ICCSI

INICIATIVA CIUDADANA PARA
EL CONTROL DEL SISTEMA
DE INTELIGENCIA

ESTADO DEL MARCO REGULATORIO DE LA INTELIGENCIA EN ARGENTINA

2025

Documento de trabajo de la Iniciativa para el Control del Sistema de Inteligencia (ICCSI).

5 de diciembre de 2025.

Con el apoyo de

HEINRICH BÖLL STIFTUNG
BUENOS AIRES
Argentina | Uruguay | Paraguay

CONTENIDOS

ICCSI

I. INTRODUCCIÓN

Durante los años 2024[1] y 2025 se llevaron adelante en Argentina una serie de reformas que modificaron de manera significativa la estructura, el alcance y las prácticas del Sistema de Inteligencia Nacional, así como las funciones de la policía y fuerzas de seguridad federales. Estas reformas se realizaron a través de decisiones administrativas, decretos de necesidad y urgencia, modificaciones presupuestarias, reestructuraciones orgánicas y quedaron plasmadas en los lineamientos estratégicos del supuesto nuevo Plan de Inteligencia Nacional (PIN)[2].

Todas estas modificaciones convergen en un mismo proceso: la expansión del poder de vigilancia estatal, la centralización de funciones en organismos de inteligencia, el debilitamiento de los mecanismos de control democrático y el aumento del secreto en la producción, almacenamiento y uso de información. Estas medidas no sólo reconfiguran el equilibrio institucional previsto por las leyes de Inteligencia, Seguridad Interior y Defensa Nacional, así como Protección de Datos Personales y Acceso a la Información, sino que impactan directamente en derechos fundamentales como la libertad de expresión, la protesta social, la participación política, la privacidad, la libertad personal, la igualdad y no discriminación, la presunción de inocencia, entre otros.

En este documento analizamos cuatro aspectos clave de las reformas del sistema de inteligencia: 1) los lineamientos conocidos del Plan de Inteligencia Nacional que habilita vigilancia sobre la disidencia política y social, 2) la ampliación de facultades de inteligencia en fuerzas de seguridad federales, 3) la centralización de la política de ciberseguridad en la SIDE y el intercambio de información personal, y 4) el aumento presupuestario para las actividades de inteligencia.

[1] Nos referimos en particular a la reforma del Sistema de Inteligencia hecha por DNU 614/24 y su reglamentario 615/24, cuya constitucionalidad discutimos judicialmente. Para más información sobre la causa judicial y la reforma en general, recomendamos ICCSI (2024), "Comentarios sobre la reforma del sistema de inteligencia" y CELS (2024), "Pedimos al Poder Judicial que declare inconstitucional el dnu que reformó el sistema de inteligencia".

[2] Este documento fue filtrado a la prensa y publicado por el diario La Nación. Si bien fue reconocido por el entonces vocero presidencial Manuel Adorni en sus conferencias diarias, su contenido no fue confirmado oficialmente por otras autoridades ni en el marco de la causa penal que impulsamos (ver nota al pie nº 7). A lo largo de este documento nos referiremos al documento que fue difundido a través de la prensa como PIN.

II. PLAN DE INTELIGENCIA NACIONAL (PIN): VIGILANCIA DE LA DISIDENCIA

CONTEXTO

El Plan de Inteligencia Nacional (PIN) elaborado por la SIDE constituye el principal instrumento de orientación estratégica del sistema de inteligencia argentino. Debe definir prioridades, riesgos, amenazas y objetivos, y está sujeto a control de la Comisión Bicameral de Fiscalización de Organismos y Actividades de Inteligencia (Ley 25.520, Art. 33), que debe elevar un informe anual al Congreso y al Poder Ejecutivo sobre su "consideración, análisis y evaluación de la ejecución".

En mayo de 2025 se filtraron a la prensa extractos del que sería el nuevo PIN[3] y disposiciones de una directiva secreta para "monitorear la acción de grupos sociales vulnerables"[4]. En agosto trascendió el seguimiento sistemático que la SIDE había realizado a referentes políticos y sindicales antes del cierre de listas electorales en la provincia de Buenos Aires[5], en los términos establecidos por el Plan.

