplimiento o no de las leyes y normas nacionales de derechos humanos. Para cumplir con esta responsabilidad empresarial, una empresa debe adoptar medidas tempranas, proactivas y continuas para identificar sus consecuencias reales o potenciales sobre los derechos humanos y responder a ellas, mediante la realización de la diligencia debida para identificar, prevenir, mitigar y rendir cuentas de cualquier consecuencia negativa sobre los derechos humanos que resulte de sus operaciones o como resultado de sus relaciones comerciales con otros actores.

Amnistía Internacional ha constatado que Clearview AI no ha llevado a cabo hasta la fecha una evaluación pública, transparente y continua del impacto en los derechos humanos, ni ha demostrado que la empresa haya abordado ningún efecto negativo real o potencial en los derechos humanos que sus productos o actividades empresariales puedan causar, contribuir a causar o con los que estén directamente relacionados en Argentina. En consecuencia, Clearview AI debe cesar el desarrollo, la venta, el despliegue y la exportación de tecnologías de reconocimiento facial en Argentina, o correr el riesgo de que la empresa contribuya al entorno cada vez más hostil para los derechos humanos en el país o esté directamente vinculada a él.

Previo a la publicación de este informe, Amnistía Internacional escribió a las autoridades nacionales y de la Ciudad Autónoma de Buenos Aires en Argentina para buscar sus respuestas a los hallazgos de esta investigación. Amnistía Internacional también escribió a la empresa de tecnología de reconocimiento facial Clearview AI para exponer sus preocupaciones en materia de derechos humanos relacionadas con sus productos y solicitar su respuesta a la información y a las preocupaciones de derechos humanos planteadas en este informe en relación con dichos productos. Sin embargo, al momento de la publicación de este informe, Amnistía Internacional no había recibido respuesta de la empresa.

Este informe analiza las reformas normativas y las contrataciones de tecnología llevadas a cabo por el Gobierno Nacional argentino y la Ciudad de Buenos Aires. No pretende ofrecer un análisis exhaustivo del cumplimiento de los derechos humanos por parte de las empresas implicadas. En este sentido, las alegaciones se dirigen únicamente sobre Clearview AI.

Amnistía Internacional informó además a las empresas mencionadas en los contratos y documentos de contratación pública analizados en este informe, entre las que se incluyen Maltego, DJI y NOSIS, sobre su próxima publicación, pero no llevó a cabo un análisis de las implicaciones derivadas de sus cadenas de valor. Amnistía Internacional no formula ninguna alegación contra estas empresas. En el momento de la publicación, Amnistía Internacional solo ha recibido una respuesta de Maltego.

RECOMENDACIONES PRINCIPALES

Amnistía Internacional realiza las siguientes recomendaciones clave para terminar con estas violaciones a los derechos humanos:

El Gobierno Nacional y el Gobierno de la Ciudad de Buenos Aires deberían:

- Prohibir el desarrollo, la producción, la venta y el uso, por parte de todos los actores públicos y privados, de tecnologías biométricas que permitan la vigilancia masiva y la vigilancia selectiva discriminatoria.
- Prohibir el desarrollo, la producción, la venta y el uso de sistemas de inteligencia artificial que creen o amplíen bases de datos de reconocimiento facial mediante la recopilación indiscriminada de imágenes faciales de internet o de grabaciones de circuitos cerrados de televisión (CCTV).

- Prohibir los sistemas automatizados de evaluación de riesgos y elaboración de perfiles en el contexto migratorio cuando se utilicen para determinar si las personas en movimiento representan un “riesgo” de actividad ilícita o una amenaza para la seguridad.
- Suspender de inmediato el uso de todas las tecnologías de vigilancia adquiridas o desplegadas sin una base jurídica específica, sin evaluaciones de impacto sobre los derechos humanos y la protección de datos (EIPD), o sin mecanismos de supervisión externa. Esto incluye, en particular, las herramientas de monitoreo de fuentes abiertas y de vigilancia aérea.

El Gobierno nacional, y en particular el Ministerio de Seguridad, deberían:

- Publicar de inmediato información sustantiva sobre la estructura, el presupuesto, los proveedores y los criterios técnicos de todas las funciones asignadas a la UIAAS, como requisito mínimo de transparencia y rendición de cuentas.
- Crear un grupo de trabajo intersectorial integrado por organismos de supervisión, organizaciones de la sociedad civil y personas expertas en tecnología y derechos humanos, con un mandato, plazos y resultados esperados claramente definidos, con el fin de revisar el alcance de la UIAAS y establecer criterios consensuados para su regulación.

El Congreso Nacional debería:

- Constituir y garantizar el funcionamiento efectivo de la Comisión Bicameral de Fiscalización de los Organismos y Actividades de Inteligencia, de conformidad con el artículo 31 de la Ley N.º 25.520, dotándola de los recursos y facultades necesarios para ejercer una supervisión específica sobre las tecnologías de vigilancia.

Los organismos regionales e internacionales de derechos humanos deberían:

- Promover la adopción de legislación que prohíba el uso, desarrollo, producción, venta y exportación de tecnologías de reconocimiento biométrico remoto destinadas a la vigilancia masiva, así como de tecnologías de reconocimiento biométrico remoto o de reconocimiento facial utilizadas con fines de identificación por organismos estatales y actores del sector privado dentro de sus respectivas jurisdicciones, por ser tecnologías intrínsecamente incompatibles con el derecho internacional de los derechos humanos.

2. METODOLOGÍA

2.1 CONTEXTO, MÉTODOS Y ALCANCE DE ESTE ESTUDIO

Este informe adopta un enfoque sociotécnico que examina no solo las tecnologías utilizadas, sino también las políticas que habilitan su uso, el marco normativo aplicable, los mecanismos de protección frente a abusos, el entramado de actores públicos y privados involucrados, y los grupos y derechos afectados por su despliegue.

Este informe se enfoca en el período entre diciembre de 2023 y diciembre de 2025, que coincide con los dos primeros años de la presidencia de Javier Milei a nivel nacional y con la jefatura de gobierno de la Ciudad de Buenos Aires, por parte de Jorge Macri. Este informe se centra en el análisis de tres tipos de tecnologías de vigilancia. Esta selección se basa en que se trata de tecnologías adquiridas por el Gobierno de la Nación y por el de la Ciudad de Buenos Aires. En términos generales, pueden agruparse en las siguientes categorías:

- Revisión de redes sociales e investigación/inteligencia de fuentes abiertas (OSINT)
- Reconocimiento de imágenes y biometría
- Predicción de delitos y determinación de zonas sujetas a una mayor vigilancia y presencia policial.

En términos metodológicos, este informe tiene por objetivo analizar el impacto en los derechos humanos del uso de tecnologías de vigilancia por parte del Gobierno Nacional de la Argentina. Dado que se trata de un fenómeno en pleno desarrollo, este informe provee una instantánea de los impactos en derechos humanos, sin pretender ser exhaustivo en su análisis.

El mismo integra el análisis normativo del marco de derechos humanos internacional, regional y local, aplicable al uso de tecnologías de vigilancia en Argentina con un estudio detallado de las reglamentaciones nacionales, que da lugar a las reformas de los sistemas de seguridad y de inteligencia nacional. Además, este informe recupera ejemplos locales y regionales, para dar cuenta del contexto internacional del uso de este tipo de tecnologías.

A su vez, esta investigación se propone el análisis de las tecnologías de vigilancia adquiridas por el Estado, a partir de la revisión de procesos de contratación pública, lo que permite identificar con precisión las herramientas actualmente utilizadas. Finalmente, se analiza el impacto de las políticas de vigilancia sobre las personas, incluyendo sus efectos inhibidores sobre el ejercicio de derechos humanos.

La investigación realiza esto a partir de:

ANÁLISIS DE COMPRAS Y CONTRATACIONES DE TECNOLOGÍAS DE VIGILANCIA

Para el análisis de las tecnologías descritas previamente, fue realizado un estudio de los procesos de compra en los portales abiertos de compras y contrataciones del Gobierno de la Nación y de la Ciudad de Buenos Aires, titulados ComprAR y BA Compras, respectivamente. A partir de los datos publicados en estos portales, y de sus funcionalidades, se generaron bases de datos para filtrar las compras de los Ministerios de Seguridad, así como las fuerzas de seguridad de cada jurisdicción, para los 24 meses correspondientes al alcance temporal de este informe. Sin embargo, esto ofrece apenas una instantánea de la verdadera magnitud del problema, ya que el análisis no puede incluir la información sobre adquisiciones que no son de acceso público debido a cláusulas de confidencialidad. A partir de este análisis, fueron seleccionadas 11

compras, 5 de la jurisdicción nacional y 6 de la Ciudad de Buenos Aires, con el objetivo de obtener una muestra que sirva de ilustración para la pluralidad de tecnologías adquiridas.

Para cada caso analizado, se reconstruyó el proceso de contratación llevado adelante por las entidades estatales. Esto permitió examinar aspectos como el tipo de procedimiento (contratación directa, licitación pública, etc.), la modalidad de adquisición (orden de compra abierta, llave en mano, etc.), la duración, el objeto y el monto, entre otros datos relevantes. El análisis se basa en la información contenida en los propios expedientes de contratación, así como en las órdenes de compra asociadas y en las resoluciones que les otorgan respaldo institucional. Para identificar con mayor precisión el objeto de cada adquisición y las funcionalidades esperadas de las tecnologías, se utilizaron los Pliegos de Especificaciones Técnicas (PET), documentos que forman parte de los procesos de compra pública. Asimismo, las resoluciones permiten identificar las áreas involucradas, lo que aporta indicios sobre las políticas en las que se enmarcan dichas adquisiciones.

PEDIDOS DE ACCESO A LA INFORMACIÓN PÚBLICA

En términos de fuentes oficiales de información pública, como se mencionó previamente, este informe basa su análisis en recursos publicados de portales de compras y contrataciones, boletines oficiales de publicación normativa, gacetillas de prensa oficial, entre otras instancias de publicación proactiva por parte de los gobiernos de ambas jurisdicciones.

Sin embargo, una parte significativa de la información no se encuentra disponible en estos espacios, por lo que resultó necesario acceder a ella mediante pedidos formales de acceso a la información pública (PAI). Este derecho se encuentra regulado, en el ámbito nacional, por la Ley 27.275 de Acceso a la Información Pública² (publicada en 2016) y, en la Ciudad Autónoma de Buenos Aires, por la Ley 104 de Acceso a la Información Pública³ (modificada y actualizada en 2016).

En este sentido, algunos de los datos analizados en el presente informe surgen de pedidos de acceso a la información realizados por Amnistía Argentina entre abril de 2025 y enero de 2026. Durante ese período, la organización realizó cuatro pedidos de acceso a la información pública para conocer distintos aspectos del uso de tecnologías de vigilancia por ambas jurisdicciones de gobierno. A continuación, se presenta un listado de cada uno de estos pedidos:

TABLA 1: PEDIDOS DE ACCESO A LA INFORMACIÓN PÚBLICA SOBRE TECNOLOGÍAS DE VIGILANCIA

DESTINATARIO	INFORMACIÓN REQUERIDA (RESUMEN)	FECHA PEDIDO	FECHA RESPUESTA
MINISTERIO DE SEGURIDAD NACIONAL	Información sobre funcionamiento, regulación, presupuesto y actividades de la Unidad de IA Aplicada a la Seguridad; uso de reconocimiento facial por fuerzas de seguridad (tecnología, bases de datos, contratos, evaluaciones e impacto); y tareas de ciberpatrullaje en redes sociales (monitoreo, herramientas, datos personales y acuerdos con empresas).	8 de mayo 2025	26 de junio 2025
MINISTERIO DE SEGURIDAD NACIONAL	Normativa, protocolos, equipos y uso del registro fílmico de fuerzas de seguridad en manifestaciones, incluyendo cámaras y drones, acceso a las imágenes, fines de utilización, controles, almacenamiento y áreas responsables.	17 de diciembre 2025	3 de febrero 2026
MINISTERIO DE SEGURIDAD NACIONAL	Estado operativo de la UIAAS (estructura, actividades, normativa, contrataciones y cooperación internacional); implementación del protocolo de reconocimiento facial (software, compras y uso de bases de datos); y aplicación del protocolo de ciberpatrullaje (implementación, herramientas, monitoreo y tratamiento de datos personales).	19 de diciembre de 2025	2 de febrero de 2026

² Disponible en: <https://servicios.infoleg.gob.ar/infolegInternet/anexos/265000-269999/265949/norma.htm>

³ Disponible en: <https://boletinoficial.buenosaires.gob.ar/normativaba/norma/982>

DESTINATARIO	INFORMACIÓN REQUERIDA (RESUMEN)	FECHA PEDIDO	FECHA RESPUESTA
MINISTERIO DE SEGURIDAD DE LA CIUDAD DE BUENOS AIRES	Información sobre contrataciones, especificaciones técnicas e implementación de sistemas de videovigilancia, análisis forense digital, reconocimiento facial y detección de prófugos en el GCABA, incluyendo cámaras, software, licencias, auditorías, controles institucionales e integración con otros sistemas.	4 de febrero de 2026	16 y 17 de marzo de 2026 ⁴

Fuente: Cuadro elaborado por Amnistía Internacional.

Si bien estos pedidos fueron respondidos por las autoridades, en su mayoría se trata de respuestas parciales. En el caso del primer pedido enviado, por ejemplo, las preguntas sobre uso de reconocimiento facial fueron respondidas parcialmente, amparándose en las reservas por razones de seguridad nacional establecidas por la Ley 27.275, Art. 8 inc. A y decretos reglamentarios. En el mismo pedido, en lo relativo a las preguntas sobre patrullaje de redes sociales (o *ciberpatrullaje*), la negatoria fue total, en este caso amparada bajo la confidencialidad de las actividades del Sistema Nacional de Inteligencia, según lo establecido en la Ley Nacional de Inteligencia (Ley 25.520, Art. 16 y 16 bis).

ENTREVISTAS: ANÁLISIS DEL EFECTO INHIBIDOR DE LAS TECNOLOGÍAS DE VIGILANCIA

Para operacionalizar el análisis de los efectos inhibidores en esta investigación, seguiremos la metodología utilizada por Murray *et al*⁵, quienes consideran este fenómeno como un conjunto de modificaciones del comportamiento que surgen del temor, la alerta o la anticipación de la vigilancia, incluyendo la autocensura, la renuencia a relacionarse con personas u organizaciones que se perciben como vigiladas y la erosión de la confianza interpersonal que socava la acción colectiva.⁶

Entre octubre y diciembre de 2025, fueron entrevistadas 21 personas pertenecientes a distintos perfiles, incluyendo trabajadores de prensa (diseñadores, fotógrafos, periodistas, integrantes de canales de *streaming* y representantes sindicales), estudiantes y jóvenes,⁷ activistas de derechos humanos y personas jubiladas. Todas ellas son residentes en la Ciudad de Buenos Aires, dado que una de las metas de este trabajo consiste en analizar las experiencias de individuos y comunidades que participaron de las movilizaciones en las inmediaciones del Congreso de la Nación, motivadas por la oposición a las reformas económicas de la administración actual, incluidas amplias medidas de austeridad, desregulación y recortes del gasto público. Trece personas fueron entrevistadas de forma individual y remota y las ocho restantes fueron entrevistadas en encuentros grupales de forma presencial.

En estas entrevistas, fueron abordadas las siguientes dimensiones de análisis:

1. Percepciones de la vigilancia

- a. Conocimiento/concienciación sobre las tecnologías de vigilancia.
- b. Distinción entre vigilancia real y vigilancia percibida.
- c. Influencia de las herramientas tradicionales (cámaras, policía) frente a las digitales (vigilancia telefónica, recopilación de datos).

2. Libertad de reunión y participación política

- a. Erosión de la confianza dentro de los grupos.
- b. Renuencia a asistir u organizar protestas/reuniones.
- c. Evitar a personas u organizaciones que se perciben como vigiladas.

⁴ Debido a una dificultad técnica para acceder a la información, Amnistía Internacional pudo acceder al contenido de las respuestas enviadas por el GCABA el 27 de mayo de 2026.

⁵ Murray, D., Fussey, P., Hove, K., Wakabi, W., Kimumwe, P., Saki, O., & Stevens, A. (2024). The chilling effects of surveillance and human rights: Insights from qualitative research in Uganda and Zimbabwe. *Journal of Human Rights Practice*, 16(1), 397–412. <https://doi.org/10.1093/jhuman/huad020>

⁶ Op. Cit., Capítulo 6: "Conclusions".

⁷ Fueron entrevistadas cuatro personas de forma grupal, del grupo de jóvenes de Amnistía Internacional, un espacio donde jóvenes de 15 a 25 años participan en campañas de activismo voluntario por los derechos humanos. Por razones de privacidad, se hablará de las respuestas del grupo como un conjunto. No fueron entrevistados menores en este informe.

3. Libertad de expresión

- a. Prácticas de autocensura.
- b. efectos intimidatorios (directos o indirectos).
- c. Expresión en línea frente a expresión fuera de línea.

Estas dimensiones fueron operacionalizadas en un cuestionario semi-estructurado de catorce preguntas, que ordenaron las entrevistas individuales y las grupales por igual. Estas preguntas fueron diseñadas para involucrar a los participantes en su papel como miembros de grupos u organizaciones, más que como individuos aislados.

Previo a la publicación de este informe, Amnistía Internacional escribió a las autoridades nacionales y de la Ciudad Autónoma de Buenos Aires en Argentina para buscar sus respuestas a los hallazgos de esta investigación. Amnistía Internacional, además, escribió a la compañía Clearview AI para solicitar su respuesta a la información mencionada en este informe acerca de la empresa, así como a DJI, Maltego y NOSIS. A la fecha de publicación de este informe, solo había respondido la empresa Maltego.

CÁMARA DE VIDEOVIGILANCIA: CONSTRUCCIÓN COLABORATIVA DE LA INFORMACIÓN

El Gobierno de la Ciudad de Buenos Aires (GCABA) no tiene publicada información relativa a la ubicación específica de las Cámaras del Sistema de Videovigilancia de la Ciudad, algo que es de suma importancia a la hora de analizar el respeto de la privacidad de las personas que buscan manifestarse, así como su derecho a la protesta pacífica.

En este sentido, desde Amnistía Internacional, junto con organizaciones de derechos humanos de la Argentina, fue realizado un *hackathon*, en octubre de 2025. El evento tuvo el objetivo de mapear colaborativamente la cobertura de las cámaras de vigilancia ubicadas en las cercanías del Congreso Nacional, y así conocer su cobertura para un potencial uso de tecnologías de reconocimiento facial, sea en tiempo real o a partir de un procesamiento posterior. Esto fue realizado utilizando imágenes de Google Street View.

El lugar fue seleccionado por ser un espacio frecuentemente utilizado por la sociedad civil, en particular durante las protestas, y sirvió como referencia para establecer el alcance y el grado de exposición a una posible vigilancia masiva. Como Amnistía Internacional ha documentado previamente, mediante el mapeo de la ubicación de las cámaras de videovigilancia (CCTV) es posible estimar el alcance potencial de la exposición al reconocimiento facial, ya que esta tecnología suele utilizarse como software asociado a dichas cámaras. Este método no distingue si la exposición al reconocimiento facial se produce en tiempo real o mediante el procesamiento posterior de las imágenes por parte del GCABA o las autoridades nacionales en esa zona.

Para ello, las personas participantes recorrieron las calles dentro de un radio de 8 cuadras alrededor del Congreso Nacional en busca de cámaras instaladas en edificios y otros elementos de infraestructura pública (por ejemplo, postes de alumbrado, semáforos, etc.), y elaboraron un listado con las coordenadas de las cámaras identificadas. Posteriormente, ese listado fue sometido a una revisión por pares entre las personas participantes y, a partir de las coordenadas recopiladas, se elaboró un mapa.

Los resultados de este evento permitieron generar un mapa, así como un espacio de debate e intercambio entre las organizaciones participantes.⁸

2.2 HISTORIA DE LA VIGILANCIA EN ARGENTINA Y LA REGIÓN

Entre diciembre 2023 y diciembre 2025, el Gobierno Nacional generó una serie de reformas de las funciones de las fuerzas de seguridad y comenzó a adquirir una serie de tecnologías tendientes a aumentar sus capacidades de vigilancia. Este período representa los primeros dos años de la gestión de gobierno de la Libertad Avanza, una alianza partidaria que se presentó electoralmente en el año 2021, por primera vez. En 2023, en su segunda experiencia electoral, logró ganar las elecciones presidenciales, lo que llevó al entonces diputado Javier Milei a alcanzar la presidencia. Su campaña electoral tuvo una marcada impronta

⁸ Los resultados del hackathon están disponibles en la sección 6.2.

en propuestas de recortes económicos, que fueron manifestados por el entonces candidato con el uso de una motosierra en los actos previos a las elecciones.

Además de la agenda económica, la agenda de seguridad tuvo un lugar relevante en la propuesta electoral de La Libertad Avanza. El uso de tecnologías de vigilancia fue interés de la alianza de gobierno desde sus inicios, como quedó plasmado en la plataforma presentada ante la autoridad electoral nacional.⁹ En ese documento, el apartado con las propuestas de “seguridad nacional” manifestó la vocación de “crear a nivel nacional una base de datos de personas con pedido de captura vinculada a cámaras de seguridad con identificación de rostro [...]”, así como de “invertir en tecnologías para todas las fuerzas de seguridad”. Esto muestra un indicio de la centralidad que tenían en las actividades de vigilancia y el uso de tecnologías en la agenda de las entonces personas candidatas, aspirantes al gobierno.

Tanto las promesas de ajuste como las de vigilancia fueron implementadas por la nueva gestión. En materia económica, el gobierno generó ajustes en áreas como seguridad social, salud, educación y desarrollo productivo.¹⁰ En materia de vigilancia, durante sus primeros dos años de gestión, generó reformas de los sistemas de seguridad y de inteligencia nacional, que fueron luego complementadas con nuevas áreas y protocolos para tareas como el armado de bases de datos de manifestantes, vigilancia de redes sociales y fuentes abiertas, uso de tecnologías de reconocimiento facial, uso de drones y cámaras móviles, entre otras.¹¹

De esta manera, estas amenazas a los derechos económicos y sociales se vieron complementadas por un proceso acelerado de reconfiguración institucional, marcado por la expansión de prácticas autoritarias, una ofensiva explícita contra las agendas de género y diversidad y una transformación radical de la política exterior. El Gobierno impulsó reformas que ampliaron su capacidad coercitiva sin fortalecer mecanismos de supervisión y rendición de cuentas, donde las tecnologías de vigilancia ocupan un lugar central. No se trata de herramientas neutrales, sino de dispositivos que pueden reforzar el control social, la persecución de la disidencia y la restricción del espacio cívico, especialmente en contextos de baja transparencia y débiles controles institucionales. Así, el impacto de la tecnología en los derechos humanos debe analizarse en conexión con esta deriva autoritaria: como parte de una infraestructura de poder que amplifica la vigilancia, el perfilamiento y las represalias de personas y grupos, con efectos sobre el derecho a la privacidad, la libertad de expresión, la asociación y la reunión.

2.3 VIGILANCIA MASIVA SIN CONTROL: RECONOCIMIENTO FACIAL DE PRÓFUGOS EN LA CIUDAD DE BUENOS AIRES

La Ciudad Autónoma de Buenos Aires, Capital de la Argentina, cuenta con un historial que da cuenta de usos abusivos de tecnologías de vigilancia masiva. El caso del Sistema de Reconocimiento Facial de Prófundos (SRFP), implementado por el Gobierno de la Ciudad de Buenos Aires (GCABA) entre 2019 y 2020 y suspendido judicialmente en 2022¹² resulta ilustrativo por haber sido una de las primeras experiencias de aplicación de inteligencia artificial a tareas policiales en el país y por haber evidenciado impactos graves sobre los derechos humanos.¹³ Muchos de los actores, tecnologías e infraestructuras involucradas en ese sistema continúan activos en la actualidad y pueden tener un rol clave en una potencial colaboración entre los gobiernos de la Nación y de la Ciudad frente a las políticas de vigilancia impulsadas por el gobierno de Javier Milei.