En un contexto de conflictividad social e importantes restricciones al espacio cívico, y en un año electoral, directivas de estas características remiten a una larga experiencia de órdenes que dieron lugar a vigilancia ilegal de referentes, familiares, organizaciones sociales y políticas, y en algunos casos justificaron intervenciones represivas muy violentas. Resultan violatorias de la ley 25.520 y de los límites que imponen los estándares internacionales a las acciones de los organismos de inteligencia de cualquier Estado. Es correcto que desde la SIDE se produzca información sistematizada para informar al Presidente, pero de ninguna manera puede hacerlo sobre la base de objetivos ilegales. Un instrumento de esta naturaleza requiere definiciones precisas y compatibles con las previsiones legales y estándares democráticos, como por ejemplo la exclusión de toda vigilancia por motivos políticos, ideológicos o sociales. Este Plan iría en sentido contrario.

DE QUÉ SE TRATA

El Plan y la directiva que lo operativiza redefinen los riesgos y amenazas a la seguridad nacional de una manera tan amplia que consolida al aparato de inteligencia como una herramienta política del gobierno orientada a vigilar la disidencia.

[3] Alconada Mon, H. (25/05/2025) "La SIDE pone la mira en quienes "manipulen la opinión pública" o erosionen la confianza en los funcionarios", *La Nación.*
[4] Alconada Mon, H. (27/05/2025) "La SIDE emitió una directiva secreta para "monitorear" la acción de "grupos sociales vulnerables", *La Nación.*
[5] Lacour, Pedro (5/08/2025) "Los tribunales y el Congreso ponen la lupa sobre la SIDE, mientras el gobierno niega que haya espionaje político", *El Diario Ar.*

Según la información disponible en los medios de comunicación[6], el Plan de Inteligencia Nacional elaborado presenta como focos de interés para su actividad a "todos aquellos que busquen 'erosionar' la confianza de la opinión pública sobre los funcionarios", o quienes "generen o puedan generar una 'pérdida de confianza' en las 'políticas económicas' del Gobierno". También a "todos aquellos que puedan 'manipular' a la opinión pública durante los procesos electorales o propagar la 'desinformación' (...) promuevan la 'distorsión' de la 'percepción' y afecten los procesos 'cognitivos' de la opinión pública". Define, luego, una serie de amenazas sobre las que se ordenan prácticas de vigilancia, totalmente contrapuestas a las habilitaciones legales con las que hoy cuenta la SIDE.

La Ley de Inteligencia 25.520, en su art. 4.2, prohíbe taxativamente *"Obtener información, producir inteligencia o almacenar datos sobre personas, por el solo hecho de su raza, fe religiosa, acciones privadas, u opinión política, o de adhesión o pertenencia a organizaciones partidarias, sociales, sindicales, comunitarias, cooperativas, asistenciales, culturales o laborales, así como por la actividad lícita que desarrollen en cualquier esfera de acción"*. En el inciso siguiente, prohíbe la influencia de los organismos de inteligencia en los asuntos públicos del país ("situación institucional, política, militar, policial, social y económica del país, en su política exterior, en la vida interna de los partidos políticos legalmente constituidos, en la opinión pública, en personas, en medios de difusión o en asociaciones o agrupaciones legales de cualquier tipo"). Cuestiones que este Plan parecería estar promoviendo: hipótesis de seguimiento político e influencia en la opinión pública, estrictamente prohibidas[7].

"AMENAZAS"

En el marco del PIN se redefine el concepto de "amenaza" de manera tan amplia que habilita la vigilancia política, social y cultural de sectores que históricamente fueron objeto de inteligencia ilegal. Algunos de los ejes que se enumeran como amenazas prioritarias son:

- La distorsión de la percepción pública, la confianza en las políticas económicas o la conversación pública: se habilita la vigilancia de actividades y expresiones políticas y sociales que consideren amenazas en este sentido (Objetivo Particular de Inteligencia 5), a través de facultades amplias y vagas, sin explicitar límites ni definir de manera precisa el alcance de estos términos. Resulta grave en tanto se trata de categorías de información sensible especialmente protegidas por el derecho internacional en general, y por la ley 25.520 en particular. En los hechos, esta caracterización amplia puede potencialmente incluir periodistas, analistas

[6] Para más información sobre el contenido del plan ver Colectivo Editorial Crisis (13/06/2025), "Controlar al pueblo para entregar la patria", Revista Crisis.