El SRFP consistió en el uso de algoritmos de reconocimiento facial aplicados a imágenes captadas por cámaras de videovigilancia en el espacio público, contrastadas automáticamente con las bases de datos de la Consulta Nacional de Rebeldías y Capturas (Co.Na.R.C.) y con la base de datos biométricos SIBIOS del

⁹ Puntos 10 y 14 respectivamente. Link al documento:

<https://www.electoral.gob.ar/nuevo/paginas/pdf/plataformas/2023/PASO/JUJUY%2079%20PARTIDO%20RENOVADOR%20FEDERAL%20PLATAFORMA%20LA%20LIBERTAD%20AVANZA.pdf> Consultado en marzo 2026.

¹⁰ Según datos analizados por el CEPA, en base a datos oficiales de ejecución presupuestaria. El informe está disponible en el siguiente link: <https://centrocepa.com.ar/informes/735-la-ejecucion-presupuestaria-de-la-administracion-publica-nacional-datos-a-diciembre-2025> Consultado en marzo 2026.

¹¹ Las reformas realizadas por el Gobierno Nacional en la materia son analizadas en profundidad en la sección 5 de este informe.

¹² Para más información, este escrito del Centro de Estudios Legales y Sociales (CELS), uno de los organismos que judicializó el sistema: <https://www.cels.org.ar/web/2023/04/confirman-la-inconstitucionalidad-del-uso-del-sistema-de-reconocimiento-facial/> Consultado en marzo 2026.

¹³ Amnistía Argentina solicitó, junto con otras organizaciones de derechos humanos, la suspensión del SRFP por su alto potencial para la afectación de derechos humanos. El comunicado, de octubre de 2020, está disponible en el link: <https://amnistia.org.ar/noticias/la-legislatura-portena-debe-rechazar-el-uso-de-la-tecnologia-de-reconocimiento-facial-para-la-vigilancia-del-espacio-publico>

Registro Nacional de las Personas (Re.Na.Per.).¹⁴ Si bien la Resolución 398/2019¹⁵ del Ministerio de Justicia y Seguridad del GCABA establecía límites estrictos al uso del sistema y la obligación de destruir los datos una vez cesada la orden judicial, su implementación excedió esos límites, lo que derivó en su suspensión judicial. Como surge de la causa judicial, uno de los principales problemas del SRFP fue la baja calidad de los datos de la base Co.Na.R.C., lo que dio lugar a múltiples casos de personas detenidas por error. A ello se sumó la falta de información pública sobre el funcionamiento del sistema algorítmico y la dependencia de software propietario sin auditorías independientes, lo que limitó la capacidad del Estado para ejercer un control.¹⁶

Aunque el SRFP continúa suspendido al momento de la escritura de este informe, el GCABA realizó importantes inversiones en infraestructura de videovigilancia, ampliando y renovando su sistema, que incluye cámaras fijas, móviles, drones, sistemas aerostáticos y dispositivos en patrulleros. Sin embargo, no existe información pública sobre la ubicación de estos dispositivos, y el Gobierno se negó a responder pedidos de acceso a la información alegando razones de seguridad pública.¹⁷

La judicialización del SRFP, iniciada en 2020 a partir de una acción de amparo colectivo¹⁸ promovida por el Centro de Estudios Legales y Sociales (CELS) y el Observatorio de Derecho Informático Argentino (ODIA), permitió dimensionar con mayor claridad la magnitud de las irregularidades en su funcionamiento. En el marco de ese proceso¹⁹ se constató que el Gobierno de la Ciudad Autónoma de Buenos Aires había realizado casi diez millones de consultas de datos biométricos al ReNaPer, pese a que el universo de personas habilitadas para ser identificadas mediante el sistema —correspondiente a la base de la Co.Na.R.C.— no superaba las cuarenta mil. Asimismo, la pericia informática confirmó que 15.459 personas habían sido incorporadas al motor de búsqueda del SRFP sin encontrarse registradas en esa base de datos y, por lo tanto, sin que existiera una orden judicial que habilitara su identificación mediante reconocimiento facial. Estas irregularidades se produjeron, además, en un contexto caracterizado por la ausencia de mecanismos efectivos de control institucional, la falta de evaluaciones de impacto previas y la opacidad en torno al funcionamiento del sistema.

En este sentido, el antecedente del SRFP no debe ser leído como un episodio aislado o superado, sino como una advertencia concreta sobre los riesgos que implica el fortalecimiento de políticas de vigilancia y control en ausencia de marcos normativos robustos, controles efectivos y garantías suficientes para la protección de los derechos humanos. El despliegue de estas tecnologías en la Argentina plantea interrogantes centrales sobre los límites al poder estatal, el impacto sobre la participación política, la protesta social, y la necesidad de evaluar estas prácticas a la luz de los estándares internacionales de derechos humanos.

2.4 EXPERIENCIAS REGIONALES: AMÉRICA LATINA FRENTE A LA EXPANSIÓN DE LA VIGILANCIA MASIVA

América Latina vive actualmente un crecimiento sostenido en el uso de tecnologías de vigilancia por parte de los gobiernos. Esto se da a partir de la combinación de herramientas tradicionales, como cámaras de videovigilancia, con sistemas de reconocimiento facial automatizado, monitoreo masivo de datos, patrullaje de redes sociales, interceptación de comunicaciones y análisis predictivo mediante inteligencia artificial.

Uno de los ejemplos más visibles de esta tendencia es la expansión de sistemas de videovigilancia en grandes ciudades. En Ciudad de México, por ejemplo, el sistema C5 integra cientos de miles de cámaras conectadas a centros de comando que utilizan análisis automatizado de imágenes, y cuya falta de controles,

¹⁴ Según consta en el Anexo de la Resolución 398/19 que establece las pautas del funcionamiento del sistema.

<https://documentosboletinoficial.buenosaires.gob.ar/publico/PE-RES-MJYSGC-MJYSGC-398-19-ANX.pdf>

¹⁵ Resolución 398/2019. Disponible en: <https://boletinoficial.buenosaires.gob.ar/normativaba/norma/464360> Consultado en Diciembre 2025.

¹⁶ Según consta en el Fallo que establece la suspensión del SRFP, la base de datos fue depurada en el año 2020, lo que produjo la reducción de 46.000 a 33.000 registros. El titular del área encargada de la gestión de la base de datos afirmó que la utilización de ésta en el marco del SRFP puede ocasionar falsos positivos dados distintos problemas de gestión interna o provisión errónea de datos. (fallo del Juzg. CAyT N.º 4, Sec. 7, Observatorio de Derecho Informático Argentino (ODIA) y otros c/ GCBA s/ amparo – otros, Expte. N.º 182908/2020-0. (Septiembre de 2022) El fallo está disponible en el siguiente link:

<https://repositorio.mpd.gov.ar/jspui/handle/123456789/4658>

¹⁷ La infraestructura de vigilancia se enmarca en gran medida en el Programa Trenes Seguros, de jurisdicción nacional, mediante el cual se instalaron cámaras y centros de monitoreo en múltiples estaciones de tren gestionadas por el gobierno nacional. Más información: <https://www.argentina.gob.ar/viajaseguro/si-viajas-en-tren> Consultado en marzo 2026.

¹⁸ Procedimiento judicial expedito destinado a la protección de los derechos fundamentales frente a actos u omisiones que los vulneren o amenacen con vulnerarlos.

¹⁹ En el marco de la causa “Observatorio de Derecho Informático Argentino O.D.I.A. y otros c/ GCBA s/ amparo - otros”. Sentencia del Juzgado CAyT de la CABA del 7 de septiembre de 2022 disponible en: <https://repositorio.mpd.gov.ar/jspui/handle/123456789/4658> Consultado en diciembre 2025.

opacidad y falta de certidumbre legal respecto de su operación fue advertida por organizaciones de la sociedad civil.²⁰

Brasil es un caso paradigmático por el uso de reconocimiento facial durante eventos masivos, como en espectáculos deportivos y grandes eventos, donde las autoridades reportaron detenciones basadas en coincidencias biométricas.²¹ Estas experiencias han sido presentadas como exitosas en términos de seguridad, pero organizaciones de derechos humanos han advertido sobre los sesgos estructurales y los errores sistemáticos de identificación que estas tecnologías implican, con una resultante y bien documentada reproducción de desigualdades y discriminación sobre poblaciones negras, indígenas y otras personas.²²

Otro ámbito clave es la vigilancia digital focalizada y la interceptación de comunicaciones. En México el uso y la documentación del software Pegasus para espiar a periodistas,²³ activistas y figuras públicas evidenció la adquisición de herramientas de ciberespionaje por parte de agencias estatales.²⁴ En El Salvador, organizaciones internacionales han señalado el uso de tecnologías para monitorear comunicaciones en el contexto del régimen de excepción.²⁵ Estos casos muestran cómo la vigilancia no se limita al espacio físico, sino que se extiende al entorno digital.

También es relevante el desarrollo de bases de datos biométricos y sistemas de identificación nacional. Países como Argentina y Chile han modernizado sus registros civiles incorporando huellas digitales, reconocimiento facial y verificación remota de identidad para trámites públicos, una tendencia que se incrementó luego de la pandemia de Covid-19, en 2020. Si bien estas innovaciones pretenden mejorar la eficiencia administrativa, también amplían la capacidad estatal de rastrear movimientos y actividades de la población a una escala sin precedentes.

Organizaciones de la sociedad civil protectoras de derechos humanos vienen siguiendo este fenómeno. Todos estos procesos, por citar algunos ejemplos, fueron analizados recientemente en una publicación del colectivo Al Sur²⁶, donde se sostiene que el uso de estas tecnologías no solo se incrementa en contextos de ausencia de regulación específica, como también se enmarca en una tendencia regional a legitimar medidas de vigilancia masiva e indiscriminada incompatibles con los estándares internacionales de derechos humanos. La organización Access Now también analizó en detalle²⁷ el suministro de las tecnologías utilizadas para la vigilancia en la región, y afirmó que las empresas que las proveen están pasando inadvertidas, vendiendo tecnología de vigilancia que se despliega en toda América Latina “sin la transparencia ni el escrutinio público suficientes”, y cuyas herramientas, según el estudio, se ven frecuentemente implicadas en violaciones de derechos humanos perpetradas contra la sociedad civil.

De esta manera, podemos ver tendencias y patrones comunes en la región: una expansión acelerada en la implementación de tecnologías de vigilancia, que se ve agravada por marcos normativos insuficientes y mecanismos de control público débiles o inexistentes.

²⁰ Más información en <https://r3d.mx/2025/08/26/ojos-que-vigilan-ciudad-de-mexico-sera-la-ciudad-mas-videovigilada-de-america-latina/> Consultado en febrero 2026.

²¹ El proyecto O Panóptico lleva un registro de los usos de reconocimiento facial en distintas regiones del país. Disponible en: <https://www.opanoptico.com.br/> Consultado en febrero 2026.

²² El proyecto “Tire Meu Rosto da Sua Mira” reclama la suspensión de los sistemas de reconocimiento facial en Brasil, por su uso “abusivo y poco transparente”. Su campaña está disponible en: <https://tiremeurostodasuamira.org.br/> Consultado en febrero 2026.

²³ El *Security Lab* de Amnistía Internacional tuvo un rol importante en la exposición de la evidencia forense relevante: Ver: <https://www.amnesty.org/en/latest/news/2022/03/the-pegasus-project-how-amnesty-tech-uncovered-the-spyware-scandal-new-video/>

²⁴ México fue el estado con más víctimas documentadas del sistema Pegasus, con 456 personas espiadas. Más información: <https://r3d.mx/2025/04/14/gobierno-mexicano-uso-pegasus-para-espiar-al-menos-a-456-personas-en-2019/> Consultado en febrero 2026.

²⁵ Más información: <https://articulo19.org/investigaciones-periodisticas-revelan-estrategias-hechas-por-funcionarios-allegados-a-bukele-para-espiar-y-vigilar-a-funcionarios-del-gobierno-y-periodistas-con-voces-criticas/> Consultado en febrero 2026.

²⁶ Al Sur (2025) Tendencias y prácticas de vigilancia en América Latina. Estudios de caso de Brasil, Chile, Colombia, El Salvador, México, Perú y Paraguay. Link:

<https://www.alsur.lat/reporte/tendencias-practicas-vigilancia-en-america-latinaestudios-caso-brasil-chile-colombiael>

²⁷ Access Now (2021) Tecnologías de Vigilancia en América Latina: Hecha en el exterior, utilizada en casa <https://www.accessnow.org/tecnologia-de-vigilancia-en-america-latina/>

3. ESTÁNDARES LEGALES APLICABLES AL USO DE TECNOLOGÍAS DE VIGILANCIA EN ARGENTINA

El marco normativo aplicable al uso de tecnologías de vigilancia en Argentina se inscribe en un conjunto de obligaciones en materia de derechos humanos que comprende el derecho internacional de derechos humanos con jerarquía constitucional y la legislación nacional específica sobre protección de datos personales y acceso a la información pública.²⁸ Este conjunto normativo establece límites claros al despliegue de tecnologías de vigilancia, particularmente cuando estas pueden afectar derechos humanos como la privacidad, la libertad de expresión, la libertad de asociación, la libertad de reunión, la participación política, que son el objeto de análisis de esta investigación.

En este capítulo, se presenta un análisis estructurado a partir de los derechos específicos que serán analizados en este informe, en función de los distintos marcos normativos: los instrumentos del ámbito internacional, en particular el Pacto Internacional de Derechos Civiles y Políticos (PIDCP),²⁹ como principal referencia para el respeto de la privacidad, la libertad de expresión y la libertad de asociación frente a prácticas de vigilancia. En segundo lugar, se analizan los tratados y estándares del sistema interamericano de protección de derechos humanos, dada su centralidad en la región y el desarrollo específico de criterios aplicables a contextos de protesta, actividad periodística y participación política. Finalmente, se consideran los desarrollos normativos y de política pública relevantes a nivel nacional y local, en particular la normativa en materia de protección de datos personales, acceso a la información pública y otras regulaciones aplicables al accionar estatal, que establecen límites y obligaciones concretas al uso de tecnologías de vigilancia.

²⁸ La reforma constitucional de 1994 incorporó al bloque de constitucionalidad argentino diversos tratados internacionales de derechos humanos, otorgándoles jerarquía constitucional y carácter directamente aplicable y obligatorio para todas las autoridades del Estado (art. 75 inc. 22, Constitución Nacional).

Disponible en:

https://www.argentina.gob.ar/sites/default/files/derechoshumanos_publicaciones_colecciondebolsillo_01_constitucion_nacion_argentina.pdf

²⁹ Disponible en:

https://www.argentina.gob.ar/sites/default/files/derechoshumanos_publicaciones_colecciondebolsillo_06_derechos_civiles_politicos.pdf

3.1 DERECHO A LA PRIVACIDAD Y PROTECCIÓN DE DATOS PERSONALES

En el ámbito internacional, el mencionado Pacto Internacional de Derechos Civiles y Políticos constituye el principal instrumento vinculante para el análisis del uso de tecnologías de vigilancia. En particular, su artículo 17 protege a todas las personas frente a injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia, así como frente a ataques ilegales a su honra y reputación. Este derecho humano resulta especialmente relevante frente a prácticas de vigilancia que implican la recolección, el almacenamiento y el análisis sistemático de información personal, tanto en entornos digitales como físicos.

En el ámbito regional, la Convención Americana sobre Derechos Humanos (Convención Americana)³⁰ refuerza y complementa las obligaciones del Estado argentino para proteger el derecho a la vida privada y a la honra (art. 11).

A nivel interno, la Constitución Nacional garantiza la protección de la privacidad (art. 19) y reconoce la inviolabilidad de la correspondencia y los papeles privados. Asimismo, la reforma constitucional de 1994 incorporó expresamente el derecho a la protección de los datos personales, reconociendo el derecho de toda persona a conocer, actualizar y suprimir información sobre sí misma contenida en registros o bancos de datos, públicos o privados (art. 43). Este reconocimiento adquiere particular relevancia en contextos de vigilancia tecnológica, donde la recolección y el tratamiento de información personal pueden realizarse de manera masiva, sistemática y con escasa visibilidad pública.

La normativa nacional de protección de datos personales³¹ establece los principios que deben regir el tratamiento de datos por parte del Estado, incluyendo los de legalidad, finalidad, proporcionalidad, calidad y seguridad de la información. Estos principios resultan directamente aplicables a los sistemas de vigilancia y a las tecnologías utilizadas para la identificación, el seguimiento o el perfilamiento de personas. En particular, la exigencia de finalidades determinadas y explícitas, así como la prohibición de tratamientos excesivos o incompatibles con los objetivos declarados (art. 4), constituye un límite relevante frente a prácticas de vigilancia que pueden derivar en persecución política, sindical o laboral, o en la criminalización de la protesta social y la labor periodística. En este mismo sentido, Argentina ha adherido³² al Convenio 108+ del Consejo de Europa, asumiendo compromisos internacionales relevantes en materia de protección de datos personales, aun cuando estos no hayan sido plenamente reflejados en la legislación interna vigente. Este convenio representa un estándar de protección orientado específicamente a la protección frente al tratamiento automatizado de datos.

3.2 Libertad de expresión

El Pacto Internacional de Derechos Civiles y Políticos (art. 19) y la Convención Americana (art. 13) garantizan la libertad de expresión. A nivel interno, la Constitución Nacional garantiza la libertad de expresión en los artículos 14 y 32.

En el sistema interamericano, la Relatoría Especial para la Libertad de Expresión de la CIDH (RELE) ha desarrollado estándares específicos sobre vigilancia, criminalización de la protesta y restricciones indirectas al ejercicio de derechos, estándares que resultan directamente aplicables al análisis de tecnologías que monitorean, identifican o registran a personas en contextos de manifestación pública.

En junio de 2024, la CIDH y la RELE expresaron su preocupación por el uso desproporcionado de la fuerza contra manifestantes y periodistas durante las protestas en Argentina, reiterando que el Estado debe tratar la protesta pacífica como ejercicio legítimo de derechos, abstenerse de criminalizarla o estigmatizarla, y garantizar condiciones seguras para el periodismo.³³

El vínculo entre libertad de expresión y vigilancia tecnológica fue explicitado en 2025, en una declaración conjunta de la Relatoría de la ONU sobre reunión y asociación, la RELE y otras relatorías regionales³⁴. Allí advirtieron que el uso arbitrario e ilegal de tecnologías de vigilancia, como spyware, reconocimiento facial con inteligencia artificial, amplifica la criminalización de la protesta y la sociedad civil. La declaración señala que estas herramientas habilitan detenciones preventivas incluso tiempo después de una manifestación y generan un efecto disuasorio sobre la organización, la participación y la cobertura periodística. En

³⁰ Disponible en: https://www.oas.org/dil/esp/1969_Convencion_Americana_sobre_Derechos_Humanos.pdf

³¹ Ley 25.326. Disponible en: <https://servicios.infoleg.gob.ar/infolegInternet/anexos/60000-64999/64790/texto.htm> Consultado en diciembre de 2025.

³² Mediante la Ley 27.699, de noviembre de 2022. Disponible en: <https://www.boletinoficial.gob.ar/detalleAviso/primera/276783/20221130> Consultado en diciembre de 2025.

³³ Disponible en: <https://www.oas.org/es/cidh/jsForm/?File=/es/cidh/prensa/comunicados/2024/158.asp> Consultado en diciembre de 2025.

³⁴ Disponible en: https://www.oas.org/es/cidh/jsForm/?File=/es/cidh/expresion/documentos_basicos/declaraciones/2025.asp Consultado en diciembre de 2025.

consecuencia, llama a prohibir la vigilancia masiva e indiscriminada en contextos de protesta y a establecer salvaguardas estrictas que incluyen decisiones caso por caso, transparencia, supervisión independiente y mecanismos de reparación.

3.3 LIBERTAD DE REUNIÓN PACÍFICA Y ASOCIACIÓN

El Pacto Internacional de Derechos Civiles y Políticos reconoce la libertad de asociación (art. 22) y el derecho de reunión pacífica (art. 21). La Convención Americana protege la libertad de reunión pacífica (art. 15) y la libertad de asociación (art. 16), derechos que el sistema interamericano ha interpretado de manera interdependiente. A nivel interno, la Constitución Nacional garantiza el derecho a asociarse y reunirse en el artículo 14 bis.

Tanto el Comité de Derechos Humanos como la CIDH han reconocido que la mera existencia de prácticas de vigilancia ilegítimas o desproporcionadas puede generar efectos disuasorios sobre la participación política, la organización colectiva, la actividad sindical, la protesta social o el ejercicio del periodismo, aún en ausencia de sanciones explícitas o restricciones formales. Ese principio está desarrollado con precisión en la Observación General Nro. 37 del Comité de Derechos Humanos (2020), dedicada al derecho de reunión pacífica. El Comité establece allí que ese derecho no se limita al espacio físico público, sino que abarca también los entornos digitales, y advierte que las tecnologías de vigilancia, aunque puedan usarse legítimamente para detectar amenazas de violencia, comprometen la privacidad de participantes y transeúntes y pueden desalentar el ejercicio mismo del derecho que pretenden proteger.³⁵

En el plano regional, la CIDH documentó esa dinámica en concreto: en sus observaciones tras la visita a Colombia (junio de 2021), identificó que el perfilamiento de usuarios de redes sociales y la estigmatización de manifestantes mediante categorías como "terrorismo" o "vandalismo" generan un entorno hostil con efecto disuasorio sobre la protesta y la libertad de expresión, especialmente en entornos digitales.³⁶ La referencia es pertinente como precedente regional aplicable al análisis de prácticas similares en Argentina.

3.4 DERECHO A LA IGUALDAD Y NO DISCRIMINACIÓN

El derecho a la igualdad y a la no discriminación constituye un principio transversal del derecho internacional de los derechos humanos y un eje interpretativo clave para analizar el uso de tecnologías de vigilancia. El Pacto Internacional de Derechos Civiles y Políticos establece en sus artículos 2 y 26 la obligación de los Estados de garantizar a todas las personas el goce de los derechos reconocidos en el tratado sin distinción alguna, así como el derecho autónomo a la igualdad ante la ley y a la protección contra toda forma de discriminación.

En el ámbito regional, la Convención Americana consagra este principio en sus artículos 1.1 y 24, estableciendo la obligación de respetar y garantizar los derechos sin discriminación y reconociendo el derecho a la igualdad ante la ley.

Aplicado al uso de tecnologías de vigilancia, este marco normativo adquiere particular relevancia frente a los riesgos de sesgos algorítmicos o perfilamiento automático. Un informe reciente³⁷ de la Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos, que analiza el papel de los datos como fuente de discriminación y desigualdad en sectores clave, advierte que los sistemas automatizados y de reconocimiento biométrico pueden incorporar sesgos y generar impactos desproporcionados sobre determinados grupos, así como facilitar el perfilamiento basado en características protegidas y la identificación de manifestantes y disidentes, lo que puede constituir una forma de discriminación.³⁸

Frente a esos riesgos, los estándares internacionales han comenzado a exigir evaluaciones de impacto en derechos humanos que contemplen específicamente los riesgos de discriminación en el diseño e implementación de sistemas tecnológicos. Eso implica transparencia en los criterios de funcionamiento,

³⁵ Publicado en CCPR/C/GC/37, disponible en: <https://docs.un.org/es/CCPR/C/GC/37> Consultado en diciembre de 2025.