[7] Frente a estas graves implicancias en junio presentamos una denuncia penal por abuso de autoridad contra los titulares de la SIDE responsables del Plan y la directiva secreta asociada, por violación de los artículos 4 y 248 del Código Penal. La causa sigue en instrucción: el trámite no está teniendo la celeridad que correspondería frente a una denuncia de esta gravedad. Para más información ver CELS (19/06/2025), "Denunciamos a la SIDE por habilitar tareas de inteligencia ilegal".

políticos, actores gremiales, organizaciones sociales, referentes territoriales, activistas o cualquier persona que se exprese de manera disidente. Según el Plan, una parte sustancial de las tareas de inteligencia, que son esencialmente secretas, estaría volcada a vigilar la conversación pública.

- Las hipótesis de terrorismo, que se amplían. El documento incluye categorías como "ideología exacerbada", "terrorismo anarquista", "extremismo religioso" o "separatismo indígena" (referido en particular al pueblo mapuche, acusado sin fundamento de poner en riesgo la unidad nacional). Estas nociones no sólo son doctrinariamente inconsistentes, sino que pueden funcionar como habilitadores de vigilancia o inteligencia sobre comunidades religiosas, pueblos originarios o espacios políticos y culturales diversos.

- La promoción de "potenciales impactos negativos en el desarrollo del sistema de Defensa Nacional" o al "interés nacional" (Objetivo Particular 6), que incluye, por ejemplo, al activismo ambientalista y pueblos indígenas. Quienes promuevan acciones para evitar estas consecuencias de la matriz productiva extractivista son considerados actores "adversos al interés nacional".

IMPLICANCIAS

El PIN incorpora prácticas prohibidas por la propia ley de inteligencia, que resultan muy preocupantes para el ejercicio de derechos. En detalle:

1. Promueve la vigilancia sistemática de la disidencia:

- Permite espiar periodistas, organizaciones políticas y activistas: ordena el monitoreo sistemático de la conversación pública (medios, redes sociales, plataformas y espacios digitales abiertos) bajo criterios extremadamente vagos. Esto es contrario al art. 4.2 de la ley 25.520, que establece motivos prohibidos para realizar inteligencia, como por razones políticas o de pertenencia institucional, y al art. 4.3, que prohíbe la influencia de los organismos de inteligencia en los asuntos públicos del país. En este sentido, la realización de tareas de inteligencia prohibidas está penado con entre 3 y 10 años de prisión (art. 43 de la misma ley).

- Afecta al derecho a la privacidad y a la presunción de inocencia -todos podemos ser vigilados- pero también disuade el ejercicio de otros derechos (libertad de expresión, protesta, asociación).

2. Criminaliza la protesta y la defensa del ambiente, en función de las amenazas que establece y la vigilancia que ordena sobre estas actividades.

3. Pone el aparato de inteligencia al servicio de funciones de propaganda expresamente prohibidas por ley, como identificar audiencias, clasificar aliados y adversarios y evaluar el impacto de la comunicación oficial. Este esquema reedita las lógicas de manipulación y espionaje político propias de los "troll centers" y milicias digitales, ahora con financiamiento estatal y un marco legal opaco.

4. Habilita la persecución política interna al ampliar arbitrariamente el concepto de "terrorismo" y fusionar inteligencia interna y militar. Diluye las fronteras entre defensa y seguridad interior (por ejemplo con las hipótesis de terrorismo por "separatismo indígena").

5. Establece el seguimiento de instancias internacionales –sistemas de protección de derechos, cooperación internacional pública y privada–, por ejemplo aquellos mecanismos que intervengan frente a los conflictos socioambientales.

6. Subordina los lineamientos de inteligencia nacional a las agendas de política exterior de Estados Unidos e Israel.

Un ejemplo claro de esta orientación del PIN es **el informe elaborado por la Agencia de Seguridad Nacional (ASN), organismo de la SIDE, que trascendió en los medios de comunicación en agosto de este año[8],** que da cuenta de tareas de inteligencia orientadas a dirigentes políticos opositores (no oficialistas), candidatos/as, agrupaciones sindicales y grupos sociales que se manifiestan contra las medidas del Gobierno Nacional. El documento está fechado justo en el día previo al cierre de alianzas electorales que competirían en los siguientes comicios de la provincia de Buenos Aires. Se trata de reportes minuciosos sobre reuniones y movimientos de estos actores, sin siquiera presentar alguna hipótesis que pueda implicar un riesgo para la seguridad nacional o el orden público. Según la prensa, allí se "precisó cuáles serían los horarios, recorridas y lugares específicos de concentración de cada una, sin que el informe consignara si implicaban amenazas a la seguridad de los argentinos o del Estado nacional. Tampoco exponía una orden judicial que justificara esa vigilancia"[9].