³⁶ Las observaciones y recomendaciones de la CIDH están disponibles en este link:

https://www.oas.org/es/cidh/informes/pdfs/ObservacionesVisita_CIDH_Colombia_SPA.pdf Consultado en diciembre de 2025.

³⁷ Publicado en A/HRC/56/68, de 2024. Disponible en: <https://docs.un.org/es/A/HRC/56/68>

³⁸ Publicado en A/HRC/60/45, de 2025. Disponible en: https://digitallibrary.un.org/record/4088727/files/A_HRC_60_45-ES.pdf

auditabilidad de los algoritmos, calidad y representatividad de los datos, y mecanismos efectivos de supervisión y rendición de cuentas.³⁹

EL TEST DE TRES PARTES: LEGALIDAD, LEGITIMIDAD Y PROPORCIONALIDAD

El PIDCP (arts. 17, 19, 21 y 22) y la Convención Americana (arts. 11, 13, 15 y 16) comparten una arquitectura común: reconocen de manera expresa la protección de la vida privada, la libertad de expresión, la libertad de reunión pacífica y la libertad de asociación, y prohíben injerencias arbitrarias, pero a la vez admiten restricciones bajo condiciones estrictas.

Toda medida de vigilancia estatal, incluidas las mediadas por tecnologías digitales o sistemas automatizados, debe cumplir tres requisitos: estar prevista por ley, perseguir un fin legítimo, y ser necesaria y proporcional al objetivo que se invoca. En el derecho internacional de los derechos humanos, esta exigencia se conoce como el test de tres partes o prueba tripartita⁴⁰. Los tres requisitos operan de manera conjunta y acumulativa: el incumplimiento de cualquiera de ellos hace incompatible la medida con el derecho internacional, sin importar que los restantes estén satisfechos.

Legalidad: La vigilancia debe ser acompañada por una norma accesible, precisa y previsible. No alcanza con que exista una ley: la ley debe definir con claridad quién puede ordenar la vigilancia, bajo qué condiciones, con qué alcance y por cuánto tiempo. En el contexto tecnológico, esto significa que los sistemas no deben ser desplegados sin base legal explícita, autorizaciones ambiguas que habilitan usos discrecionales, o marcos normativos que no contemplan las capacidades específicas de las herramientas utilizadas. Ejemplos de tecnologías que caen en esta categoría incluyen el reconocimiento facial o analíticas predictivas basadas en vigilancia masiva.

Legitimidad: La medida debe perseguir un fin reconocido como legítimo por el derecho internacional: seguridad nacional, orden público, salud pública o protección de los derechos de terceros. Este elemento opera como un filtro de propósito: la vigilancia orientada a monitorear la actividad política, sindical o periodística, o a identificar participantes en protestas sociales, no satisface este requisito aunque esté formalmente autorizada. En casos donde el fin declarado es la seguridad pero el uso efectivo es el control de la disidencia, la medida falla en este umbral.

Necesidad y proporcionalidad. La medida debe ser la menos restrictiva disponible para alcanzar el objetivo legítimo, y el grado de afectación a los derechos no puede ser mayor al estrictamente necesario. Aplicado a la vigilancia digital, esto implica que la vigilancia masiva e indiscriminada es incompatible con este estándar por definición: si el objetivo puede alcanzarse mediante vigilancia dirigida con orden judicial, el despliegue de sistemas de reconocimiento facial en espacios públicos o el monitoreo de redes sociales a escala no supera este test. La proporcionalidad también exige que las afectaciones colaterales sobre transeúntes, periodistas, personas no investigadas sean mínimas y justificadas.

En este marco, la prueba de las tres partes opera como una herramienta clave para evaluar no sólo las restricciones expresas, sino también aquellas injerencias estatales que, por su alcance, opacidad o intensidad, resultan incompatibles con estándares regionales e internacionales de derechos humanos.

³⁹ Por ejemplo, la metodología de Evaluación de Impacto en Derechos Humanos, Democracia y Estado de Derecho Para Sistemas de Inteligencia Artificial (HUDERIA, por sus siglas en inglés) impulsado por el Consejo de Europa. Disponible en: <https://www.coe.int/en/web/artificial-intelligence/huderia-risk-and-impact-assessment-of-ai-systems>

⁴⁰ Este estándar ha sido desarrollado y precisado por órganos internacionales de interpretación autorizada, en particular por el Comité de Derechos Humanos de las Naciones Unidas (CCPR, por sus siglas en inglés), que en su Observación General N° 34 de 2011 sostuvo que toda restricción a la libertad de expresión debe cumplir de manera estricta y acumulativa con los requisitos de legalidad, finalidad legítima y necesidad y proporcionalidad, y que el incumplimiento de cualquiera de ellos hace incompatible la medida con el PIDCP. Disponible en: <https://www.acnur.org/fileadmin/Documentos/BDL/2012/8507.pdf> Consultado en diciembre de 2025.

En el mismo sentido, la Corte Interamericana de Derechos Humanos (Corte IDH) ha reiterado que las restricciones a los derechos protegidos por la Convención Americana deben ser excepcionales, estar claramente delimitadas y no vaciar el contenido esencial del derecho afectado. Ver, por ejemplo, la Opinión Consultiva OC-5/85. Disponible en: https://www.corteidh.or.cr/docs/opiniones/seriea_05_esp.pdf Consultado en diciembre de 2025.

3.5 TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PÚBLICA

La normativa nacional de acceso a la información pública⁴¹ establece obligaciones de transparencia activa y pasiva que resultan centrales para la supervisión de las políticas de vigilancia, al permitir conocer qué tecnologías se adquieren, con qué finalidades, bajo qué marcos normativos y con qué salvaguardas institucionales. Sin embargo, el gobierno de Javier Milei generó una regresión en este sentido, al incorporar un instrumento reglamentario con una visión restrictiva del alcance de la ley, dado que amplía las excepciones y permite negar información con criterios más amplios.⁴²

3.6 ESTÁNDARES INTERNACIONALES NO PRESCRIPTIVOS Y DESARROLLOS RECIENTES

Junto a los instrumentos jurídicamente vinculantes, existen estándares internacionales de carácter no prescriptivo que resultan relevantes para el análisis del uso de tecnologías de vigilancia. En este ámbito, la UNESCO ha impulsado procesos multilaterales orientados a promover el uso ético de tecnologías automatizadas e inteligencia artificial, con un enfoque centrado en los derechos humanos. En años recientes, Argentina no solo participó activamente en estos procesos, sino que también avanzó en la elaboración de lineamientos y recursos normativos inspirados en la Recomendación sobre la Ética de la Inteligencia Artificial adoptada por dicho organismo.⁴³ Asimismo, el Estado argentino fue signatario de la Declaración de Santiago,⁴⁴ adoptada en el marco de la Cumbre Ministerial sobre Ética de la Inteligencia Artificial en América Latina y el Caribe, celebrada en octubre de 2023, es decir, pocos meses antes del cambio de gobierno. Sin embargo, el gobierno de la gestión de Javier Milei no suscribió la Declaración de Montevideo, el documento de la última reunión ministerial que tuvo lugar en dicha ciudad, en octubre de 2024.⁴⁵

A partir de este marco, el apartado siguiente se centra en el análisis de las políticas implementadas por el nuevo gobierno, con particular atención al uso de tecnologías para la vigilancia, su encuadre normativo y sus efectos sobre el ejercicio de los derechos humanos.

⁴¹ Ley 27.275. Disponible en: <https://servicios.infoleg.gob.ar/infolegInternet/anexos/265000-269999/265949/norma.htm> Consultado en diciembre de 2025.

⁴² Se trata del Decreto 780/2024. Para más información sobre las restricciones generadas por el Decreto, sugerimos este artículo de la Asociación por la Igualdad y la Justicia (AIJ): <https://acij.org.ar/el-poder-ejecutivo-reglamento-de-forma-restrictiva-y-regresiva-el-derecho-de-acceso-a-la-informacion-publica/> Consultado en diciembre de 2025.

⁴³ Más información en este artículo de la UNESCO: <https://www.unesco.org/es/articles/argentina-implementa-normativa-en-base-la-recomendacion-sobre-la-etica-de-la-inteligencia-artificial> Consultado en diciembre de 2025.

⁴⁴ Disponible en: https://minciencia.gub.cl/uploads/filer_public/40/2a/402a35a0-1222-4dab-b090-5c81bbf34237/declaracion_de_santiago.pdf Consultado en diciembre de 2025.

⁴⁵ Más información en: <https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-conocimiento/comunicacion/noticias/aprobacion-declaracion-montevideo> Consultado en diciembre de 2025.

4. IMPACTOS EN LOS DERECHOS HUMANOS DE LAS TECNOLOGÍAS DE VIGILANCIA

A la luz de los principios y estándares internacionales de derechos humanos expuestos, resulta necesario atender a ciertas características estructurales de estas tecnologías, que plantean preocupaciones específicas para los derechos humanos, en particular cuando permiten recolectar, integrar y analizar grandes volúmenes de información personal, automatizar procesos de identificación o clasificación, inferir vínculos o comportamientos, y ampliar la capacidad estatal de monitoreo sobre la población.

Estas tecnologías no son neutrales. Su diseño, las fuentes de datos que utilizan, los criterios con los que operan y los contextos en los que se despliegan pueden afectar de manera directa o indirecta derechos como la privacidad, la libertad de expresión, la libertad de reunión y asociación, la igualdad y no discriminación, así como el acceso a la información y las garantías frente al ejercicio arbitrario del poder estatal. Además, su uso suele caracterizarse por altos niveles de opacidad, dificultades de supervisión, dependencia de proveedores privados y escasas posibilidades de control o impugnación por parte de las personas afectadas.

En este marco, antes de examinar de manera específica las tecnologías adquiridas o utilizadas por el gobierno nacional, son subrayados los principales riesgos que puede tener el despliegue de los tres tipos de tecnología que son de interés para este análisis, desde una perspectiva de derechos humanos.

4.1 RECONOCIMIENTO DE IMÁGENES Y BIOMETRÍA

Las tecnologías de reconocimiento de imágenes y biometría permiten procesar rasgos físicos o conductuales de las personas, como el rostro, la huella dactilar, la voz o ciertos patrones corporales, con el objetivo de identificarlas, verificar su identidad o seguir sus movimientos a través de distintos entornos. En el caso del reconocimiento facial aplicado a cámaras de videovigilancia, estas herramientas pueden convertir registros visuales del espacio público en mecanismos de identificación y rastreo individualizado, habilitando formas de vigilancia persistente y a gran escala de grupos de individuos.

Es importante distinguir entre los diferentes tipos de reconocimiento facial, que generalmente se presentan en dos modalidades: 1:n (reconocimiento facial para *identificación*, o *de uno a muchos*) y 1:1 (reconocimiento facial para *autenticación* o verificación, o *de uno a uno*). La investigación de Amnistía Internacional, incluido el presente informe, se centra en el reconocimiento facial para identificación, ya que

esta tecnología está diseñada sobre la base de la vigilancia masiva por diseño (como fue establecido previamente por Amnistía Internacional), y su utilización genera vulneraciones inadmisibles de los derechos a la privacidad, la igualdad y la no discriminación, así como de otros derechos humanos conexos, entre ellos la libertad de reunión pacífica y de asociación.⁴⁶

Los sistemas de reconocimiento facial para identificación pueden ser diferenciados entre los que funcionan *en tiempo real* y aquellos utilizados de forma retrospectiva (*ex post*). Los primeros operan de forma simultánea a la captación de imágenes, identificando o verificando personas mientras circulan por el espacio público y habilitando respuestas inmediatas por parte de las fuerzas de seguridad. En cambio, los usos *ex post* consisten en el análisis posterior de imágenes o registros audiovisuales ya capturados, por ejemplo, grabaciones de cámaras de seguridad, fotografías o videos de redes sociales, con el objetivo de identificar personas luego de ocurrido un hecho determinado. Aunque suelen presentarse como herramientas de investigación forense, estos sistemas también amplían significativamente las capacidades estatales de identificación y rastreo retrospectivo, especialmente cuando se combinan con bases masivas de datos biométricos o motores de búsqueda facial contruidos a partir de imágenes obtenidas de internet.

La especial sensibilidad de estas tecnologías radica en que operan sobre datos biométricos, es decir, sobre información íntimamente vinculada a la identidad de las personas. Su uso puede afectar gravemente el derecho a la privacidad y a la protección de datos personales, pero también incidir sobre la libertad de circulación, la libertad de expresión y el derecho a la protesta, especialmente cuando posibilita la identificación de personas en manifestaciones, reuniones o actividades políticas. A ello se suman problemas de opacidad, errores de identificación, sesgos algorítmicos y riesgos de discriminación, particularmente cuando los sistemas se entrenan con datos no representativos de las personas sobre las que operan, o se utilizan sobre grupos históricamente expuestos a prácticas de vigilancia selectiva. Aun cuando la tecnología “funciona” a nivel técnico, las investigaciones de Amnistía Internacional han demostrado que los agentes encargados de hacer cumplir la ley pueden identificar rápidamente a las personas manifestantes para acosarlas, y que esta tecnología corre el riesgo de reforzar los patrones existentes de actuación policial discriminatoria.⁴⁷

El caso del Sistema de Reconocimiento Facial de Prófugos de la Ciudad de Buenos Aires da cuenta de los potenciales usos abusivos que el gobierno puede realizar sin las medidas de control efectivo ni normativa clara sobre medidas de auditoría y reparación. Como fue detallado en el apartado 2.2, este sistema fue implementado con datos desactualizados o erróneos, y el Gobierno lo utilizó para seguir personas que no tenían pedido de captura, además de no haber implementado los mecanismos de control necesarios.

En cuanto a estudios de caso fuera de América Latina, resulta ilustrativo observar contexto documentados por Amnistía Internacional en el marco del proyecto Ban The Scan.⁴⁸ Estas investigaciones muestran que el reconocimiento facial no solo amplía la capacidad estatal de vigilancia, sino que ha sido utilizado en contextos concretos para identificar, rastrear y detener personas, incluyendo manifestantes y activistas. En ciudades como Nueva York, se ha documentado el uso reiterado de estas herramientas por parte de fuerzas policiales a gran escala, en investigaciones que revelaron que estas tecnologías fueron utilizadas de forma arbitraria sobre personas que protestan.⁴⁹ La investigación también reveló que la exposición a reconocimiento facial está centrada asimétricamente en comunidades históricamente marginalizadas y, en particular, racializadas.⁵⁰ En otros casos, como Hyderabad,⁵¹ el despliegue de infraestructuras masivas de videovigilancia integradas con reconocimiento facial en tiempo real se ha realizado en ausencia de marcos normativos adecuados, ampliando significativamente la capacidad estatal de monitoreo sin garantías suficientes. El Centro de Comando y Control de Hyderabad permite procesar datos procedentes de hasta 600.000 cámaras de forma simultánea, con la posibilidad de ampliar considerablemente esta capacidad en toda la región. Estas cámaras pueden utilizarse en combinación con el software de reconocimiento facial ya empleado por la Policía de Hyderabad para rastrear a personas.⁵² Finalmente, en contextos como los

⁴⁶ Amnistía Internacional, Ban the Scan, <https://banthescan.amnesty.org/>

⁴⁷ Amnistía Internacional, USA: Facial recognition technology reinforcing racist stop-and-frisk policing in New York – new research, 15 February 2022, <https://www.amnesty.org/en/latest/news/2022/02/usa-facial-recognition-technology-reinforcing-racist-stop-and-frisk-policing-in-new-york-new-research/> (accessed on 17 July 2026)

⁴⁸ Link al informe completo: <https://banthescan.amnesty.org/nyc/index.html>

⁴⁹ Amnistía Internacional, USA: Facial recognition technology reinforcing racist stop-and-frisk policing in New York – new research, 15 February 2022, <https://www.amnesty.org/en/latest/news/2022/02/usa-facial-recognition-technology-reinforcing-racist-stop-and-frisk-policing-in-new-york-new-research/> (accessed on 17 July 2026)

⁵⁰ Amnistía Internacional, Amnesty International, S.T.O.P. Lawsuit Reveals NYPD Surveillance Abuses, 13 November 2025, <https://www.amnesty.org/en/latest/news/2025/11/amnesty-and-s-t-o-p-reveal-nypd-surveillance-abuses/> (accessed on 17 July 2026)

⁵¹ Link al informe completo: <https://banthescan.amnesty.org/hyderabad/index.html>

⁵² Amnistía Internacional, India: Hyderabad ‘on the brink of becoming a total surveillance city’, 9 November 2021, <https://www.amnesty.org/en/latest/news/2021/11/india-hyderabad-on-the-brink-of-becoming-a-total-surveillance-city/> (accessed on 17 July 2026)

Territorios Ocupados de Palestina, estas tecnologías han sido utilizadas como parte de sistemas más amplios de control poblacional, facilitando formas de vigilancia permanente y diferenciada que impactan de manera directa sobre los derechos de los Palestinos, incluyendo la restricción arbitraria de la libertad de movimiento y la violación de los derechos a la privacidad, la igualdad y la no discriminación.⁵³

Amnistía Internacional concluyó que las tecnologías de reconocimiento facial para la identificación y vigilancia masiva son fundamentalmente incompatibles con la legislación internacional de derechos humanos y por eso es necesaria su prohibición.⁵⁴

4.2 PREDICCIÓN DE DELITOS Y DELIMITACIÓN DE ÁREAS DE VIGILANCIA

Las tecnologías de predicción de delitos y delimitación de áreas a vigilar y someter a control policial utilizan grandes volúmenes de datos y técnicas algorítmicas para identificar patrones, establecer correlaciones y producir estimaciones sobre posibles conductas futuras, zonas consideradas de riesgo o personas que podrían ser objeto de atención policial. Aunque suelen presentarse como herramientas orientadas a optimizar recursos y prevenir delitos, en los hechos introducen mecanismos de clasificación y anticipación que pueden influir en decisiones estatales con impactos significativos de derechos humanos en individuos y territorios.

La policía lleva décadas registrando datos: dónde hubo arrestos, a quiénes detuvo, qué barrios patrulló más. Un algoritmo de predicción de delitos toma esos datos históricos, encuentra patrones y produce dos tipos de resultados: mapas de zonas "de riesgo" (dónde el sistema estima que hay más probabilidad de que ocurra un delito) o puntajes de riesgo individuales (qué probabilidad tiene una persona de cometer o ser víctima de un delito). El problema central es que esos datos históricos no son neutrales: reflejan las decisiones pasadas de la propia policía. Si históricamente se patrulló más en barrios pobres o se detuvo más a personas de ciertos grupos, eso es lo que el sistema registra como "zona de riesgo" o "perfil de riesgo", no necesariamente donde más delitos ocurren. El algoritmo aprende de esa historia y predice más delitos en los mismos lugares y sobre las mismas personas. Se envía más efectivos ahí, produce más arrestos, y esos nuevos datos alimentan la próxima predicción. El sistema se retroalimenta, no detecta dónde hay delito, sino que confirma y amplifica dónde la policía ya intervenía.

Desde el punto de vista de los derechos humanos, estas tecnologías despiertan preocupaciones porque tienden a basarse en datos históricos atravesados por sesgos institucionales, reforzando prácticas previas de discriminación policial, estigmatización basada en el territorio y discriminación estructural. En este sentido, estos sistemas perpetúan y reproducen desigualdades, especialmente cuando asocian riesgo con determinados barrios, grupos sociales o características personales. Asimismo, su funcionamiento suele ser difícil de auditar y explicar debido a su opacidad, en términos de la información acerca de qué sistemas son usados, sus especificaciones técnicas, su justificación legal y su alimentación desde bases de datos sensibles. Esto es típicamente un resultado del uso de excepciones por parte de las fuerzas de seguridad para eludir la aplicación de la legislación en materia de protección de datos. Esto obstaculiza el control, la rendición de cuentas y la posibilidad de cuestionar decisiones que afectan derechos. Por ello, su uso exige un escrutinio dada la documentada violación de los principios de legalidad, necesidad y proporcionalidad en perpetuar la discriminación. Amnistía Internacional ha llamado previamente a la prohibición de los sistemas de policiamiento predictivo.⁵⁵

En el informe "*Automated Racism*",⁵⁶ publicado en 2025, Amnistía Internacional, ha documentado los impactos de estos sistemas y muestra que al menos 33 fuerzas policiales en el Reino Unido han utilizado sistemas de predicción, perfilamiento o evaluación de riesgo, basados en datos provenientes del propio sistema policial y de justicia penal. Estos datos reflejan prácticas estructurales de discriminación y sesgos institucionales, como registros de inteligencia policial, detenciones, controles o requisas, en los que determinados grupos y territorios se encuentran sobrerrepresentados como resultado de prácticas previas de vigilancia selectiva. En consecuencia, los sistemas algorítmicos desarrollados a partir de estos datos tienden a predecir una mayor probabilidad de delito en esas mismas áreas o a atribuir mayor riesgo a personas pertenecientes a ciertos grupos, en particular grupos racializados y comunidades históricamente

⁵³ Link al informe completo: <https://banthescan.amnesty.org/opt/index.html>

⁵⁴ Amnistía Internacional, Ban The Scan: <https://banthescan.amnesty.org/>

⁵⁵ Link al reporte: <https://media.amnesty.org.uk/documents/Automated20Racism20Report20-20Amnesty20International20UK20-202025.pdf>

⁵⁶ Ver nota anterior.

marginadas, orientando nuevas intervenciones policiales sobre ellos. Este proceso genera bucles de retroalimentación en los que los datos producidos por la propia actividad policial refuerzan nuevas predicciones sesgadas, profundizando la discriminación y la criminalización de manera estructural.

En la región, un antecedente particularmente relevante de este tipo de políticas es el del Sistema Predictivo del Delito Urbano, implementado en Chile, que puede ayudar a observar cómo la adopción de tecnologías de predicción del delito puede reforzar desigualdades preexistentes.⁵⁷ En el marco del estudio, se analizó que este sistema se alimentaba principalmente de dos fuentes de datos: casos policiales vinculados a delitos de mayor connotación social (DMCS) y registros de la plataforma AUPOL, operada por la fuerza de Carabineros, que incluye información personal de víctimas, testigos y denunciantes (como nombre, número de identificación, domicilio, género y profesión). Sin embargo, estos datos no son neutros: estos reflejan lógicas institucionales y sociales que pueden incorporar errores, prácticas arbitrarias o sesgos sistemáticos. La consecuencia es la generación de un sistema que tiende a reforzar patrones de vigilancia en zonas ya estigmatizadas, perpetuando controles de identidad preventivos y otras prácticas discriminatorias sin mecanismos claros de auditoría externa ni evaluación de impacto.

4.3 REVISIÓN DE REDES SOCIALES E INVESTIGACIÓN DE FUENTES ABIERTAS (OSINT)

Las herramientas de revisión de redes sociales e investigación de fuentes abiertas (OSINT, por su sigla en inglés) permiten recolectar, combinar y analizar información disponible en internet, como publicaciones en redes sociales, sitios web, foros, registros públicos y otras fuentes digitales abiertas. Aunque esta información haya sido publicada en entornos accesibles, su tratamiento automatizado y a gran escala modifica cualitativamente su alcance, al permitir reconstruir trayectorias, mapear vínculos entre personas, identificar patrones de comportamiento y generar perfiles o inferencias sobre actividades, opiniones, afinidades o relaciones sociales.

Estas capacidades generan preocupaciones porque amplían la posibilidad de monitoreo estatal intrusivo sobre la vida social y política de las personas sin necesidad de recurrir a medidas tradicionales. En particular, pueden afectar la privacidad, la libertad de expresión y la libertad de reunión pacífica y asociación, así como facilitar prácticas de perfilamiento o vigilancia selectiva sobre periodistas, activistas o personas críticas del gobierno. En esta línea, la Relatoría Especial para la Libertad de Expresión de la CIDH ha advertido, en el reporte “El impacto de la vigilancia digital en la libertad de expresión en las Américas”, que los Estados de la región recurren cada vez más a prácticas de “ciberpatrullaje” y perfilamiento en línea mediante herramientas avanzadas de inteligencia de fuentes abiertas, configurando nuevas formas de vigilancia masiva orientadas a monitorear y, en algunos casos, reprimir expresiones críticas. Según la información relevada, estas prácticas incluyen la contratación de servicios privados para analizar redes sociales, la caracterización de usuarios en función de sus opiniones sobre el gobierno, y la utilización de perfiles falsos por parte de fuerzas de seguridad para interactuar con personas en entornos digitales.⁵⁸

⁵⁷ Buschmann, J. (2021). Sistema predictivo del delito urbano: Producción algorítmica de zonas de vigilancia y control en la ciudad. Derechos Digitales. https://www.derechosdigitales.org/wp-content/uploads/02_Informe-Chile-Sistema-Predictivo-del-Delito-Urbano_ES_28042022.pdf

⁵⁸ Relatoría Especial para la Libertad de Expresión de la Comisión Interamericana de Derechos Humanos (RELE-CIDH). (2025) El impacto de la vigilancia digital en la libertad de expresión en las Américas. Link: <https://www.oas.org/es/cidh/expresion/informes/vigilanciaRELE.pdf>

5. POLÍTICAS Y TECNOLOGÍAS DE VIGILANCIA: UN NUEVO PARADIGMA

Desde el inicio de sus funciones en diciembre de 2023, el Gobierno actual en la Argentina generó una infraestructura orientada a aumentar su capacidad de vigilancia y control sobre el espacio público, tanto físico como digital, implementada mediante decretos y resoluciones del Poder Ejecutivo, sin participación del Congreso Nacional. Dicha infraestructura se configuró a través de la creación de nuevas áreas de gobierno, la publicación de protocolos específicos para las fuerzas federales, la modificación del Sistema de Inteligencia Nacional, la asignación presupuestaria, así como mediante una serie de compras y contrataciones destinadas a la implementación de estas nuevas funciones y objetivos.

Estas acciones del Gobierno pueden dividirse en dos dimensiones. Por un lado, las reformas institucionales necesarias para proveer las bases o los fundamentos sobre los que el sistema de vigilancia operará. Por otro lado, la creación de las condiciones operativas y materiales para ejercer las actividades de vigilancia y control de forma efectiva.

5.1 AMPLIACIÓN DEL ALCANCE DE INVESTIGACIÓN DEL SISTEMA DE INTELIGENCIA Y DE LAS FUERZAS FEDERALES

El gobierno generó la reforma de dos de las principales instituciones en términos de investigación de delitos federales: los sistemas de inteligencia y las fuerzas federales de seguridad. A continuación, se analizará en detalle en qué consistieron esas reformas y cómo aumentaron y habilitaron nuevas competencias para la vigilancia interna.

5.1.1 REFORMA DEL SISTEMA DE INTELIGENCIA NACIONAL

En julio de 2024, el Gobierno llevó adelante una reforma integral del Sistema de Inteligencia Nacional (SIN),⁵⁹ denominación oficial de la comunidad de inteligencia de la Argentina. El SIN fue creado en 2001 y su configuración actual resulta de las modificaciones introducidas por los decretos 614 y 615 de 2024⁶⁰ y 941 de diciembre de 2025.⁶¹ En apenas dos años de gestión, el gobierno actual realizó dos reformas estructurales del SIN.

El Decreto 941/2025 es de suma importancia para los fundamentos de la vigilancia interna, dado que separa la agenda de ciberseguridad, a la que separa del SIN⁶², de la ciberinteligencia, que deja bajo su competencia⁶³. Además, (i) amplía significativamente el alcance de las funciones de inteligencia y contrainteligencia mediante definiciones amplias y vagas que podrían habilitar la vigilancia de personas u organizaciones bajo un encuadre expansivo; (ii) establece el secreto como regla general para las actividades de inteligencia, debilitando la transparencia y la rendición de cuentas; (iii) fortalece la capacidad de los organismos para acceder a información en poder de otras agencias públicas y centralizar grandes volúmenes de datos personales sin controles judiciales robustos; (iv) habilita el intercambio de información con otros organismos, incluso potencialmente extranjeros, aumentando los riesgos de transferencias ulteriores y vacíos de responsabilidad; (v) autoriza la “aprehensión” de personas por parte de agentes de inteligencia sin control judicial y (vi) amplía el rol de las fuerzas armadas en tareas de inteligencia, todo ello en el marco de un decreto de necesidad y urgencia adoptado sin debate legislativo, lo que plantea serias objeciones constitucionales y preocupaciones en términos de Estado de derecho.⁶⁴

Esta reforma genera una nueva área específica para las tareas de inteligencia en el entorno digital, la Agencia Federal de Ciberinteligencia (AFC). Según establece el artículo 9 del Decreto 941/2025, será el órgano responsable de “la producción de Inteligencia Nacional sobre actores, hechos, riesgos, oportunidades y amenazas que se desarrollen en el dominio del ciberespacio y el espacio radioeléctrico y puedan afectar la seguridad nacional, las infraestructuras críticas digitales, el patrimonio del Estado Nacional, la soberanía tecnológica y/o la integridad de la información pública y privada”.⁶⁵ La formulación amplia de las funciones del área, sumado a las reformas generales enumeradas en el párrafo anterior, generan preocupación sobre la posible habilitación a un conjunto amplio de actividades, que pueden implicar la vigilancia interna de personas a través de medios digitales.

5.1.2 REFORMA DEL ESTATUTO DE LA POLICÍA FEDERAL

Hubo una segunda iniciativa que fue clave para establecer las bases de la vigilancia estatal en Argentina. En junio de 2025, tuvo lugar la reforma del estatuto de la Policía Federal,⁶⁶ la cual creó una nueva división de investigación, el Departamento Federal de Investigaciones (DFI). A partir de esta reforma, la Policía Federal quedó habilitada para monitorear redes sociales y otras fuentes digitales abiertas sin autorización judicial, formalizando el “ciberpatrullaje” como una función oficial.⁶⁷ El decreto, además, establece procesos de

⁵⁹ Ley 25.520 de Inteligencia Nacional. Disponible en <https://servicios.infoleg.gob.ar/infolegInternet/anexos/70000-74999/70496/texact.htm> Consultado en diciembre 2025.

⁶⁰ Decretos 614/2024 y 615/2024. Disponibles en: <https://www.boletinoficial.gob.ar/detalleAviso/primera/310495/20240716> y <https://www.boletinoficial.gob.ar/detalleAviso/primera/310496/20240716> Consultados en diciembre de 2025.

⁶¹ Decreto 941/2025. Disponible en: <https://www.boletinoficial.gob.ar/detalleAviso/primera/337032/20260102> Consultado en diciembre 2025.

⁶² Decreto 941/2025, Artículo 31.

⁶³ Decreto 941/2025, Artículo 9.

⁶⁴ En el Decreto 941/2025, (i) El concepto de “amenaza” persiste en el texto sin una definición clara. Por ejemplo, en los Art. 8, y 9, respectivamente, establece que la Agencia Nacional de Contrainteligencia, así como Agencia Federal de Ciberinteligencia son responsables de producir tareas de inteligencia frente a potenciales “amenazas a la seguridad nacional”; (ii) En el Art 2, el DNU establece que “Todas las actividades que se realizan en el ámbito de la Inteligencia Nacional revisten carácter encubierto [...]”; (iii) El artículo 14 establece la creación de la Comunidad Informativa Nacional (CINF), la cual está integrada por distintos organismos de la Administración Pública Nacional, así como de otras jurisdicciones, las cuales deberán proveer información según criterios que serán establecidos por la Secretaría de Inteligencia del Estado (Art. 17); (iv) El decreto, en reforma del texto de la Ley de Inteligencia Nacional, establece que “en el marco del desarrollo de actividades de inteligencia, auxilio o requerimiento judicial y/o comisión de delitos en flagrancia, el personal de inteligencia podrá proceder a la aprehensión de personas, debiendo dar aviso inmediato a las Fuerzas Policiales y de Seguridad competentes” (Art. 9).

⁶⁵ Decreto 941/2025. Disponible en: <https://www.boletinoficial.gob.ar/detalleAviso/primera/337032/20260102> Consultado en diciembre 2025.

⁶⁶ Decreto 383/2025. Disponible en: <https://www.boletinoficial.gob.ar/detalleAviso/primera/326993/20250617> Consultado en diciembre 2025.

⁶⁷ El nuevo Estatuto, en su Art. 6 sobre las facultades de la Policía Federal Argentina, establece, entre otras, la de “Realizar, sin necesidad de autorización judicial, tareas de prevención del delito en espacios públicos digitales, tales como redes sociales abiertas, sitios web públicos y otras fuentes abiertas, conforme a las pautas y principios rectores dictados para dichas actividades por la autoridad

actualización de la fuerza, a partir de “modernizar protocolos, procesos y mecanismos de articulación, en particular los referentes a investigación” y “adquirir y utilizar en forma efectiva las Tecnologías de la Información y Comunicación y Tecnología Forense” (art. 2.d y 2.e). Esta reforma, al igual que la mayoría de las iniciativas analizadas, fue realizada por decreto, sin debate parlamentario, en el marco de los poderes especiales atribuidos al Poder Ejecutivo por la “Ley de Bases y Puntos de Partida para la Libertad de los Argentinos”, la Ley 27.742, de julio de 2024.

En complemento de esta reforma, en julio de 2025, el Ministerio de Seguridad publicó la Resolución 828/2025,⁶⁸ que establece el Protocolo Particular Para La Actuación De Los Agentes Encubiertos Y Reveladores Digitales, un marco específico para la designación, actuación y protección de funcionarios de las fuerzas federales que intervienen en investigaciones penales mediante identidades ficticias en entornos digitales. El protocolo, publicado en el Anexo 1 de la Resolución 828/2025 del Ministerio de Seguridad Nacional, detalla un procedimiento orientado a crear, resguardar y, eventualmente, suprimir identidades ficticias y “avatares” digitales utilizados en las investigaciones. Una vez designado el agente, se define una biografía ficticia, que se registra bajo un código único y se mantiene bajo custodia reservada (Art.4); si es necesario, se gestionan documentos físicos o digitales a través del Registro Nacional de las Personas, a pedido de la Unidad Especial (Art. 5), entre otras funciones. El protocolo, por otro lado, ordena la creación y registro de identidades digitales ficticias (“avatares”) por parte de las fuerzas y de la estructura de cibercrimen (Art. 11), que quedan a disposición de los agentes encubiertos y reveladores digitales para su empleo procesal. Al mismo tiempo, prevé un sistema de certificación periódica de “agentes altamente calificados”, para desempeñar estas tareas en investigaciones donde se requiera esta técnica especial (Art. 12).

5.2 ELEMENTOS OPERATIVOS PARA IMPLEMENTAR LAS TAREAS DE VIGILANCIA INTERNA

La expansión de las capacidades de vigilancia se materializó en acciones concretas como la creación de nuevas áreas, adquisición de tecnologías y publicación de protocolos específicos. Estos elementos responden a una lógica común: construir capacidad institucional para el monitoreo de la protesta social y el espacio digital. A continuación, se describen en detalle estos elementos.

5.2.1 El “Protocolo Antipiquetes”

Una de las primeras acciones del nuevo gobierno fue la creación del “Protocolo para el mantenimiento del orden público ante el corte de vías de circulación”, promulgado por la Resolución 943/2023 (conocido como “Protocolo Antipiquetes”).⁶⁹ Con la excusa de evitar los cortes de calle durante las protestas, este protocolo funcionó como un instrumento para la intervención de las fuerzas federales ante protestas, sin necesidad de orden judicial previa, al considerar estas situaciones como delitos flagrantes por defecto.⁷⁰

El Protocolo no se limita a regular el control del espacio público, sino que incorpora, de manera explícita, mecanismos de identificación, registro y sistematización de información. En ese sentido, habilita (i) la identificación de lo que el texto llama “autores, cómplices e instigadores”, mediante filmaciones y medios digitales o manuales, con un registro prioritario de datos sobre líderes y organizaciones vinculadas. Este esquema se complementa con la recolección de información sobre los vehículos utilizados para el traslado de manifestantes, los organizadores, formales o informales y, (ii) en el caso de personas extranjeras con residencia provisoria, el envío de sus datos a la autoridad migratoria. Finalmente, (iii) el Protocolo prevé la creación de registros específicos de organizaciones involucradas y del número de infractores identificados, consolidando un enfoque orientado a la producción y sistematización de información más allá de la gestión inmediata del orden público.⁷¹

Publicado sólo cinco días después del comienzo de la gestión de gobierno, el 15 de diciembre de 2023, el Protocolo marcó el rumbo con el que el gobierno ha tratado lo relacionado con el disenso y la protesta social: uso de tecnologías para la vigilancia y despliegue de fuerzas federales para la represión en las calles. Luego de este puntapié inicial, el entramado normativo tomó formas más específicas en ambas dimensiones. Respecto de la vigilancia con el uso de tecnología, el gobierno generó una serie de medidas

competente.” (inciso 11) Anexo del Decreto 383/202, disponible en <https://www.boletinoficial.gob.ar/detalleAviso/primera/326993/20250617>

⁶⁸ Disponible en: <https://www.boletinoficial.gob.ar/detalleAviso/primera/328352/20250715> Consultado en Diciembre 2025.

⁶⁹ Disponible en: <https://www.boletinoficial.gob.ar/detalleAviso/primera/300917/20231215> Consultado en diciembre 2025.

⁷⁰ Desde el 10 de diciembre de 2023 el Ministerio de Seguridad dictó diferentes resoluciones que vulneran derechos. Desde Amnistía Argentina fue generado un registro de esas iniciativas gubernamentales, que sirven de marco para el sistema represivo del gobierno: <https://amnistia.org.ar/disenso-en-riesgo/marco-normativo>

⁷¹ (i) En sus Arts. 6 y 7, lo que se complementa con el Art.8, que establece el envío de la información recopilada al Ministerio de Seguridad; (ii) Establecido en el Art. 11 del Decreto; (iii) Establecido en el Artículo 12 del Decreto.

específicas que serán profundizadas a continuación. Estas medidas sin precedentes serán analizadas en cuanto pueden considerarse un complemento para las medidas de producción y sistematización de información, con foco en el procesamiento de la misma.

5.2.2 LA UNIDAD DE INTELIGENCIA ARTIFICIAL APLICADA A LA SEGURIDAD (UIAAS)

En 2024, el gobierno creó la UIAAS⁷² con el objetivo declarado de prevenir, detectar, investigar y perseguir delitos mediante el uso de tecnologías basadas en inteligencia artificial⁷³. Esta unidad se estructura bajo la órbita de la Dirección de Ciberdelito y Asuntos Cibernéticos (DCAC), y se integra con representantes de las Fuerzas Policiales y de Seguridad Federales.

La DCAC funciona bajo la órbita de la Unidad de Gabinete de Asesores del Ministerio de Seguridad y es uno de los actores más relevantes en este ecosistema. Su responsabilidad primaria radica en el diseño de políticas y programas vinculados a la lucha contra el ciberdelito, así como en la articulación con las Fuerzas Policiales y de Seguridad Federales. Las acciones asignadas a esta Dirección, en el Anexo 2 de la Decisión Administrativa 340/2024⁷⁴ del MINSEG, refuerzan su función de asistencia técnica, planificación y vinculación interinstitucional, sin que se le asignen tareas de ejecución directa en operativos o investigaciones. La DCAC participó en los procesos de compra de algunas de las tecnologías más relevantes adquiridas por el MINSEG durante 2024 y 2025, tales como herramientas de investigación de fuentes abiertas (OSINT) y tecnologías de reconocimiento facial (TRF).

La norma de creación de la UIAAS enumera una serie amplia de funciones⁷⁵, que combinan tecnologías diversas orientadas al patrullaje de redes sociales abiertas, aplicaciones y sitios de Internet, análisis de datos masivos y actividades en línea, uso de reconocimiento facial y análisis de imágenes en tiempo real, vigilancia mediante cámaras, drones y otras tecnologías, utilización de algoritmos de aprendizaje automático para predicción del delito, detección de amenazas cibernéticas, así como procesamiento de información para investigación criminal y coordinación entre fuerzas de seguridad. De esta manera, la UIAAS parece concebirse como un organismo transversal y operativo, sin mención a controles externos ni evaluaciones de impacto en derechos humanos.

Amnistía Internacional realizó dos pedidos de acceso a la información pública al Ministerio de Seguridad Nacional, en mayo y diciembre de 2025, con el objetivo de conocer detalles sobre la reglamentación interna de la UIAAS y su articulación con las fuerzas de seguridad. Sobre el primer punto, el Ministerio no aportó detalles sustantivos más que afirmar que las reglamentaciones se encontraban en proceso, y que el trabajo se estaba realizando de forma articulada con las fuerzas de seguridad, con quienes, además, el Ministerio afirmó que se estaba trabajando de forma coordinada para una evaluación estratégica para “optimizar la dinámica funcional y la arquitectura organizacional de las UIAAS”.⁷⁶ En una respuesta a un segundo pedido de información, el Ministerio de Seguridad Nacional manifestó que la Prefectura Naval, Servicio Penitenciario, Policía de Seguridad Aeroportuaria y Gendarmería Nacional (cuatro de las cinco fuerzas de seguridad nacionales) “no poseen sistemas activos ni antecedentes sobre UIAAS”.⁷⁷ La mera aclaración de qué dependencias no tienen sistemas activos con la UIAAS no disipa las dudas sobre la adecuación con los estándares de derechos humanos del área.⁷⁸

5.2.3 EL PROTOCOLO DE “CIBERPATRULLAJE”

En mayo de 2024, el Ministerio de Seguridad de la Nación publicó el “Protocolo general para la prevención policial del delito con uso de fuentes digitales abiertas”,⁷⁹ conocido popularmente como “Protocolo de

⁷² Creada por la Resolución 710/2024 del Ministerio de Seguridad de la Nación. Disponible en:

<https://www.boletinoficial.gob.ar/detalleAviso/primera/311381/20240729> Consultado en diciembre 2025.

⁷³ Resolución 710/2024 del Ministerio de Seguridad de la Nación, Artículo 3.

⁷⁴ Disponible en: <https://www.boletinoficial.gob.ar/detalleAviso/primera/307616/20240517> Consultado en diciembre 2025.

⁷⁵ Según los incisos establecidos en el artículo 4° de la Resolución 710/2024.

⁷⁶ Ministerio de Seguridad Nacional, Respuesta a pedido de acceso a la información. Nota NO-2025-68968733-APN-SSLE#MSG, del 26 de junio de 2025, página 2 del PDF.

⁷⁷ Ministerio de Seguridad Nacional, Respuesta a pedido de acceso a la información. Nota NO-2026-11569659-APN-DNTEI#MSG, del 2 de febrero de 2026. Página 1 del PDF.

⁷⁸ Por ejemplo, a partir de este pedido conjunto de información realizado por Amnistía Argentina, el CELS, Fundación Vía Libre, ODIA, Access Now, Democracia en Red e ILSED: <https://www.vialibre.org.ar/pedimos-a-bullrich-que-informe-de-que-manera-hara-vigilancia-masiva-a-los-ciudadanos/>

⁷⁹ Resolución 428/2024. Disponible en <https://www.boletinoficial.gob.ar/detalleAviso/primera/308291/20240528> Consultado en Diciembre 2025. Si bien previamente ya se había aprobado un protocolo similar a través de la Resolución 144/2020, este fue derogado dos años

Ciberpatrullaje”, donde formaliza el uso de fuentes abiertas para la investigación por parte de las fuerzas federales. El protocolo establece la competencia para investigar una amplia gama de delitos en el ciberespacio, incluyendo amenazas, acoso, delitos sexuales, trata de personas, lavado de dinero y terrorismo, así como la comercialización de bienes ilícitos. También abarca la búsqueda de personas requeridas por la justicia o desaparecidas. Aunque menciona el respeto a la Constitución y a la Ley de Protección de Datos Personales, incluye una cláusula abierta que permite intervenir ante “cualquier otro delito del que se pueda obtener noticia a través del ciberespacio”⁸⁰, lo que introduce un margen de ambigüedad que podría dar lugar a usos discrecionales más allá de lo expresamente previsto.⁸¹

5.2.4 RECONOCIMIENTO FACIAL *EX POST*: EL PROTOCOLO DE RECONOCIMIENTO Y COMPARACIÓN FACIAL

El Ministerio de Seguridad publicó, en noviembre de 2024, el Protocolo para el Reconocimiento y Comparación Facial.⁸² Este documento, firmado por especialistas de las fuerzas de seguridad federales, establece pautas para el manejo de bases de datos, la formación de personal técnico especializado, así como prerrogativas de índole operativo, como el envío de imágenes para peritar o la aptitud de las imágenes respecto de su umbral mínimo de calidad. Este protocolo establece los procedimientos de trabajo acordados en relación al uso de reconocimiento facial.

Dada la falta de precisiones sobre este punto, y la fallida experiencia del Sistema de Reconocimiento Facial de Prófugos de la Ciudad de Buenos Aires, suspendido judicialmente, Amnistía Internacional realizó un pedido de información con una serie de preguntas al respecto. Si bien el Gobierno se negó a responder sobre la mayoría de los interrogantes realizados, se ocupó de dar una respuesta sobre el uso de TRF por parte de las fuerzas de seguridad. Afirmó que la Policía Federal Argentina (PFA) posee un sistema de reconocimiento facial operado por especialistas bajo autorización judicial, en el marco de investigaciones judiciales activas. Luego, la respuesta hace énfasis en lo siguiente: “no es un sistema online y activo de manera permanente en la vía pública, sino que se trabaja con los elementos probatorios que surgen de una investigación judicial en curso”. Luego, agrega: “Es importante señalar que la utilización del sistema es realizada *ex post*. [...] En tal sentido, el análisis realizado por el software es solo un indicador y/o elemento que el perito analizará emitiendo una opinión técnica”.⁸³

De esta manera, el Gobierno Nacional reconoce el uso de TRF, pero no con un sistema de escaneo continuo, sino, según sus declaraciones, de forma “*ex-post*” a requerimiento de la autoridad competente, amparándose en el uso del mencionado Protocolo de Reconocimiento y Comparación Facial. La tecnología automatizada, según la respuesta ministerial, sirve de apoyo al trabajo de los peritos y no como determinante para la detención de personas. Sin embargo, Amnistía Internacional ha documentado previamente cómo los sistemas de reconocimiento facial retrospectivo 1:n son sujetos a los mismos riesgos e incompatibilidades para los derechos humanos que los sistemas de reconocimiento facial en tiempo real, por lo que deben ser tratados con las mismas preocupaciones.⁸⁴ Asimismo, utilizar el software propietario de una empresa privada puede generar problemas a la hora de intentar auditar el sistema y el funcionamiento de los algoritmos, como pasó en el caso del judicializado y suspendido.⁸⁵

después por la Resolución 720/2022 con fundamento en que su dictado había obedecido al contexto particular de la pandemia de COVID-19.

⁸⁰ Resolución 428/2024, Artículos 2 y 3.

⁸¹ En el pasado, en Argentina, otras gestiones de gobierno, de distintas ramas políticas, también generaron protocolos para la utilización de fuentes abiertas justificadas en tareas de prevención del delito. El primero fue publicado en 2018, durante la presidencia de Mauricio Macri, a través del Ministerio de Seguridad (con Patricia Bullrich como ministra). Dos años más tarde, en 2020, estos lineamientos fueron derogados y reemplazados por una nueva versión, a partir de la Resolución 144/20 del mismo Ministerio. Esta vez, en un nuevo Gobierno, bajo otro partido político, opositor al gobierno anterior: el gobierno de Alberto Fernández. Esta resolución fue derogada en 2022 por la misma gestión, el gobierno argentino estuvo sin un protocolo de vigilancia por fuentes abiertas hasta fines de mayo pasado.

⁸² Resolución 1234/2024, disponible en <https://www.boletinoficial.gob.ar/detalleAviso/primera/317094/20241119> Consultado en diciembre de 2025.

⁸³ Ministerio de Seguridad Nacional, Respuesta a pedido de acceso a la información. Nota NO-2025-68968733-APN-SSLE#MSG, del 26 de junio de 2025, página 4 del PDF.

⁸⁴ Ver Amnistía Internacional: “EU proposals too weak to protect us from dangerous AI systems”:

<https://www.amnesty.org/en/latest/news/2021/04/eu-legislation-to-ban-dangerous-ai-may-not-stop-law-enforcement-abuse-2/>

⁸⁵ Para más información sobre la problemática para auditar el sistema del SRFP, este comunicado de la organización Vía Libre:

<https://www.vialibre.org.ar/comunicado-de-prensa-el-reconocimiento-facial-sigue-suspendido-en-buenos-aires/>

6. ANÁLISIS DE COMPRAS Y CONTRATACIONES DE TECNOLOGÍAS DE VIGILANCIA

En un paso más hacia la implementación efectiva de las tareas de vigilancia con el uso de tecnología, el Gobierno generó órdenes de compras y contrataciones por, al menos, un monto superior a 1.2 millones de dólares, una suma significativa en el marco de políticas de recorte económico.

TABLA 2: COMPRAS Y CONTRATACIONES DE TECNOLOGÍA POR PARTE DEL MINISTERIO DE SEGURIDAD NACIONAL.⁸⁶

ID ⁸⁷	FECHA ADQUISICIÓN	DESCRIPCIÓN DEL PROCESO	PROCESO DE SELECCIÓN	MONTO EN USD
NAC-01	29/10/2025	Adquisición de software para reconocimiento facial Clearview AI.	Contratación Directa	33.500
NAC-02	15/10/2025	Adquisición de licencia de plataforma OSINT Maltego.	Contratación Directa	239.013
NAC-04a	28/08/2024	Adquisición de drones compactos para Seguridad Pública.	Licitación Pública	551.685
NAC-04b	9/09/2024			
NAC-05a	1/12/2025	Adquisición de estaciones terrestres de operación de drones.	Licitación Pública	391.325
NAC-05b	23/12/2025			
NAC-06	13/11/2024	Servicio de información de antecedentes crediticios Nosis.	Contratación Directa	17,863.79

⁸⁶ La información detallada de cada uno de los procesos de compra junto con links a los portales oficiales de compra está disponible en el Anexo 1 de este informe.

⁸⁷ El campo ID fue creado como referencia metodológica. En el Anexo 1 pueden consultarse los detalles de los procesos de compra, cada uno con su ID correspondiente.

Todo ello se encuadra en un aumento del gasto en materia de seguridad y en una reorientación más amplia de las prioridades presupuestarias del Estado. En un contexto de fuerte ajuste fiscal y recortes en todas las áreas de protección social como salud, seguridad social, educación, vivienda, alimentación, entre otros, durante 2025, los aumentos más significativos en el presupuesto devengado se vieron en el Ministerio de Seguridad (29%) e Inteligencia (6%).⁸⁸

A continuación, se analizarán en detalle los objetos de cada una de esas compras teniendo en cuenta las características técnicas, los proveedores, los tipos de procesos y el marco de las políticas en las que se implementan. Como eje ordenador, se dividirá este análisis según el tipo de tecnología.

6.1 TECNOLOGÍAS ADQUIRIDAS POR EL GOBIERNO NACIONAL

6.1.1 VIGILANCIA DE FUENTES ABIERTAS Y DE REDES SOCIALES

La Dirección de Ciberdelito y Asuntos Cibernéticos (DCAC), bajo la cual funciona la UIAAS, intervino en la contratación de un software para investigación en fuentes abiertas con un amplio abanico de funcionalidades,⁸⁹ principalmente concentradas en la aplicación Maltego (Res. MSG 105/2025). Según el pliego técnico de la contratación (PET), se trata de una plataforma integral de investigación OSINT orientada a fortalecer las capacidades de análisis e investigación de las fuerzas. El software a contratar debía permitir la recolección, integración, cruce y visualización de grandes volúmenes de datos provenientes de más de un centenar de fuentes abiertas, incluidas redes sociales, *deep* y *dark web*, datos personales y de contacto, infraestructura técnica, criptomonedas, brechas de seguridad y ciberamenazas, así como el monitoreo en tiempo real con asistencia de IA, análisis de vínculos complejos, generación de perfiles, documentación y colaboración en casos, auditoría de uso y gestión de evidencias (incluida mensajería). Además, debía contar con conectividad avanzada, mediante conectores preconfigurados, integraciones con sistemas de inteligencia y seguridad, y conectores personalizados según las necesidades de los contratantes.

Este tipo de formulaciones plantea serios riesgos de vigilancia masiva sin orden judicial, y sin notificación ni consentimiento de las personas vigiladas, lo que entra en tensión con el artículo 19 de la Constitución Nacional Argentina y los estándares internacionales sobre privacidad y libertad de expresión, mencionados anteriormente. Al integrar este tipo de prácticas en el accionar policial sin controles independientes ni mecanismos de rendición de cuentas, se habilita un escenario de vigilancia opaca que puede tener efectos inhibidores sobre el discurso público y la participación pública, especialmente en contextos de protesta o disenso político. Por otro lado, estas prácticas pueden llevar a la recopilación masiva de información de formas no alineadas con el principio de proporcionalidad, según lo establecido en el marco jurídico internacional (como mencionado, según el test de las tres partes), a causa del tipo de información que recopila, así como por la posibilidad de vigilancia de personas no sospechosas de haber cometido un delito.

Las tareas de vigilancia en fuentes abiertas pueden verse complementadas con la contratación de otros servicios, que pueden responder al ejercicio de tareas de vigilancia o meramente a cuestiones procedimentales de áreas administrativas o de comunicación de las respectivas jurisdicciones. Por ejemplo, la adquisición del Ministerio del servicio de NOSIS,⁹⁰ una empresa argentina que recopila, procesa y comercializa información crediticia, comercial y patrimonial sobre personas y empresas. Sus servicios se usan principalmente para evaluar riesgo crediticio y verificar antecedentes comerciales, funciones mencionadas en el PET del proceso de compra.

⁸⁸ Ministerio de Economía de la Nación, *Presupuesto Abierto. Sitio del ciudadano*, disponible en: <https://www.presupuestoabierto.gob.ar/sici/>

⁸⁹ Adjudicado por Res. 105/2025 del Ministerio de Seguridad. Disponible en la web del proceso de compra: <https://comprar.gob.ar/PLIEGO/VistaPreviaPliegoCiudadano.aspx?qs=BQoBkoMoEhzoP5YumDII4h/V7IltKylNARzyvwBVeJ9/G8if3InkZcQqA6MdIUlOeGIXtThISv3Daj5fr3fg/eFloYnbKzCfni6kA7RCrZ436YqOP5pi6vhE6tMK9DsB7H1eDnkwGW1WcLgVhKfA9lpsfor6LCL>. Consultado en diciembre de 2025.

⁹⁰ Contratada por Disposición número DI-2024-124849263-APN-SSGA#MSG.

6.2.2 PROCESAMIENTO DE IMÁGENES CON TECNOLOGÍAS DE RECONOCIMIENTO FACIAL

El uso de tecnologías de reconocimiento facial por parte de las fuerzas de seguridad plantea serias preocupaciones en materia de derechos humanos. Estas herramientas implican el tratamiento de datos biométricos sensibles y pueden afectar la privacidad, la protección de datos personales y las garantías del debido proceso, especialmente cuando se implementan sin suficientes mecanismos de control y transparencia. A continuación, se analizan las tecnologías adquiridas en detalle.

El 20 de octubre de 2025, el Ministerio de Seguridad Nacional generó un proceso de compra directa por una “licencia de reconocimiento facial para apoyo en investigaciones en el marco del ForCIC”, con el objetivo de “identificar instantáneamente a una persona con una foto.”⁹¹ El ForCIC es el Programa de Fortalecimiento en Ciberseguridad e Investigación del Ciberdelito, que funciona en el ámbito de la mencionada DCAC, que también intervino en este proceso de compra. La tecnología adquirida es el software Clearview AI y fue adquirida no solo por el Gobierno de la Nación, sino también por el Ministerio Público Fiscal de la Ciudad de Buenos Aires⁹² y el Gobierno de la Ciudad de Buenos Aires, quien contrató el servicio en noviembre de 2025.⁹³

Según describe Clearview en su web,⁹⁴ la empresa desarrolló una plataforma impulsada por tecnología de reconocimiento facial que “incluye la mayor base de datos conocida, con más de 70.000 millones de imágenes faciales procedentes de fuentes web de acceso público, como medios de comunicación, sitios web de fichas policiales, redes sociales públicas y otras fuentes abiertas”. Esta plataforma, continúa la descripción, está orientada al “empoderamiento” de agencias para “obtener información, combatir el crimen y mejorar la seguridad pública al revelar pistas, datos y relaciones, ayudando a los investigadores a resolver delitos tanto simples como complejos”. Sin embargo, las prácticas de Clearview fueron cuestionadas en múltiples países, donde fue multada e incluso prohibida dada la explotación masiva de datos personales de la que dependen sus operaciones.

En Europa, las autoridades de protección de datos de países como Francia, Italia, Países Bajos, Austria y Grecia impusieron multas a la empresa por la violación a distintos artículos de la Ley General de Protección de Datos europea (GDPR).⁹⁵ Por ejemplo, en Francia, la autoridad de protección de datos impuso una multa de 20 millones de euros y ordenó el cese de sus actividades debido al tratamiento ilícito de datos biométricos. En particular, la recolección y el uso de imágenes faciales obtenidas de múltiples sitios web sin una base legal válida, así como la eliminación de los datos personales de personas ubicadas en el país. En los Países Bajos, la autoridad nacional de protección de datos (*Autoriteit Persoonsgegevens*) sancionó a Clearview AI con una multa de 30,5 millones de euros por la recolección y el tratamiento ilícito de datos personales y biométricos con fines de reconocimiento facial, sin una base legal válida. Asimismo, la autoridad ordenó el cese de las infracciones en curso mediante órdenes de cumplimiento bajo apercibimiento de sanciones adicionales.

Pero esta tecnología no es controversial solamente por su tratamiento problemático de datos personales. En octubre de 2025, el Centro de Empresas y Derechos Humanos (CEDH) publicó un artículo donde denuncia el uso de Clearview para identificar y detener estudiantes involucrados en protestas pro-Palestina.⁹⁶

⁹¹ Según información del PET. Adjudicación confirmada por Disposición 75/2025 del Ministerio de Seguridad. Disponible en la web del Proceso de Compra: <https://comprar.gob.ar/PLIEGO/VistaPreviaPliegoCiudadano.aspx?qs=BQoBkoMoEhxMnJfhTnfzgmq2csat2luK//I95vshX6TtCLuptwo9rlzhnoTMKNtPbvoD5me/KOfoOIzVztiKn7APcYOCSPtguP6Cj88WhwziHnXaRQpew==> Consultado en diciembre de 2025.

⁹² vía Contratación Directa aprobada por la Disposición OAF 36/2025 del MPF, en junio de 2025. Disponible en <https://mpfciudad.gob.ar/storage/archivos/29fa8b177881168fc41dcf9979f63f08.pdf> Consultado en diciembre de 2025.

⁹³ vía Orden de Compra 347-0095-OC25. Proceso disponible en: <https://www.buenosairescompras.gob.ar/PLIEGO/VistaPreviaPliegoCiudadano.aspx?qs=BQoBkoMoEhwLUetZJKeBjz2KRumWQOnwu7F2M9pcCyTbVr1XyjUKSxomSCR3RSwou0leCfn1E8FaOnzyd2OZBAlysYLycw6kulYeCX7rRo4M%2fMbE6j6pYzPQwu9EquMSy96BILTrM2civDINs6ozRydT21DcoPNx4uUr6Bhw8IKtZY6OgoOOnZkG7pPAvAT> Consultado en diciembre de 2025.

⁹⁴ Fuente: <https://www.clearview.ai/overview> Consultado en diciembre de 2025. Traducción propia.

⁹⁵ Los casos están disponibles en la web de la *European Data Protection Board*:

-Francia: https://www.edpb.europa.eu/news/national-news/2023/facial-recognition-french-sa-imposes-penalty-payment-clearview-ai_en

-Italia: https://www.edpb.europa.eu/news/national-news/2022/facial-recognition-italian-sa-fines-clearview-ai-eur-20-million_en

-Austria: https://www.edpb.europa.eu/news/national-news/2023/decision-austrian-sa-against-clearview-ai-infringements-articles-5-6-9-27_en

-Países Bajos: https://www.edpb.europa.eu/news/national-news/2024/dutch-supervisory-authority-imposes-fine-clearview-because-illegal-data_en

-Grecia: https://www.edpb.europa.eu/news/national-news/2022/hellenic-dpa-fines-clearview-ai-20-million-euros_en

Consultados en diciembre de 2025.

⁹⁶ Ver: <https://www.business-humanrights.org/es/%C3%BAltimas-noticias/usa-police-used-clearview-ai-facial-recognition-tool-to-arrest-pro-palestinian-students-in-a-protest-despite-its-use-being-forbidden-incl-co-non-response/> Consultado en Diciembre de 2025.

La negativa de Clearview a cumplir con la normativa internacional de protección de datos, así como la falta de transparencia con la que opera, llevó a distintas organizaciones europeas a endurecer sus reclamos.⁹⁷ A las sanciones administrativas y órdenes de cese impuestas por autoridades de protección de datos en Europa, se suman los reclamos sostenidos de organizaciones de la sociedad civil, que han documentado impactos directos sobre derechos humanos y han impulsado litigios estratégicos.⁹⁸ Según un informe publicado en diciembre de 2025 por Privacy International (PI), estas violaciones, de carácter grave, sistemático y transfronterizo, están llevando a algunas jurisdicciones a explorar mecanismos de responsabilidad penal, al considerar que las multas bajo el GDPR resultan insuficientes para disuadir prácticas empresariales basadas en la explotación masiva de datos biométricos.⁹⁹ El informe de PI menciona el comienzo de operaciones en Argentina como uno de los pasos preocupantes de expansión de la empresa que, lejos de responder los cuestionamientos, busca expandir sus operaciones de forma constante.

El presente informe no dispone de evidencia que permita afirmar cómo o en qué marco se utilizan las licencias Clearview para el reconocimiento facial en el marco de las actividades de seguridad nacional en Argentina, dado que el Ministerio de Seguridad Nacional no dio información específica de empresas o proveedores a la hora de informar el uso de tecnologías de reconocimiento facial por parte de la Policía Federal.¹⁰⁰

LAS RESPONSABILIDADES DE CLEARVIEW AI EN MATERIA DE DERECHOS HUMANOS

Las empresas tienen la responsabilidad de respetar todos los derechos humanos en cualquier lugar del mundo en el que operen y en todas sus actividades. Se trata de una norma de conducta ampliamente reconocida que figura en las normas internacionales sobre empresas y derechos humanos, como los Principios Rectores de la ONU sobre las Empresas y los Derechos Humanos (Principios Rectores de la ONU).¹⁰¹ Estas normas dejan claro que la responsabilidad de las empresas de respetar los derechos humanos es independiente de las propias obligaciones de un Estado en materia de derechos humanos, y se trata de una responsabilidad adicional a la de cumplir las leyes y normas nacionales de protección de los derechos humanos.¹⁰²

El Principio Rector 13 de la ONU establece que la responsabilidad de las empresas la responsabilidad de respetar los derechos humanos implica el requisito de «evitar que sus propias actividades provoquen o contribuyan a provocar consecuencias negativas sobre los derechos humanos y hagan frente a esas consecuencias cuando se produzcan; y tratar de prevenir o mitigar las consecuencias negativas sobre los derechos humanos directamente relacionadas con operaciones, productos o servicios prestados por sus relaciones comerciales, incluso cuando no hayan contribuido a generarlos». Para cumplir con su responsabilidad empresarial de respetar los derechos humanos, todas las empresas, incluidas las del sector tecnológico, deben contar con procesos continuos y proactivos de diligencia debida en materia de derechos humanos para identificar, prevenir, mitigar y rendir cuentas de cómo abordan su impacto sobre los derechos humanos.¹⁰³

En el contexto descrito en este informe, esto significa que todas las empresas que suministran tecnología de vigilancia a las autoridades argentinas deben llevar a cabo la diligencia debida en materia de derechos humanos para evaluar si existe algún riesgo de que sus productos o servicios contribuyan

⁹⁷ La organización con base en Viena, Noyb, ha presentado una denuncia penal contra Clearview AI y sus directivos en octubre 2025. Ver: <https://noyb.eu/en/criminal-complaint-against-facial-recognition-company-clearview-ai>. Consultado en Diciembre de 2025.

⁹⁸ Por ejemplo, el realizado por el colectivo Reclaim Your Face, integrado por organizaciones originarias de distintas partes de Europa: <https://reclaimyourface.eu/about-clearviewai-mockery-human-rights-those-fighting-eu-intervene/>

⁹⁹ Ver: <https://www.privacyinternational.org/long-read/5715/clearview-and-long-arm-law> Consultado en Diciembre 2025.

¹⁰⁰ Ministerio de Seguridad Nacional, Respuesta a pedido de acceso a la información. Nota NO-2026-11569659-APN-DNTEI#MSG, del 2 de febrero de 2026, Página 1 del PDF.

¹⁰¹ Esta responsabilidad fue reconocida expresamente por el Consejo de Derechos Humanos el 16 de junio de 2011, al respaldar los Principios rectores de la ONU sobre las Empresas y los Derechos Humanos (Principios rectores de la ONU), y el 25 de mayo de 2011, cuando los 42 Estados que se habían adherido a la Declaración sobre Inversión Internacional y Empresas Multinacionales de la OCDE suscribieron por unanimidad una versión revisada de las Líneas Directrices de la OCDE para Empresas Multinacionales. Véase Consejo de Derechos Humanos, resolución 17/4: Los derechos humanos y las empresas transnacionales y otras empresas, 6 de julio de 2011, doc. ONU A/HRC/RES/17/4; Líneas Directrices de la OCDE para Empresas Multinacionales, 2011, www.oecd.org/corporate/mne

¹⁰² Principios Rectores de la ONU, Principio 11, incluyendo el comentario.

¹⁰³ 104 PNUD, Diligencia debida intensificada en materia de derechos humanos para empresas en contextos afectados por conflictos. Una guía, 16 de junio de 2022, https://www.undp.org/sites/g/files/zskgke326/files/2022-11/UNDP_Heightedened_Human_Rights_Due_Diligence_for_Business_in_Conflict-Affected_Contexts_ES.pdf

a abusos contra los derechos humanos o estén vinculados a ellos y, si identifican un riesgo, tomar medidas para evitar que se produzcan dichos abusos.

No cabe duda de que, antes de celebrar un contrato con Argentina, los empleados de Clearview AI sabían o deberían haber sabido de los riesgos en materia de derechos humanos derivados de sus operaciones comerciales, incluso en Argentina. Esto se basa en la información incluida en este informe y en documentos anteriores de Amnistía sobre el reconocimiento facial en los que se describen las incompatibilidades de la tecnología con el derecho internacional de los derechos humanos, así como en las múltiples impugnaciones legales y de aplicación presentadas contra Clearview AI. Sin embargo, hasta donde sabe Amnistía Internacional, Clearview AI no ha realizado hasta la fecha una evaluación pública, transparente y continua del impacto en los derechos humanos, ni ha demostrado que la empresa haya abordado ningún efecto negativo potencial o real sobre los derechos humanos que sus productos o actividades empresariales puedan causar o contribuir a causar o con los que estén directamente relacionados en Argentina.

Amnistía Internacional escribió a Clearview el 1 de julio de 2026 para exponerle sus motivos de preocupación en materia de derechos humanos en relación con sus productos, pero en el momento de publicar este informe no había recibido respuesta.

6.1.3 DRONES, ROBOTS Y VIGILANCIA AÉREA

El Gobierno Nacional adquirió 69 drones en agosto de 2024, que fueron presentados públicamente por la entonces Ministra de Seguridad, Patricia Bullrich, un año después, en ¹⁰⁴ de 2025. Son equipos de la marca DJI, modelos Matrice 30¹⁰⁵ y Mavic 3T. Ambos modelos de drones cuentan con funcionalidades de inteligencia artificial para el seguimiento automatizado de personas y vehículos, así como con cámara térmica, lo que puede permitir rastrear de forma continua los movimientos de personas sin su conocimiento ni consentimiento, posibilitando la elaboración de patrones de comportamiento y perfiles, lo que puede afectar el derecho a la privacidad, la libertad de circulación y generar efectos inhibidores sobre la participación en el espacio público, según surge del PET en el proceso de contratación (ver anexo 1).

A mediados de diciembre de 2025, el Ministerio complementó la compra de drones con la adquisición de once estaciones terrestres de operación de VANT, en modalidad "Cautivos". Entre ambas compras, el Ministerio de Seguridad Nacional dedicó cerca de un millón de dólares a la adquisición de drones y recursos asociados para su uso y capacitación de personal (ver tabla 2, al inicio de esta sección).

Durante la presentación pública junto con las fuerzas de seguridad, en septiembre de 2025, la entonces Ministra de Seguridad Nacional, Bullrich, en respuesta a la pregunta de un periodista, afirmó que "no tenemos reconocimiento facial en estos drones, y son para investigaciones criminales, que nada tienen que ver con manifestaciones".¹⁰⁶ Sin embargo, hay evidencia del uso de los drones para la vigilancia de protestas, al menos, en dos oportunidades.

La primera, anterior a esta presentación, el 19 de marzo de 2025, a partir de un registro audiovisual realizado por un canal de noticias, en el marco de un operativo de las fuerzas federales durante una protesta en el Congreso Nacional. Las imágenes muestran a personal de las fuerzas de la Policía Federal utilizando uno de los drones adquiridos en 2024.

¹⁰⁴ Prensa Ministerio de Seguridad Nacional (25 de septiembre de 2025) La ministra Patricia Bullrich entregó 69 drones de última generación a las Fuerzas Federales <https://www.argentina.gob.ar/noticias/la-ministra-patricia-bullrich-entrego-69-drones-de-ultima-generacion-las-fuerzas-federales>

¹⁰⁵ Información provista a partir de un pedido de acceso a la información, registrada bajo el Expediente EX-2025-140781452-APN-DNPAIP#AAIP. Ver Anexo 3 para más información.

¹⁰⁶ Video del 25 sept 2025 "Bullrich entrega drones de última tecnología a las fuerzas de seguridad": Link: <https://www.youtube.com/watch?v=vlegUppvw9o> (minuto 10:15).

IMAGEN 1: DESPLIEGUE DE DRONES POR LAS FUERZAS POLICIALES DURANTE UNA PROTESTA EN FRENTE AL CONGRESO NACIONAL EL 19 DE MARZO DE 2025



↑ *Izquierda: personal de la Policía Federal con el equipamiento correspondiente. Derecha: el drone DJI Matrice 30T en vuelo, con el Congreso de fondo. Fuente: Cuenta de Youtube del canal de noticias A24.¹⁰⁷*

La segunda evidencia, que a la vez muestra que se trata de una práctica sistemática, corresponde a un video oficial de la cuenta de la Policía Federal Argentina, publicado el 28 de febrero de 2026. En ese video, titulado “El rol de los drones en los operativos policiales”, oficiales de estas fuerzas muestran los usos de estos dispositivos en el accionar policial. Este video tiene la particularidad de haber sido filmado en el contexto de una manifestación. Uno de los oficiales entrevistados en el video, del área de “video y comunicaciones aeronáuticas” afirma que “el rol nuestro en las manifestaciones es brindar imágenes al comando institucional, [...] ya sea por transmisión 4G, con mochilas de transmisión; o a través de transmisión satelital, mediante antenas *Starlink*”.¹⁰⁸ Luego, otro de los entrevistados afirma: “Contamos con equipos de última generación que [...] nos permiten tener una mayor ventaja en la toma de registros filmicos, con la capacidad de zoom que tienen, para un posterior procesamiento de imágenes, el reconocimiento facial, y así identificar a las personas”.¹⁰⁹ En los minutos 0:08 y 2:28, el video muestra imágenes de transeúntes con las caras difuminadas, aparentemente a modo ilustrativo de las capacidades de este equipamiento.

Estos testimonios dan cuenta de tres preocupaciones respecto del uso de drones. Primero, la respuesta de la entonces ministra no se corresponde con la evidencia de usos de los drones adquiridos en el contexto de manifestaciones tanto antes como después de su presentación oficial. Segundo, el hecho de que estos drones no tienen capacidades de reconocimiento facial, pero las imágenes son enviadas por transmisión 4G o satelital a las áreas que así lo requieran. Estas áreas pueden tener capacidad de reconocimiento facial para la identificación de personas, según lo manifestado por el oficial, así como el conocimiento que surge de los pedidos de información realizados, como fue expresado arriba. Por último, hay poca o nula transparencia acerca de cómo son procesadas las imágenes que se transmiten en tiempo real, cómo se archivan y ordenan. Desde Amnistía Internacional fueron realizadas preguntas específicas al respecto, pero la respuesta fue negada bajo el argumento del resguardo de la seguridad nacional.¹¹⁰

6.1.4 ALGORITMOS PREDICTIVOS: HERRAMIENTAS DE REFUERZO DE ESTEREOTIPOS

El uso de algoritmos predictivos y sistemas de perfilamiento automatizado en materia de seguridad pública plantea serias preocupaciones desde una perspectiva de derechos humanos. Estas herramientas, lejos de ser neutrales, pueden amplificar sesgos estructurales presentes en los datos que utilizan, derivando en

¹⁰⁷ Video del 19 de marzo de 2025 “CONGRESO BLINDADO: INHIBIDORES DE SEÑAL Y DRONES CON LA SEGURIDAD DEL G20”. Link: <https://www.youtube.com/watch?v=nNR1AgSg2tE> (minuto 6:33)

¹⁰⁸ Video del 28 de febrero de 2026 “PREVENIR | ROL DE LOS DRONES EN LOS OPERATIVOS POLICIALES” cuenta PFAoficial (Policía Federal Argentina). Link: <https://www.youtube.com/watch?v=pRmQ3XxgleA> (Minuto 0:53)

¹⁰⁹ Video citado, minuto 2:22.

¹¹⁰ Pregunta: Pedido de acceso a la información enviado el 8 de mayo de 2025. Pregunta 2.G. Página 4 del PDF. Respuesta: Ministerio de Seguridad Nacional, Respuesta a pedido de acceso a la información. Nota NO-2025-68968733-APN-SSLE#MSG, del 26 de junio de 2025, página 2 del PDF.

prácticas discriminatorias, afectaciones a la privacidad, erosión de la presunción de inocencia y restricciones indirectas a libertades. Si bien no hay información detallada sobre compras de estas tecnologías, las funciones de la UIAAS incluyen un punto específico al respecto.¹¹¹

El Programa de Policiamiento de Puntos Calientes, implementado por el Ministerio de Seguridad de la Nación con apoyo del Banco Interamericano de Desarrollo, en 2017¹¹² es un programa que merece mención en este apartado. Aunque no hacía uso explícito de inteligencia artificial, el programa ya aplicaba una lógica de focalización territorial basada en datos históricos de criminalidad para asignar recursos policiales. Este tipo de estrategias, que identifican zonas con alta concentración delictiva y priorizan su vigilancia, pueden contribuir a reforzar sesgos espaciales preexistentes, al tiempo que normalizan la presencia policial constante en barrios históricamente estigmatizados.

Este tipo de impactos debe ser considerado seriamente al proyectar herramientas similares bajo la órbita de la UIAAS, especialmente si no se definen estándares técnicos, criterios de exclusión o mecanismos de rendición de cuentas públicos.

6.2 TECNOLOGÍAS DE VIGILANCIA ADQUIRIDAS POR LA CIUDAD DE BUENOS AIRES: AUMENTO DE COBERTURA DE VIDEOVIGILANCIA Y NUEVAS TECNOLOGÍAS DE RECONOCIMIENTO FACIAL

La expansión de la infraestructura de la Ciudad de Buenos Aires para la vigilancia, en particular la que se da en las cercanías del Congreso Nacional, ha sido particularmente preocupante, dado que ese es uno de los epicentros de la movilización social en Argentina. En este sentido, resulta relevante observar cómo las infraestructuras de ambas jurisdicciones se complementan y refuerzan entre sí: el gobierno nacional contrató tecnología orientada al abordaje de delitos federales a escala nacional, mientras que el GCABA adquirió herramientas que habilitan una mayor cobertura espacial en tareas de vigilancia dentro de la Ciudad. En conjunto, ambas capas tecnológicas configuran un entramado más denso y extendido de vigilancia en la Ciudad Autónoma de Buenos Aires.

TABLA 3: CONTRATACIÓN DE INFRAESTRUCTURA PARA LA VIGILANCIA POR EL GOBIERNO DE LA CABA.

ID	AÑO ADQUISICIÓN	DESCRIPCIÓN DEL PROCESO	PROCESO DE SELECCIÓN	MONTO EN USD
CABA-01	23/12/2025	Contratación de servicios de análisis de imágenes de video y gestión de alertas.	Licitación pública	4.997.281
CABA-02	06/11/2025	Adquisición de software de reconocimiento facial (Clearview) entre otros productos.	Licitación pública	828.916
CABA-03	17/10/2025	Servicio de mantenimiento eléctrico y energización de puntos de captura de video	Licitación pública	810.956
CABA-04	02/10/2025	Servicio de información de antecedentes crediticios Nosis.	Licitación pública	93.804

¹¹¹ Artículo 4° de la Resolución 710/2024 inc d: “Utilizar algoritmos de aprendizaje automático a fin de analizar datos históricos de crímenes y de ese modo predecir futuros delitos y ayudar a prevenirlos.”

¹¹² El financiamiento que dio origen a esta política parece estar aún vigente, a partir del Programa Federal de Seguridad, financiado por el BID con USD 25 millones, donde la eficientización de los sistemas de datos de política criminal tenían un rol de suma importancia. Ver <https://www.iadb.org/es/proyecto/AR-L1255>

ID	AÑO ADQUISICIÓN	DESCRIPCIÓN DEL PROCESO	PROCESO DE SELECCIÓN	MONTO EN USD
CABA-05	23/06/2025	Servicio de conectividad para los dispositivos pertenecientes a la plataforma de seguridad por video.	Licitación pública	14.184.463
CABA-06	8/5/2025	Adquisición de puntos de captura y el hardware y software para su procesamiento y almacenamiento.	Licitación pública	27.077.219

Fuente: en base a procesos de compras y contrataciones publicadas en la plataforma Buenos Aires Compras (BAC).

La Tabla 3¹¹³ muestra la adquisición de tecnologías que no necesariamente refieren a vigilancia en los términos descritos en el apartado metodológico de esta investigación, sino la infraestructura habilitante para la adquisición y procesamiento de imágenes, así como su mantenimiento. Los montos son muy superiores a los de la Nación, aunque responden a tecnologías distintas. Solo en las contrataciones seleccionadas, la Ciudad gastó cerca de 48 millones de dólares.

La expansión del sistema de videovigilancia representa más de la mitad de ese monto, como puede verse en el cuadro, en el ítem “Adquisición de puntos de captura y el hardware y software para su procesamiento y almacenamiento”. Según informa el Gobierno, el sistema de videovigilancia alcanzó el “82% de cobertura” de la ciudad en julio de 2025.¹¹⁴ El Gobierno adquirió, en 2025, 850 puntos de captura, por un total de 3400 cámaras.¹¹⁵ Si bien la información es fragmentaria, hay para considerar que la misma empresa no sólo provee el software de reconocimiento facial,¹¹⁶ sino también el resto de los puntos de captura que fueron instalados en la Ciudad de Buenos Aires entre 2018 y la actualidad.¹¹⁷

El GCABA no publicó información oficial sobre las características de las cámaras instaladas entre 2019 y 2023,¹¹⁸ la cual es de utilidad para comprender de forma oficial las capacidades de estos dispositivos para el registro de personas, por ejemplo, en el marco de protestas en el espacio público. Sin embargo, a partir de 2024, el Pliego de Especificaciones Técnicas (PET) del Proceso de Compra 3202-0540-LPU24, provee detalles sobre las características técnicas de las cámaras tipo *Bullet* (fijas) y PTZ (domos).

TABLA 4: REQUERIMIENTOS PARA LAS CÁMARAS DE VIDEOVIGILANCIA DEL GOBIERNO DE LA CIUDAD DE BUENOS AIRES 2024-2025, SEGÚN REQUERIMIENTOS TÉCNICOS DEL PROCESO DE COMPRA 3202-0540-LPU24

ASPECTO	CÁMARA FIJA	DOMO PTZ
FUNCIÓN PRINCIPAL	Captura continua sobre un punto fijo	Vigilancia dinámica con seguimiento y exploración del entorno

¹¹³ Este informe analiza las reformas normativas y adquisiciones de tecnología por parte del Gobierno Nacional de la Argentina y la Ciudad de Buenos Aires. No busca proveer un análisis integral del cumplimiento de los derechos humanos por parte de los actores corporativos involucrados. En este sentido, no se realizan alegaciones en contra de ninguna empresa involucrada en el desarrollo o la provisión local de las tecnologías analizadas, incluidas las empresas nombradas en las fuentes de información analizadas en el presente informe.

¹¹⁴ GCABA (2025) “Jorge Macri supervisó la instalación de 1.200 cámaras para ampliar la vigilancia urbana” https://buenosaires.gob.ar/gcaba_historico/noticias/jorge-macri-superviso-la-instalacion-de-1200-camaras-para-ampliar-la Consultado en marzo 2026.

¹¹⁵ El proceso de adquisición de los puntos de captura de video para el plan integral de videovigilancia se inició con la Orden de Compra original aprobada por la Resolución 984/MSEGC/24 del 11 de octubre de 2024, que contemplaba la compra e instalación de 150 unidades por un monto de USD 2.341.800. Posteriormente, mediante la Resolución 1186/MSEGC/24 del 11 de diciembre de 2024, se aprobó un primer incremento que amplió significativamente el alcance en 400 unidades adicionales por USD 6.244.800. Finalmente, la Resolución 511/MSEGC/25 del 8 de mayo de 2025 incorporó un tercer incremento de 300 unidades por USD 4.683.600. De esta manera, el proceso completo consolidó la adquisición de un total de 850 puntos de captura, combinando la compra original con sus ampliaciones sucesivas.

¹¹⁶ El proceso de contratación 2900-0472-CDI19, iniciado en 2019 y prorrogado en 2020 y 2021, hace referencia en su pliego técnico a la “Contratación de un servicio de análisis integral de video”, pero en la descripción del proceso en BA Compras hace referencia a “Servicio de Instalación De Camara De Video Para Sistema De Vigilancia Vial. El Servicio Incluye, Ferretería Para Montaje, Insumos Menores Y Mano De Obra Para Su Correcto Funcionamiento”. El período 2019-2025 fue el de mayor aumento del Sistema de Videovigilancia de la Ciudad.

¹¹⁷ En octubre de 2018, a partir de un conflicto por la instalación de cámaras de videovigilancia frente a la vivienda de la expresidenta Cristina Kirchner, el proveedor publicó un comunicado donde manifestó haber instalado “cerca de 8 mil” equipos en la vía pública, aclarando que la empresa no decidía la ubicación de los equipos que instala, sino sus clientes. El comunicado fue publicado por un medio de prensa: <https://www.infobae.com/politica/2018/11/16/la-empresa-que-acuso-cristina-kirchner-aclaro-por-que-instalaba-camaras-frente-al-edificio-de-recoleta/>

¹¹⁸ El gobierno no proveyó hasta el momento información específica sobre la marca y modelo de los dispositivos instalados.

ASPECTO	CÁMARA FIJA	DOMO PTZ
RESOLUCIÓN Y SENSOR	Sensor CCD/CMOS, 4K (3840x2160)	Sensor CCD/CMOS 12 MP, 4K (3840x2160)
LENTE / ZOOM	Zoom motorizado 4–12 mm	Zoom óptico $\geq 20x$ + zoom digital $\geq 12x$
MOVIMIENTO	Sin movimiento mecánico	Paneo 360° continuo y tilt 0°–90°, alta velocidad
CAPACIDAD DÍA / NOCHE	Conmutación automática a monocromático + IR ≥ 50 m	Captura día/noche en color + modo monocromático
CONTROL Y GESTIÓN REMOTA	Gestión IP, múltiples flujos, ONVIF, ajustes remotos	Gestión IP, múltiples flujos, ONVIF, presets y tours

Fuente: elaboración propia en base a PET Proceso de Compra 3202-0540-LPU24.

Si bien las cámaras domo y los puntos de captura representan el mayor grado de cobertura en la Ciudad, los gobiernos nacional y local también incorporaron tecnología portátil o móvil a sus recursos. Ambas jurisdicciones adquirieron drones para reforzar las capacidades de vigilancia. En 2022, el GCABA adquirió un total de cuatro drones, dos “para operaciones complejas y observación desde largas distancias con cámara térmica” y dos para tareas de instrucción de pilotos.¹¹⁹ Estos recursos son utilizados por el Escuadrón de Drones de la Policía de la Ciudad. Según la jefa del Departamento de Aviación Policial, el dron más moderno del que dispone el escuadrón es el DJI Matrice 200, que “cuenta con un sistema de autotrack que permite *marcar* al auto o la persona que estamos persiguiendo, teniendo datos sobre su recorrido”.¹²⁰

6.2.1 ¿CÓMO SE TRADUCE ESTO EN UN ESCENARIO REAL DE PROTESTA EN LA CIUDAD DE BUENOS AIRES?

Para analizar las implicancias para los derechos humanos del uso de cámaras de videovigilancia con las características mencionadas, cabe utilizar un caso específico que sirva de ejemplo. En este caso, el análisis de las cámaras instaladas en las cercanías del Congreso Nacional y la Avenida 9 de Julio, en la Ciudad de Buenos Aires. Estos dos espacios han sido el espacio de muchas de las protestas más masivas que se dieron en el período analizado.

¹¹⁹ A partir del proceso 2900-1001-LPU22, adquiridos por RESOL-2022-319-GCABA-SSGA del 14 de octubre de 2022.

¹²⁰ Prensa GCABA, 30 de Enero de 2023 “Así funciona el escuadrón de drones de la Ciudad que ayuda a apagar incendios, perseguir a ladrones y encontrar personas perdidas” Link: https://buenosaires.gob.ar/gcaba_historico/noticias/asi-funciona-el-escuadron-de-drones-de-la-ciudad-que-ayuda-apagar-incendios-perseguir

IMAGE 2



Protesta sobre la plaza del Congreso (arriba) y sobre la Av. 9 de Julio (abajo).

Fuente: TOMAS CUESTA/AFP via Getty Images y ELENA BOFFETTA / AFP via Getty Images respectivamente



En este sentido, desde Amnistía Internacional, junto con organizaciones locales defensoras de derechos humanos, fue realizado un hackathon, en octubre de 2025. El evento tuvo el objetivo de mapear colaborativamente la cobertura de las cámaras de vigilancia ubicadas en las cercanías del Congreso Nacional y la Avenida 9 de Julio, y así conocer su alcance, como una referencia para un potencial uso de tecnologías de reconocimiento facial.¹²¹

El lugar fue seleccionado por ser un espacio frecuentado por la sociedad civil, en particular durante las protestas, y se utilizó como punto de referencia para determinar el alcance y el grado de exposición a una posible vigilancia masiva. Como Amnistía Internacional ha documentado anteriormente, el mapeo de la ubicación de las cámaras de videovigilancia (CCTV) permite estimar el alcance potencial de la exposición al reconocimiento facial, ya que esta tecnología suele utilizarse en combinación con dichas cámaras. Este

¹²¹ Amnistía Internacional consultó en un pedido de acceso a la información enviado al Gobierno de la Ciudad de Buenos Aires el 4 de febrero de 2026 acerca del contexto de la implementación de Clearview AI, cuya adquisición fue documentada bajo la orden de compra 3202-0419-OCA25 del 11 de noviembre de 2025. En su respuesta, con fecha del 17 de marzo de 2026, el GCABA aseguró que "Clearview, herramienta tecnológica vinculada al reconocimiento facial, no se encuentra actualmente en uso por parte del Gobierno de la Ciudad Autónoma de Buenos Aires ni por la Policía de la Ciudad, en virtud de las disposiciones judiciales vigentes que ordenaron la suspensión de la utilización de sistemas de reconocimiento facial."

método no distingue si la exposición al reconocimiento facial se produce en tiempo real o mediante el procesamiento posterior de las imágenes por parte del GCABA o el gobierno nacional en esa zona.

Para ello, las personas participantes recorren las calles dentro de un radio de ocho cuadras alrededor del Congreso Nacional en busca de cámaras instaladas en edificios u otros elementos de infraestructura pública (por ejemplo, postes de alumbrado, semáforos, etc.), elaborando un listado con las coordenadas de las cámaras identificadas. Posteriormente, dicho listado es revisado por otras personas participantes y, a partir de las coordenadas recopiladas, se elabora un mapa.

Los resultados de este evento permitieron generar un mapa de referencia de cobertura, así como un espacio de debate e intercambio entre las organizaciones participantes.

IMAGEN 3: MAPA DE LAS CÁMARAS UBICADAS EN LAS PROXIMIDADES AL CONGRESO DE LA NACIÓN



 Fuente: Amnistía Internacional basada en trabajo colaborativo

La imagen muestra una referencia de la cobertura de las cámaras domo, aunque suelen estar en puntos de captura, junto con cámaras fijas. Los círculos no representan la ubicación específica de cada cámara. Se marcaron los lugares de interés para referencia, en negro. Para las cámaras domo, se estableció un rango de alcance de 35 metros, solo a modo ilustrativo, dado que las funcionalidades expuestas permitirían alcances mayores. Para el análisis fue delimitado un perímetro que va desde 4 cuadras hacia el norte y 4 cuadras hacia el sur y 4 hacia el oeste del edificio del Congreso. Hacia el este, la cobertura fue mayor, dado que alcanza la Avenida 9 de Julio, una de las potenciales vías de salida para las personas manifestantes.

Las protestas suelen darse alrededor de la plaza del Congreso (“Plaza del Congreso” en el mapa) que, en la imagen, se ve total y desproporcionadamente cubierta por el alcance de las cámaras. También se ve una cobertura de cámaras por distintos puntos de las calles adyacentes, que también son vías de salida potenciales para las personas manifestantes, así como a lo largo de la mencionada Avenida 9 de Julio. Esta avenida, además, es uno de las principales locaciones de protesta para las organizaciones sociales, por ejemplo, de la economía popular.

En resumen, las políticas y adquisición de tecnologías por parte de ambas jurisdicciones son complementarias. Mientras que el nivel nacional genera el ecosistema para la vigilancia estatal a partir del trabajo de las fuerzas federales y de los sistemas de inteligencia, el Gobierno de la Ciudad desarrolló un nivel

de cobertura de videovigilancia con alcance para una gran porción del territorio de la Ciudad de Buenos Aires.

Como fue mencionado en el apartado anterior, organismos del sistema universal y regional de los Derechos Humanos alertaron sobre el efecto inhibitor que estas tecnologías y acciones de gobierno pueden tener sobre la población.

7. EL EFECTO INHIBIDOR: CUANDO LA PERCEPCIÓN DE LAS TECNOLOGÍAS DE VIGILANCIA AFECTA LOS DERECHOS DE LAS PERSONAS

Esta sección analiza la vigilancia estatal y los efectos inhibitorios o disuasorios (*chilling effect*) en las personas, con foco particular en cómo la vigilancia impacta sus derechos para la participación política, la libertad de expresión y la libertad de reunión en contextos urbanos, a partir de una serie de entrevistas.¹²² Para ello, a continuación, se examinan diferentes formas de autocensura y otros cambios de comportamiento relacionados con la vigilancia. También cómo la vigilancia, ya sea real o percibida, afecta a la confianza dentro de los grupos y entre las organizaciones, y cómo esto influye en su disposición a comprometerse con personas o movimientos que se consideran bajo vigilancia. Además, estudia cómo la vigilancia reduce la capacidad de los grupos para organizarse, movilizarse y emprender acciones colectivas.¹²³

Los comentarios que se presentan a continuación surgen de 21 personas consultadas, a través de entrevistas individuales y grupales orientadas a relevar impactos diferenciados y percepciones sobre el uso de tecnologías de vigilancia. Las personas entrevistadas fueron seleccionadas para reflejar distintos perfiles y niveles de exposición. Por un lado, se incluyeron estudiantes y jóvenes, personas jubiladas, defensores de derechos humanos y una autoridad estatal. Por otro, se abordó a uno de los sectores más afectados por las

¹²² Amnistía Internacional analizó los efectos inhibitorios de las tecnologías de vigilancia en múltiples oportunidades, enfatizando que su existencia refleja un incumplimiento por parte de los estados y actores privados de sus obligaciones en materia de derechos humanos. Cuando no existen garantías como transparencia, control de abusos o acceso a reparación, la percepción de vigilancia genera una desconfianza generalizada y puede restringir directamente la libertad de expresión y el derecho a la vida privada. Este argumento, por ejemplo, fue presentado por Amnistía Internacional ante el Relator Especial sobre libertad de reunión y asociación del Consejo de Derechos Humanos de las Naciones Unidas, en una contribución de 2025 sobre vigilancia digital y efectos inhibitorios. Disponible en: <https://www.amnesty.org/en/documents/ior40/0484/2025/en/>

¹²³ El apartado metodológico, al principio de este informe, tiene una descripción detallada de las entrevistas realizadas, los criterios de selección y demás detalles de la metodología implementada.

políticas de seguridad: el de las y los trabajadores de prensa. Dada la política de consentimiento informado de Amnistía Internacional, algunas de las opiniones fueron anonimizadas.

7.1 EFECTO INHIBIDOR Y AJUSTES DEL COMPORTAMIENTO COMO RESULTADO DE LA VIGILANCIA

Entre las personas entrevistadas para esta sección hay un factor común: la totalidad de ellas expresa que, de alguna u otra manera, fueron o son vigiladas o, al menos, las autoridades saben quiénes son.

“Estamos totalmente identificados todos desde hace mucho tiempo ya. [...] A veces vas caminando y de repente llegando te encontrás que tenés el dron ahí arriba cerquita de la cabeza. A veces a dos metros. ¿Por qué tan cerca? ¿Por qué es tan invasivo?”, se pregunta Ana Tapia, integrante del colectivo Jubilados Insurgentes. Las personas jubiladas marchan todos los miércoles frente al Congreso Nacional para protestar en contra de los recortes jubilatorios realizados por el Gobierno Nacional.

Por otro lado, Matías Darabós, de la Asociación Contra la Violencia Institucional (ACVI) que, entre otras cosas, busca registrar abusos policiales durante las marchas, afirma: “Hay una sensación muy fuerte de que te están controlando y que te están vigilando. Por el caso, nosotros, cuando vamos a las marchas y monitoreamos, es constante que te señalan o te filman.”

Bianca Abella, fotógrafa independiente, afirmó que la vigilancia por parte de la policía afecta su trabajo:

“tenemos a la policía a centímetros con las cámaras vigilando constantemente. Los drones también. Y es como te da un temor y una desconfianza. Te da desconfianza en tu propio trabajo un montón de veces y te interrumpe la manera de laburar en la calle. Estaba bastante complicado, por lo menos para nosotros. Bastante difícil.”

Como fue mencionado previamente en este reporte, las fuerzas federales cuentan en la actualidad con una gama variada de elementos de registro audiovisual. En respuesta a un pedido de acceso a la información realizado por Amnistía Internacional, fuentes gubernamentales confirmaron el uso de cámaras de grabación profesionales, distintos tipos de cámaras corporales y los mencionados drones.¹²⁴

Las entrevistas mostraron la percepción de un aumento específico en la vigilancia de periodistas, uno de los sectores más afectados por la represión.¹²⁵ En las entrevistas, esta situación fue particularmente analizada por parte de distintos representantes gremiales de los trabajadores de prensa. Paula Cejas, la directora de la Oficina para Latinoamérica de la Federación Internacional de Periodistas (FIP), afirmó:

“Percibimos un incremento de mecanismos de vigilancia enfocados en periodistas. No podemos dar por hecho que sea así, pero sí hay una intencionalidad de ataque hacia medios independientes y opositores. Además, existen mecanismos como la unidad de Ciberpatrullaje que hacen que uno esté más alerta”.

Cejas, además de la directora regional de la Federación, reside en Buenos Aires, por lo que su perspectiva es pertinente desde su conocimiento de lo regional, así como del escenario local.

Por otra parte, el director del Sindicato de Prensa de Buenos Aires (SiPreBA), Agustín Lecchi, afirmó:

“Tuvimos una etapa de mucha vigilancia durante el gobierno de Macri.¹²⁶ Hicieron una carátula básica a partir de un seguimiento en redes sociales del perfil político ideológico de cada uno que se acreditaba al G20.¹²⁷ Ahora tenemos una situación similar: les miran las redes sociales [a los periodistas] y en función de eso tienen

¹²⁴ Registro bajo el Expediente EX-2025-140781452-APN-DNPAIP#AAIP.

¹²⁵ Para más información sobre los resultados de la represión de la protesta social y los ataques a la prensa, consultar este balance de Amnistía Argentina, a dos años del inicio del gobierno de Javier Milei: <https://amnistia.org.ar/noticias/dos-anos-del-protocolo-antipiquetes-mas-de-2-500-personas-heridas-y-una-escalada-de-represion-a-la-protesta>

¹²⁶ Su período de gestión tuvo lugar desde el 10 de diciembre de 2015 hasta el 9 de diciembre de 2019.

¹²⁷ El evento al que hace referencia Cecchi es la Cumbre del G20 y la conferencia de la OMC, eventos internacionales que tuvieron lugar en Buenos Aires en 2018 y 2017 respectivamente, durante la gestión de gobierno federal de Mauricio Macri. En 2020, con el cambio de gestión de gobierno, la agencia de inteligencia fue intervenida y en ese marco fue denunciada la creación de perfiles detallados sobre periodistas, defensores de derechos humanos, organizaciones de la sociedad civil, entre otros, en el marco de la gestión de la autorización para acceder a la cumbre y para la habilitación de personas para ingresar al país: “Los dos eventos le sirvieron a la Agencia Federal de Inteligencia (AFI) para la realización de un espionaje masivo sobre periodistas, académicos y empresarios que se inscribieron para participar, pero también para infiltrarse entre los partidos de izquierda, que preparaban las manifestaciones de repudio.”, según describe la Fundación Vía Libre en una nota escrita en el marco de la publicidad de estos hechos (Fundación Vía Libre, 2020).

distintos niveles de persecución sindical o laboral. Y después, en las movilizaciones y protestas callejeras, hay un ensañamiento y una represión particular contra la prensa”.

Por otro lado, en el mismo sentido, una periodista, especializada en temas de derechos de las mujeres y las diversidades, que llamaremos Participante 6, afirma:

“Me doy por vigiladx, no sé cómo explicarlo, es como que ya me doy por perfiladx, al menos públicamente, porque tuve o tengo eventualmente exposición o cierta exposición o lo que sea. Doy por sentado que alguien me está vigilando, sea grupos opositores a los temas que yo trabajo, sea el gobierno, sea la fuerza de seguridad, sea el aparato de comunicación del gobierno, quien sea”.

Este sentimiento no sólo surgió entre personas que trabajan con temáticas de derechos humanos, sino también entre personas que cubrieron los eventos de campaña del partido de Gobierno: “A mí, personalmente, siento que me tienen *fichado*¹²⁸ desde ya, porque estoy desde el primer acto de Javier Milei como político en 2020”. Emilio Laszlo, coordinador general del medio de *streaming* Gelatina, hace referencia con esa frase a su cobertura periodística de la campaña presidencial del actual presidente. Sigue:

“Estaba ahí cuando eran 50, 100 personas, hasta que asumí en la Casa Rosada. Entonces, no tengo duda. Con algunos de ellos tengo buen diálogo, con otros no tengo diálogo, pero seguro que hay alguna carpeta mía y de todos los que vamos a esos lugares, con nuestros nombres, nuestras caras y dónde *laburamos*”.

Ahora bien, ¿qué haría el Gobierno con esta información? Las personas entrevistadas generaron conjeturas al respecto. Una de ellas, corresponsal internacional, a quien llamaremos “Participante 4”, expresó preocupación por el tratamiento automatizado de datos. Señaló que, aunque no se considera un objetivo individual de vigilancia, el riesgo aumenta significativamente con la automatización de estas tecnologías. Advirtió que, con pocos pasos, podrían construirse bases de datos de periodistas y monitorear su actividad en tiempo real, lo que vuelve más delicada la situación al reducir las posibilidades de anonimato. En ese contexto, también expresó preocupación por el clima político, señalando que ciertos discursos hostiles hacia el periodismo podrían habilitar el uso de estas herramientas contra este sector.

En el mismo sentido, Participante 6 señaló que, aunque no cuenta con evidencia directa de vigilancia, considera que hoy existe un seguimiento de ciertos perfiles y contenidos, facilitado por herramientas tecnológicas y de inteligencia artificial. También mencionó que redujo su exposición pública, lo que incide en su percepción sobre el monitoreo actual, aunque sostuvo: “sí creo que hay [...] empresas que se dedican a eso y hay alertas”, orientadas a rastrear lo que determinadas personas, como periodistas, publican o comparten. Sin embargo, aclaró que no ha tenido experiencias concretas recientes.

Por último, desde el grupo de jóvenes manifestaron preocupación sobre la atención que prestan a las redes sociales funcionarios del Gobierno. En este sentido, un participante menciona el caso Ian Moche, un episodio en el que representantes gubernamentales difundieron descalificaciones sobre un niño con discapacidad, a partir de su participación pública y activismo¹²⁹: “el gobierno está mirando las redes para ver qué opina la gente”, afirmó uno de los participantes.

De esta manera, entre las personas entrevistadas podemos ver consenso en la percepción tanto a que el gobierno puede disponer de información sistematizada sobre las personas o que pueden haber seguido su trabajo de cerca. A partir de esta base de su percepción de la vigilancia, las personas fueron consultadas sobre la modificación de sus prácticas en el marco de su trabajo y activismo. Estas respuestas permiten analizar si se ven afectados sus derechos a la libertad de reunión y expresión.

7.2 LA CONTRACCIÓN DEL ESPACIO DE REUNIÓN

Las respuestas de las personas entrevistadas dan cuenta de un impacto de la percepción de la vigilancia en los derechos de libertad de asociación, reunión y expresión, aunque no de forma generalizada.

Ana Tapia, por ejemplo, afirma que las fuerzas de seguridad prestan especial atención a lo que hacen desde la organización. Sin embargo, esto no las amedrenta: “No dejamos de ir, pero cambiamos estrategias”.

Por otro lado, Matías Darabós, representante de ACVI, fue víctima, al igual que Tapia, de violencia policial, lo que tuvo un impacto en su predisposición a participar y monitorear movilizaciones: “Después de la patada

¹²⁸ Modismo del español argentino (lunfardo), puede entenderse como “vigilado” o “detectado”.

¹²⁹ Amnistía Argentina generó una campaña en redes al respecto, para poner foco en la importancia de defender los derechos humanos de niños, niñas y adolescentes: <https://x.com/amnistiaar/status/1929616300768133280?s=20>

que me pegaron [las fuerzas policiales], dejé de ir a algunas marchas. Antes hacíamos uno o dos grupos para cubrir más territorio; ahora tratamos de estar todos juntos. Eso limita la capacidad operativa”.

Este fenómeno también se da en los trabajadores de prensa. “Hay compañeros y compañeras que hoy dudan en salir a las calles bajo la bandera de la organización. Sabemos que tienen todos nuestros datos, sabemos que hay compañeros que son atacados por fuerzas de seguridad, que reciben amenazas y que saben absolutamente todos nuestros movimientos”, afirma Paula Cejas. Luego, la representante de la FIP para América Latina habló sobre cómo la presencia y represión policial generaron un cambio en las formas de comunicación de las organizaciones: “Se modificaron prácticas: algunos dejaron de usar WhatsApp y pasaron a Signal o Telegram. Se entregaron elementos de protección como cascos y chalecos, algo que nunca antes se había hecho”. Lo mismo comenta la periodista especializada en temas de género, Participante 6, que no se ve disuadida de ir a las marchas, pero tomó estrategias: “lo cuento en redes, aviso a mi familia, hablo con colegas sobre qué hacer si se descontrola todo”.

Hay una tensión que se da entre la exposición requerida por el trabajo de prensa y la percepción de ser registrados por las fuerzas de seguridad. En este sentido, Alejo Fraile, integrante del Mapa de la Policía, afirma lo siguiente: “ahora ya no voy tanto a las marchas. Voy a las masivas nomás que sé que no van a reprimir”. El Mapa de la Policía es un proyecto llevado adelante por un colectivo multidisciplinario de activistas, en colaboración con organizaciones defensoras de los derechos humanos y medios periodísticos. Su trabajo permitió identificar a policías responsables de generar lesiones en manifestantes, como fue el caso del fotógrafo Pablo Grillo, herido gravemente por una munición de gas lacrimógeno lanzada de forma recta, en contra de los protocolos en la materia. Esto pudo ser comprobado gracias a un análisis forense realizado por el colectivo.¹³⁰

Ante la pregunta sobre la posibilidad de dejar de asistir a una marcha por sentirse vigilada, una persona, trabajadora de prensa, que llamaremos Participante 7, señaló que su decisión no está tanto vinculada al monitoreo, sino al riesgo de represión en el espacio físico. Explicó que la vigilancia le resulta más abstracta, mientras que la posibilidad de sufrir violencia directa, como el uso de gases o agresiones, aparece como un riesgo inmediato y concreto. En ese sentido, indicó que su situación personal, como principal sostén económico de su familia, influye en sus decisiones. Evitar daños físicos es una prioridad, ya que podrían impedirle trabajar. Por ello, afirmó que ha reducido su participación en manifestaciones y que actualmente solo asiste cuando es por motivos laborales, priorizando el cuidado personal por sobre otras motivaciones.

La conjunción de represión y políticas de vigilancia generaron un efecto puntual en los migrantes. Como fue mencionado previamente, el llamado “Protocolo antipiquetes”¹³¹ estableció que se informaría a la autoridad migratoria la presencia de personas migrantes que impidan la circulación en el marco de una protesta. Al respecto, dos personas migrantes que participaron en la entrevista grupal a jóvenes afirmaron haber dejado de participar por temor a represalias, como perder su status migratorio.

LOS JÓVENES FRENTE A LA VIGILANCIA ESTATAL: ESTRATEGIAS DE RESGUARDO Y GESTIÓN DE LA VISIBILIDAD

Aunque las entrevistas realizadas no muestran una afectación claramente diferenciada de la percepción de vigilancia en función de la edad, sí permiten identificar algunos matices relevantes en las experiencias y prácticas de las personas jóvenes entrevistadas. En términos generales, sus percepciones sobre el fenómeno, así como las estrategias desplegadas para afrontarlo, resultan similares a las observadas en otros perfiles entrevistados, especialmente entre quienes mantienen trayectorias de activismo social, político o de género. En este sentido, la pertenencia a espacios militantes o de defensa de derechos parece tener mayor incidencia que la condición etaria en sí misma.

Por otra parte, algunas de las situaciones de mayor vulnerabilidad identificadas entre jóvenes entrevistados se vinculan en características personales como, por ejemplo, la condición migrante, más que con la juventud como categoría específica. En algunos casos, estas condiciones incidieron directamente en la modificación de prácticas cotidianas, particularmente en relación con la circulación, la participación pública y la expresión en espacios digitales. En el ejemplo citado, la condición migrante asociada a las políticas de vigilancia fue determinante para la modificación de las prácticas de la persona entrevistada.

Sin embargo, sí se observa una dimensión particularmente significativa en relación con las redes sociales y los espacios digitales. Varias personas jóvenes entrevistadas mencionaron haber reducido sus

¹³⁰ Disponible en <https://mapadelapolicia.com/>. Consultado en diciembre de 2025.

¹³¹ Establecido por la Resolución 943/2023 del Ministerio de Seguridad.

publicaciones, cerrando sus perfiles o moderando sus intervenciones en plataformas digitales, principalmente a partir de experiencias de hostigamiento, mensajes de odio o amenazas recibidas en esos espacios. Si bien estas situaciones no fueron atribuidas exclusivamente a vigilancia estatal, sí aparecen vinculadas a un contexto más amplio de exposición y conflictividad percibida. En este marco, las transformaciones observadas no remiten únicamente a prácticas de autocensura, sino también a estrategias de autocuidado y gestión selectiva de la visibilidad, orientadas a reducir riesgos percibidos en entornos considerados potencialmente adversos.

Dado que las redes sociales ocupan un lugar central en las formas contemporáneas de sociabilidad, expresión e intercambio político, estas modificaciones adquieren una relevancia específica para las personas jóvenes entrevistadas. En este sentido, más que una afectación diferencial asociada directamente a la vigilancia, los testimonios sugieren procesos de autocuidado y gestión de la visibilidad digital frente a escenarios percibidos como potencialmente hostiles.

7.3 AUTOCENSURA Y FALTA DE GARANTÍAS PARA LA LIBERTAD DE EXPRESIÓN

Las entrevistas muestran una variedad de posturas frente a este punto. Por ejemplo, la fotógrafa Bianca Abella no deja de ir a las protestas ante la represión y la vigilancia policial, aunque marca un matiz:

“a mí lo que me pasa es que yo necesito ir a cubrir eso y mostrar lo que sucede, necesito mostrarlo, aunque muchas veces te cuidás demasiado y eso limita también lo que vos querés mostrar. También limita que vaya cada vez menos gente o que no pueda sacarle fotos porque tienen miedo de salir publicadas en algún medio”.

En el mismo sentido, desde el colectivo de personas jubiladas, Ana Tampia manifestó: “Yo digo lo que tengo que decir, sea donde sea... no hay que callarse. Lo menos que uno puede hacer es callarse”.

En el mismo sentido, desde el Sindicato de Prensa de Buenos Aires, Agustín Cecchi señaló que, frente a un contexto percibido como más represivo, desde el sindicato adoptaron medidas de mayor cuidado y coordinación en la participación en movilizaciones, pero afirmó que ello no implicó dejar de manifestarse ni modificar sustantivamente sus posiciones públicas o formas de expresión.

Dos personas manifestaron preocupación respecto de un punto críticamente significativo para el trabajo del periodismo, que es el cuidado de la privacidad de las fuentes. Paula Cejas, de la Federación Internacional de Periodistas (FIP), destacó la magnitud del sistema de videovigilancia en la Ciudad de Buenos Aires y su potencial para monitorear e identificar personas en el espacio público. Señaló que esta situación afecta, en términos de percepción y como demanda del sector, el ejercicio del periodismo, especialmente por el impacto en la confidencialidad de las fuentes. En sus palabras, “es muy difícil poder tener libertad para tener contacto con esas fuentes” en un contexto de cámaras, posible intervención de comunicaciones y acceso a datos biométricos. Además, cuestionó la falta de información por parte de las autoridades sobre el alcance y funcionamiento de estos sistemas de vigilancia.

En el mismo sentido, Participante 4 señaló que, si bien los periodistas no suelen ser el foco principal de vigilancia, su principal preocupación radica en la protección de sus fuentes. Advirtió que los sistemas de monitoreo podrían permitir reconstruir sus movimientos, por ejemplo, al identificar dónde se reúnen con entrevistados o con quiénes se encuentran, lo que pone en riesgo la confidencialidad. Mencionó además que este tipo de seguimiento ya se ha observado en otros contextos, como en un caso en Brasil, y subrayó que, aunque no tenga evidencia directa en Buenos Aires, considera que es técnicamente posible y relativamente fácil de implementar.

Por su parte, Participante 7 relató una experiencia personal marcada por episodios de espionaje en dos momentos distintos. Por un lado, al igual que otras experiencias mencionadas, durante el G20 bajo el gobierno de Mauricio Macri, cuando se elaboró un perfil político sobre su persona a partir de sus publicaciones en redes sociales, interpretando incluso contenidos publicados como indicios de posicionamiento político. Por otro, en el contexto de una investigación periodística que llevaba adelante, identificó que tanto ella como su colega habían sido incluidas en pedidos masivos de datos y que, en su caso, tuvo evidencia de seguimientos con datos biométricos en distintas ocasiones. Asimismo, señaló que en ese momento intentaron avanzar para conocer cómo se había obtenido la información y qué datos habían sido efectivamente recolectados. Sin embargo, ante la posibilidad de iniciar acciones legales, decidió

no continuar con el proceso por temor a posibles represalias, incluyendo riesgos para su familia, en particular para sus hijos, considerando el nivel de acceso estatal a información personal. En consecuencia, optaron por no seguir adelante, en un ejercicio de autocensura.

ATAQUES Y CAMBIOS DE ACTITUD EN LAS PLATAFORMAS: MANIFESTACIONES DIGITALES DE LA AUTOCENSURA

Varias de las personas entrevistadas señalaron haber modificado su comportamiento en redes sociales, incluso cuando mantienen perfiles públicos o desarrollan actividades que requieren visibilidad. Estos cambios no siempre se vinculan de manera directa con actos de vigilancia estatal, pero sí aparecen asociados a un clima de hostigamiento digital, discursos violentos, amenazas por mensajes directos y ataques coordinados de forma actual o en base a la percepción de las personas entrevistadas. En muchos testimonios, además, las personas entrevistadas perciben una relación entre el aumento de la represión estatal, la estigmatización pública de voces críticas y el accionar de grupos organizados o semiorganizados en redes sociales.

En este sentido, Alejo Fraile, del Mapa de la Policía, señaló que, a partir del trabajo de monitoreo que realizan desde espacios de investigación vinculados a medios como Revista Crisis, han podido identificar patrones sistemáticos en prácticas de hostigamiento en redes sociales, particularmente en casos de *doxéo* y ataques coordinados. Indicó que, a través de herramientas de registro y seguimiento, detectaron que muchas de las cuentas que participan en estos ataques presentan características similares, como perfiles con escasa actividad orgánica, pocos o ningún seguidor y comportamientos repetitivos. Estos ataques se dan en publicaciones sobre investigaciones que critican el accionar policial.

Asimismo, Emilio Lazlo, del canal de *streaming* Gelatina, mayoritariamente opositor al gobierno actual, describió episodios concretos en los que, ante determinadas publicaciones o apariciones públicas, se producen oleadas de comentarios agresivos dirigidos a personas específicas, muchas veces con referencias a su vida personal o familiar. Según su análisis, estos comportamientos no responden a dinámicas espontáneas, sino que evidencian cierto grado de organización y coordinación.

Matías Darabós, referente de ACVI, se refirió puntualmente a los comentarios recibidos en las publicaciones en redes sociales, uno de los principales canales de difusión del trabajo de la organización, donde analizan abusos policiales: “Siempre en las publicaciones hay gente insultándote, amenazándote... eso te hace ser precavido y pensar cómo uno se expone. Algunos compañeros prefieren no dar la nota, no aparecer”.

Paula Cejas, de la FIP, expresó que las redes sociales no son un espacio seguro: “Ya no es un espacio seguro ni las redes ni las calles para los periodistas. Incluso yo misma pienso qué voy a subir en las redes de la FIP, qué lenguaje usar para que no me metan en una lista y después recibamos hostigamiento”.

En el mismo sentido, Participante 6 afirmó que cambió totalmente su participación en redes: “Antes opinaba de todo, ahora lo uso de manera recreativa. Pienso mucho las palabras que uso, moderé mi discurso y bajé mi participación 100%, sobre todo en Twitter. Represento todo lo que molesta: soy mujer, periodista, feminista y defensora de derechos humanos”.

En la entrevista grupal a jóvenes este punto tuvo particular relevancia. Por un lado, muchas de las personas entrevistadas manifestaron haber configurado sus redes sociales de modo privado, para tener un mejor control de seguidores, por ejemplo, afirmando que a partir de ahora si les pide seguir una persona con quien no tienen seguidores en común no lo aceptan porque “no puede dejar entrar a cualquier persona”. Las personas entrevistadas manifiestan que los comentarios de odio son uno de los principales motivos para restringir el acceso de terceros desconocidos a sus redes sociales, dado el aumento excesivo de este tipo de manifestaciones en algunas publicaciones por parte de personas dedicadas específicamente a descalificar.

En resumen, si bien muchas de las personas entrevistadas han persistido en su activismo y en defender su derecho a la protesta pese a las prácticas de vigilancia, también es cierto que muchas de ellas manifestaron haber generado cambios de comportamiento, tanto en el ejercicio de libertad de asociación y protesta, como del derecho a la libertad de expresión. Estas modificaciones en el comportamiento son resultado del

despliegue de políticas que tienen como finalidad la represión y vigilancia gubernamental: las políticas de vigilancia restringen el ejercicio de derechos aún más cuando son acompañadas por el uso de la fuerza en las calles.

8. CONCLUSIONES Y RECOMENDACIONES INICIALES

En este artículo fueron analizadas las reformas de los sistemas de seguridad e inteligencia, así como las tecnologías de vigilancia adquiridas por el Gobierno Nacional y de la Ciudad de Buenos Aires. Vimos Como fue analizado, el Gobierno Nacional generó reformas estructurales, a partir de la modificación de las competencias y funciones del Sistema de Inteligencia Nacional y fuerzas de seguridad, como la Policía Federal, y que adquirió un amplio abanico de tecnologías que pueden ser utilizadas para la vigilancia de las personas. Esto trae serios riesgos al marco de derechos humanos aplicable a la Argentina, que responde a estándares internacionales reconocidos por la Constitución Nacional y complementados por normativa local en materias como protección de datos personales y acceso a la información.

El análisis realizado permite afirmar que las prácticas de vigilancia y control apoyadas en tecnologías digitales se han consolidado como una de las áreas de mayor expansión dentro de las políticas de seguridad del Estado. La creación de nuevas unidades, protocolos y herramientas tecnológicas, así como la ampliación de facultades operativas de las fuerzas de seguridad, evidencian una priorización creciente del uso de tecnologías de vigilancia, incluidas aquellas basadas en inteligencia artificial, análisis de datos y monitoreo digital. Sin embargo, este proceso de expansión se ha desarrollado sin un marco normativo claro y específico, sin controles externos adecuados y con niveles insuficientes de transparencia, lo que plantea serias tensiones con las obligaciones internacionales del Estado argentino.

En particular, las prácticas analizadas muestran una tendencia a concentrar amplias capacidades de vigilancia que abarcan desde el monitoreo de redes sociales y fuentes digitales abiertas, hasta el uso de sistemas biométricos, drones y herramientas de análisis automatizado, sin que existan garantías claras respecto de su necesidad, proporcionalidad y legalidad. La amplitud y superposición de estas funciones, sumadas a la falta de delimitación precisa de competencias y responsabilidades institucionales, debilitan los mecanismos de supervisión y dificultan la rendición de cuentas. Este escenario resulta especialmente problemático a la luz de las obligaciones asumidas por el Estado argentino en materia de protección de los derechos de la privacidad, la libertad de expresión, la libertad de reunión pacífica y la libertad de asociación.

Quedan aún algunas dudas respecto del uso retrospectivo de tecnologías de reconocimiento facial para la identificación realizado por la Policía Federal. En caso de que, por ejemplo, la contratación de Clearview esté vinculada a este proceso, esto implicaría el análisis de datos masivos de ciudadanos que no necesariamente cuentan con procesos judiciales activos o pedidos de captura. Además, este tipo de softwares presentan desafíos a la hora de ser auditados.

Asimismo, el estudio de los efectos inhibidores de estas tecnologías permitió generar evidencia respecto de la modificación de las prácticas de las personas, por la represión en el contexto de las protestas y por sentirse vigiladas por el Gobierno.

Si bien las tecnologías y las políticas de vigilancia se han introducido como herramientas destinadas, en apariencia, a hacer frente a determinadas formas de actividad delictiva, la investigación de Amnistía

Internacional demuestra que la amplitud de las disposiciones legales y el historial documentado de abusos y uso indebido de estas tecnologías en Argentina vulneran los derechos a la privacidad, a la igualdad y la no discriminación, y a la libertad de expresión y de reunión pacífica, al tiempo que socavan la transparencia y el derecho de acceso a la información.

En este contexto, y considerando antecedentes recientes como el del Sistema de Reconocimiento Facial de Prófugos (SRFP), resulta imprescindible revisar y limitar el despliegue de prácticas de vigilancia tecnológica hasta tanto se adopten salvaguardas compatibles con el derecho internacional de los derechos humanos. Ello incluye la adopción de marcos legales específicos, la realización de evaluaciones de impacto sobre derechos humanos, la existencia de mecanismos de control independientes y efectivos, y la garantía de vías de recurso accesibles. En ausencia de estas condiciones, la expansión de las políticas de vigilancia representa un riesgo concreto de injerencias arbitrarias, con potenciales efectos disuasorios sobre el ejercicio del disenso, la participación política y la vida democrática.

Los hallazgos de este informe demuestra que el despliegue de tecnologías de vigilancia sin controles adecuados no solo vulnera derechos, sino que debilita la legitimidad de las políticas públicas y aumenta el riesgo de que surjan prácticas autoritarias y erosiona la confianza democrática en las instituciones del Estado. Donde el gobierno está involucrado en el despliegue de tecnologías de vigilancia masiva, como el reconocimiento facial para la identificación (1:n), esta tecnología debe ser prohibida.

Frente a este panorama, se formulan las siguientes recomendaciones:

8.1 AL GOBIERNO NACIONAL Y DE LA CIUDAD DE BUENOS AIRES:

- Prohibir el desarrollo, la producción, la venta y el uso, de tecnologías biométricas que posibiliten la vigilancia masiva y la vigilancia selectiva discriminatoria por parte de actores públicos y privados.
- Prohibir el desarrollo, la producción, la venta y el uso de sistemas de inteligencia artificial que creen o amplíen bases de datos de reconocimiento facial mediante la recopilación indiscriminada de imágenes faciales procedentes de Internet o de grabaciones de cámaras de videovigilancia (CCTV).
- Prohibir los sistemas automatizados de evaluación de riesgos y elaboración de perfiles en el contexto migratorio cuando se utilicen para determinar si las personas en movimiento representan un “riesgo” de participar en actividades ilícitas o de constituir una amenaza para la seguridad.
- Suspender de inmediato el uso de todas las tecnologías de vigilancia adquiridas o desplegadas sin un fundamento jurídico específico, sin evaluaciones de impacto sobre los derechos humanos y la protección de datos (EIPD), o sin mecanismos externos de supervisión. Esto incluye, en particular, las herramientas de monitoreo de fuentes abiertas y de vigilancia aérea.
- Establecer, en todos los procedimientos de contratación de tecnologías de vigilancia, la política pública específica en cuyo marco se utilizarán, a fin de garantizar la trazabilidad de todas las medidas adoptadas.
- Prohibir el uso de tecnologías de actuación policial predictiva, ya que estos sistemas reproducen y refuerzan sesgos históricos y carecen de fundamentos empíricos suficientes para justificar su impacto sobre los derechos fundamentales.
- Elaborar y adoptar una regulación vinculante de la inteligencia artificial basada en los derechos humanos, que cuente con mecanismos sólidos de aplicación y supervisión independiente, y garantizar que tanto la elaboración como la aplicación de dicha legislación se lleven a cabo mediante un proceso de formulación de políticas transparente, sujeto a rendición de cuentas, accesible y basado en normas, con una participación significativa de las comunidades afectadas y de las organizaciones de la sociedad civil.
- Establecer como requisito obligatorio la realización de una evaluación de impacto sobre la protección de datos (EIPD), a cargo de un organismo independiente y con consulta pública, para la implementación de cualquier herramienta que implique el tratamiento masivo o automatizado de datos personales.

- Constituir efectivamente, en el ámbito del Congreso Nacional, la Comisión Bicameral de Fiscalización de los Organismos y Actividades de Inteligencia, prevista en el artículo 31 de la Ley 25.520, y garantizar su correcto funcionamiento de conformidad con las facultades establecidas por la legislación.
- Rechazar las exenciones generales o desproporcionadas fundamentadas en motivos de actuación policial, seguridad nacional o defensa militar.
- Rechazar que se otorgue a las empresas desarrolladoras de sistemas de inteligencia artificial la facultad discrecional de quedar exentas de las normas establecidas.
- Crear y mantener bases de datos públicas, accesibles y disponibles para informar sobre el desarrollo y el despliegue de tecnologías de inteligencia artificial que puedan tener un impacto sobre los derechos humanos.
- Exigir a los proveedores de sistemas de inteligencia artificial con impacto sobre los derechos humanos que se inscriban y registren el sistema correspondiente en las bases de datos públicas pertinentes, incluso durante las pruebas de dichos sistemas en condiciones reales.
- Exigir a todas las entidades públicas y privadas que utilicen sistemas de inteligencia artificial capaces de afectar a los derechos humanos que registren su uso en las bases de datos públicas pertinentes.
- Exigir a las entidades usuarias que garanticen una transparencia significativa respecto de los sistemas de inteligencia artificial y de los procesos automatizados de toma de decisiones que tengan un impacto sobre los derechos humanos de las personas afectadas, incluso durante la fase de prueba de dichos sistemas.
- Exigir a los proveedores y a las entidades usuarias de sistemas de inteligencia artificial que divulguen de forma proactiva la información necesaria para evaluar el impacto de sus sistemas sobre los derechos humanos y que respondan a las solicitudes formuladas por organizaciones de interés público, incluidas las presentadas en ejercicio del derecho de acceso a la información.
- Establecer mecanismos de control efectivos, independientes y accesibles sobre el uso de tecnologías de vigilancia, que incluyan al menos:
 - autorización judicial previa para toda medida de vigilancia que pueda afectar derechos individuales, sujeta a criterios de legalidad, necesidad, proporcionalidad y no discriminación;
 - control administrativo a cargo de organismos con competencia en la materia, como la Agencia de Acceso a la Información Pública, la Defensoría del Pueblo y órganos de auditoría y control, entre otros que resulte necesario crear o designar, dotados de facultades efectivas de inspección, auditoría y sanción, así como la asignación de recursos suficientes;
 - revisión legislativa periódica sobre adquisiciones, uso y resultados de las políticas de vigilancia;
 - y garantía del derecho de las personas afectadas a conocer, en los términos que permita la ley, si fueron objeto de vigilancia, e impugnar su legalidad ante una instancia independiente.
- Garantizar el principio de transparencia en todas las acciones vinculadas al uso de tecnologías de vigilancia, mediante la publicación periódica y accesible de información sobre las tecnologías adquiridas, los contratos y proveedores involucrados, los protocolos de uso vigentes y los resultados de auditorías; y respondiendo de manera sustantiva los pedidos de acceso a la información pública en la materia, sin invocar excepciones de forma amplia o injustificada.

8.2 AL GOBIERNO NACIONAL Y ESPECIALMENTE AL MINISTERIO DE SEGURIDAD:

- Publicar de manera inmediata la información sustantiva sobre la estructura, presupuesto, proveedores y criterios técnicos de todas las funciones asignadas a la UIAAS, como condición mínima de transparencia y rendición de cuentas.
- Crear una mesa intersectorial con participación de organismos de control, sociedad civil, expertos en tecnología y derechos humanos, con mandato, plazos y resultados esperados definidos, orientada a revisar los alcances de la UIAAS y establecer criterios consensuados para su regulación.
- Realizar una revisión técnica e institucional de los convenios de cooperación entre el Estado nacional y las jurisdicciones locales, en especial en relación con el uso de infraestructura de videovigilancia, datos biométricos y software propietario, garantizando estándares mínimos de interoperabilidad, transparencia y control.

8.3 AL CONGRESO DE LA NACIÓN:

- Conformar y garantizar el efectivo funcionamiento de la Comisión Bicameral de Fiscalización de los Organismos y Actividades de Inteligencia, en cumplimiento del artículo 31 de la Ley 25.520, dotándola de los recursos y facultades necesarios para el control específico de las tecnologías de vigilancia.
- Promover un debate parlamentario para la regulación del uso de tecnologías de vigilancia, que establezca definiciones claras, habilitaciones específicas, límites de uso y prohibiciones, salvaguardas, mecanismos de control independiente y sanciones ante incumplimiento, en línea con los estándares internacionales de derechos humanos.

8.4 A LOS ORGANISMOS REGIONALES E INTERNACIONALES DE DERECHOS HUMANOS

- Promover la adopción de legislación que prohíba el uso, el desarrollo, la producción, la venta y la exportación de tecnologías de reconocimiento biométrico remoto para la vigilancia masiva, así como de tecnologías de reconocimiento biométrico remoto o de reconocimiento facial utilizadas con fines de identificación dentro de sus respectivas jurisdicciones, tanto por organismos estatales como por actores del sector privado, por tratarse de tecnologías fundamentalmente incompatibles con el derecho internacional de los derechos humanos.
- En tanto no se adopte dicha prohibición, y de conformidad con la recomendación de la Relatora Especial de las Naciones Unidas sobre las formas contemporáneas de racismo, la discriminación racial, la xenofobia y las formas conexas de intolerancia, adoptar “medidas rápidas y eficaces para prevenir y mitigar el riesgo de que las tecnologías digitales emergentes sean diseñadas o utilizadas de manera racialmente discriminatoria, entre otras cosas, exigiendo que la realización de evaluaciones de impacto sobre los derechos humanos en materia de igualdad racial y no discriminación constituya un requisito previo para la adopción, por parte de las autoridades públicas, de sistemas basados en dichas tecnologías. Estas evaluaciones de impacto deben incorporar oportunidades significativas de codesarrollo y coimplementación con representantes de grupos racial o étnicamente marginados. Un enfoque exclusivamente, o incluso predominantemente, voluntario respecto de las evaluaciones de impacto en materia de igualdad no será suficiente; es indispensable que dichas evaluaciones tengan carácter obligatorio”.¹³²

¹³² [United Nations Human Rights Council, Racial discrimination and emerging digital technologies: a human rights analysis: report of the Special Rapporteur on Contemporary Forms of Racism, Racial Discrimination, Xenophobia and Related Intolerance, UN Doc A/HRC/44/57, 18 June 2020. https://digitallibrary.un.org/record/3879751 accessed 2 February 20](https://digitallibrary.un.org/record/3879751)

ANEXO 1 – DETALLE DE COMPRAS Y CONTRATACIONES

COMPRAS Y CONTRATACIONES DEL GOBIERNO NACIONAL

ID	Nº DE PROCESO LIC	Nº ÓRDEN DE COMPRA	FECHA RESO OC	JURISDICCIÓN	NOMBRE DE PROCESO	PROCESO DE SELECCIÓN	DURACIÓN CONTRATO	TIPO	MONTO ARS	MONTO USD	AVAILABLE AT
NAC-01	347-0026-CDI25	347-0095-OC25	29/10/2025	Nación	Adquisición de una licencia de un software de apoyo para investigaciones en el marco del ForCIC	Contratacion Directa	12 Meses	Sin modalidad		33,500	Link
NAC-02	347-0024-CDI25	347-0091-OC25	15/10/2025	Nación	Renovación, actualización, mantenimiento y soporte de licencia de plataforma para investigación en fuentes abiertas	Contratacion Directa	12 Meses	Sin modalidad		239,013	Link
NAC-04a	347-0009-LPU24	347-0059-OC24	28/08/2024	Nación	Adquisición de Vehículos Aéreos No Tripulados (VANT) compactos, para Seguridad Pública	Licitacion Pública	90 Días corridos	Sin modalidad		417,530	Link
NAC-04b	347-0009-LPU24	347-0064-OC24	19/09/2024	Nación	Adquisición de Vehículos Aéreos No Tripulados (VANT) compactos, para Seguridad Pública	Licitacion Pública	90 Días corridos	Sin modalidad		134,155	Link

ID	Nº DE PROCESO LIC	Nº ÓRDEN DE COMPRA	FECHA RESO OC	JURISDICCIÓN	NOMBRE DE PROCESO	PROCESO DE SELECCIÓN	DURACIÓN CONTRATO	TIPO	MONTO ARS	MONTO USD	AVAILABLE AT
NAC-05a	347-0020-LPU25	347-099-OC05	01/12/2025	Nación	Adquisición centralizada de estaciones terrestres de operación de Vehículos Aéreos No Tripulados (VANT), en modalidad "Cautivos".	Licitacion Pública	90 Días corridos	Sin modalidad		355,750.00	Link
NAC-05b	347-0020-LPU25	347-0106-OC25	23/12/2025	Nación	Adquisición centralizada de estaciones terrestres de operación de Vehículos Aéreos No Tripulados (VANT), en modalidad "Cautivos".	Licitacion Pública	90 Días corridos	Sin modalidad		35,575.00	Link
NAC-06	347-0029-CDI24	347-0089-OC24	13/11/2024	Nación	Nosis Laboratorio de Investigación y Desarrollo S.A.	Contratacion Directa	12 Meses	Sin modalidad	18,381,663.36	17,863.79 ¹³³	Link

COMPRAS Y CONTRATACIONES DEL GOBIERNO DE LA CIUDAD DE BUENOS AIRES

ID	Nº DE PROCESO LIC	Nº ÓRDEN DE COMPRA	FECHA RESO OC	JURISDI CCIÓN	NOMBRE DE PROCESO	PROCESO DE SELECCIÓN	DURACIÓN CONTRATO	TIPO	MONTO ARS	MONTO USD	LINK	COMENTARIOS
CABA-01	2900-1208-LPU20	2900-0036-OCA21	23/12/2025	Ciudad	Contratación de servicios de análisis de imágenes de video y gestión de alertas	Licitación pública	24 Meses	Orden de Compra Abierta	701,656,557	4,997,281	Link	El monto en pesos representa la suma de cada prórroga con sus respectivos aumentos. El monto en dólares representa la suma de cada monto

¹³³ Tipo de cambio utilizado USD: 1028.99

ID	N° DE PROCESO LIC	N° ÓRDEN DE COMPRA	FECHA RESO OC	JURISDI CCIÓN	NOMBRE DE PROCESO	PROCESO DE SELECCIÓN	DURACIÓN CONTRATO	TIPO	MONTO ARS	MONTO USD	LINK	COMENTARIOS
												según la referencia del dólar de la fecha de resolución o apertura de llamado licitatorio.
CABA-02	3202-1155-LPU25	3202-0419-OCA25	06/11/2025	Ciudad	provisión y migración de licencias para el fortalecimiento de las capacidades forenses digitales	Licitación pública	12 meses	Orden de Compra Abierta	1,222,237,276.04	828,916	Link	Cotización utilizada: 1 USD = ARS 1474,5. En función de cotización Res de adjudicación.
CABA-03	3202-0928-LPU25	3202-0381-OCA25	17/10/2025	Ciudad	Servicio de mantenimiento eléctrico y energización de puntos de captura de video	Licitación pública	24 Meses	Orden de Compra Abierta	1,123,628,600	810,956	Link	Cotización utilizada: 1 USD = ARS 1.385,56. Según Tipo de Cambio Minorista de Referencia BCRA (comprador) para el 31 de julio de 2025, fecha de apertura de la licitación.
CABA-04	3202-0970-LPU25	3202-15648-OC25	02/10/2025	Ciudad	Contratación de un servicio de Análisis de Datos	Licitación pública	24 Meses	Sin Modalidad	120,720,000	93,804.64	Link	Cotización utilizada: 1 USD = ARS 1.286,93. Según Tipo de Cambio Minorista de Referencia BCRA (comprador) para el 13 de agosto de 2025, fecha de apertura de la licitación.

ID	N° DE PROCESO LIC	N° ÓRDEN DE COMPRA	FECHA RESO OC	JURISDI CCIÓN	NOMBRE DE PROCESO	PROCESO DE SELECCIÓN	DURACIÓN CONTRATO	TIPO	MONTO ARS	MONTO USD	LINK	COMENTARIOS
CABA-05	3202-0066-LPU25	3202-0184-OCA25	23/06/2025	Ciudad	Servicio de conectividad para los dispositivos pertenecientes a la plataforma de seguridad por video	Licitación pública	12 meses	Orden de Compra Abierta	14,823,189,156	14,184,463	Link	Cotización utilizada: 1 USD = ARS 1045,03. Según Tipo de Cambio Minorista de Referencia BCRA (comprador) para el 3 de abril de 2025, fecha de apertura de la licitación.
CABA-06	3202-0540-LPU24	3202-0132-ICA24	8/5/2025	Ciudad	Adquisición de puntos de captura y el hardware y software para su procesamiento y almacenamiento	Licitación pública	24 meses	Orden de Compra Abierta	25,102,477,483	27,077,219.07	Link	Cotización usada: 1 USD = ARS 927,07. En función de cotización en Res de adjudicación.

MONTOS ADQUISICIÓN DE PUNTOS DE CAPTURA BAJO RESOLUCIONES DE AMPLIACIÓN CABA

RENGLÓN	DESCRIPCIÓN (SEGÚN PLIEGO TÉCNICO)	OC ORIGINAL RES. 984/MSEGC/24 11 OCTUBRE 2024	INCREMENTO 1 RES. 1186/MSEGC/24 11 DICIEMBRE 2024	INCREMENTO 2 RES 26/SSGA/25 5 DE FEBRERO 2025	INCREMENTO 3 RES. 511/MSEGC/25 8 DE MAYO 2025	MONTOS TOTALES	
1	Adquisición e instalación de puntos de captura de video para el plan integral de videovigilancia.	Ciento cincuenta (150) unidades. USD 2.341.800,00	cuatrocientas (400) unidades USD 6.244.800,00	Sin incremento	Sin incremento	trescientas (300) unidades USD 4.683.600,00	USD 13.270.200,00
2	Adquisición e implementación de hardware y software para el procesamiento y gestión de dispositivos de captura de video para el sistema de Videovigilancia propiedad del MSEGC.	Tres (3) unidades. USD 429.345,00	seis (6) unidades USD 858.690,00	Sin incremento	Sin incremento	seis (6) unidades USD 858.690,00	USD 2.146.752,00
3	Adquisición e implementación de hardware y software de almacenamiento de imágenes para el sistema de Videovigilancia propiedad del MSEGC.	Tres (3) unidades. USD 1.302.854,58	seis (6) unidades USD 2.605.709,16	Sin incremento	Sin incremento	seis (6) unidades USD 2.605.709,16	USD 6.514.272,9
4	Servicio de soporte técnico, mesa de ayuda y mantenimiento del hardware para centros de monitoreo y centro	Veinticuatro (24) meses. USD 4.234.964,16	Sin incremento	Sin incremento	Sin incremento	Sin incremento	USD 4.234.964,16

REGLÓN	DESCRIPCIÓN (SEGÚN PLIEGO TÉCNICO)	OC ORIGINAL RES. 984/MSEGC/24 11 OCTUBRE 2024		INCREMENTO 1 RES. 1186/MSEGC/24 11 DICIEMBRE 2024		INCREMENTO 2 RES 26/SSGA/25 5 DE FEBRERO 2025		INCREMENTO 3 RES. 511/MSEGC/25 8 DE MAYO 2025		MONTOS TOTALES
	de datos del sistema de videovigilancia propiedad del MSEGC.									
5	Adquisición de las partes que componen los centros de monitoreo del sistema público de videovigilancia del MSEGC según ítems del CUADRO II.	Una (1) unidad.	USD 438.667,60	<i>Sin incremento</i>	<i>Sin incremento</i>	Incremento en 30 unidades para los ítems 1 y 2.	USD 457.493,40.	<i>Sin incremento</i>	<i>Sin incremento</i>	USD 896.161
6	Servicio de asistencia técnica presencial para soporte en Centro de Monitoreo.	Setenta y dos (72) módulos	ARS 13.759.200	<i>Sin incremento</i>	<i>Sin incremento</i>	<i>Sin incremento</i>	<i>Sin incremento</i>	<i>Sin incremento</i>	<i>Sin incremento</i>	ARS 13.759.200
Total USD con monto en \$:									27,077,219.07	

**AMNISTÍA INTERNACIONAL ES
UN MOVIMIENTO GLOBAL DE
DERECHOS HUMANOS.
LAS INJUSTICIAS QUE
AFECTAN A UNA SOLA
PERSONA NOS AFECTAN
A TODAS LAS DEMÁS.**

CONTÁCTANOS



contactus@amnesty.org



+44 (0)20 7413 5500

ÚNETE A LA CONVERSACIÓN



www.facebook.com/amnesty



@Amnesty

ESTADO DE VIGILANCIA

LA EXPANSIÓN DEL USO DE TECNOLOGÍAS DE VIGILANCIA MASIVA POR EL GOBIERNO DE ARGENTINA

Entre diciembre de 2023 y diciembre de 2025, el Gobierno argentino implementó una serie de reformas en materia de seguridad e inteligencia y amplió el uso de tecnologías de vigilancia. En sólo dos años, el Gobierno nacional impulsó un conjunto de reformas institucionales destinadas a ampliar sus capacidades de vigilancia e inteligencia, implementadas principalmente a través de decretos y resoluciones, sin debate parlamentario.

Este informe muestra que el despliegue de políticas y tecnologías de vigilancia en Argentina, tanto a nivel nacional como municipal, tiene repercusiones directas en los derechos humanos, además de efectos indirectos significativos en el ejercicio de los derechos humanos, al perpetuar la discriminación y coartar la libertad de expresión y de reunión pacífica