III. FUERZAS DE SEGURIDAD: AMPLIACIÓN DE FACULTADES DE INTELIGENCIA

UNA APROXIMACIÓN A LA INTELIGENCIA CRIMINAL

El Sistema de Inteligencia Nacional (SIN), creado y regulado por la Ley de Inteligencia 25.520, es el conjunto de organismos estatales habilitados para producir inteligencia en Argentina.

La SIDE es el órgano superior y rector (coordina el sistema, elabora el Plan de Inteligencia Nacional, administra los fondos y dirige el ciclo de inteligencia estratégica, por ejemplo), con sus cuatro organismos desconcentrados, creados por DNU 614/2024: el Servicio de Inteligencia Argentino; la Agencia de Seguridad Nacional; la Agencia Federal de Ciberseguridad (AFC); y la División de Asuntos Internos.

[8] Alconada Mon, H. (03/08/2025) "La SIDE redacta informes sobre las actividades políticas de la oposición, sindicatos y grupos de jubilados", La Nación.
[9] Ibídem.

Junto con la SIDE, componen el SIN la Dirección Nacional de Inteligencia Criminal (dentro del Ministerio de Seguridad) y la de Inteligencia Estratégica Militar (Ministerio de Defensa). Esto responde a los distintos tipos de inteligencia que existen[10]:

- **Inteligencia nacional (o estratégica):** conocida de ambas maneras, tiene como objetivo la producción y el análisis de información sobre riesgos y amenazas que pueden afectar la seguridad del Estado en sentido amplio. No investiga delitos concretos. Se orienta a decisiones estratégicas de alto nivel y está centralizada en la SIDE.

- **Inteligencia criminal:** se enfoca en generar información sobre fenómenos delictivos complejos (organizaciones, patrones, dinámicas), de manera preventiva y como apoyo a políticas de seguridad, por lo que se diferencia de las tareas de investigación judicial. Está a cargo de la Dirección Nacional de Inteligencia Criminal.

- **Inteligencia estratégica militar:** procura evaluar capacidades, escenarios y amenazas provenientes del ámbito externo para la defensa nacional, por lo que no puede intervenir en seguridad interior. Está a cargo de la Dirección Nacional de Inteligencia Estratégica Militar.

A la vez, es importante distinguirlas de la *investigación* criminal, que forma parte del proceso penal y busca reconstruir hechos delictivos concretos, con controles judiciales y reglas probatorias. Debe mantenerse separada de cualquier actividad de inteligencia.

Toda actividad de inteligencia debe regirse por la ley 25.520, y sus respectivas reglamentaciones deben adecuarse a ella. En este marco, todas quedan bajo el control de la Comisión Bicameral Permanente de Fiscalización de los Organismos y Actividades de Inteligencia del Congreso, de acuerdo con las previsiones de la ley y su propio reglamento.

LA AMPLIACIÓN DE LAS FACULTADES DE INTELIGENCIA DE LAS POLICÍAS Y FUERZAS DE SEGURIDAD FEDERALES

Entre junio y julio de 2025, el Poder Ejecutivo dictó cinco decretos que reformaron las estructuras orgánicas de policía federal y de las fuerzas de seguridad federales y sus competencias sobre inteligencia criminal.

En particular, se emitieron los siguientes decretos: nº 383/25, modificatorio de la Policía Federal Argentina (PFA); nº 454/25, modificatorio de la Gendarmería Nacional (GNA); nº 455/25, modificatorio del Servicio Penitenciario Federal (SPF); nº 456/25, modificatorio de la Policía de Seguridad Aeroportuaria (PSA); y nº 457/25, modificatorio de la Prefectura Naval Argentina (PNA).

[10] ICCSI (2021), "Acerca de la inteligencia criminal en Argentina. Apuntes para su discusión."

Con el argumento de modernizar la legislación ante el avance de nuevas tecnologías, el Ejecutivo modificó aspectos que se encontraban contemplados en la Ley de Inteligencia Nacional y amplió campos de actuación operativos de las fuerzas de seguridad, reestructurando sus misiones y funciones. Más allá de las particularidades de cada decreto y cómo afectan a cada una de las fuerzas, es posible mencionar una serie de cuestiones problemáticas transversales:

1. **Ampliación de funciones por decreto**

Las nuevas atribuciones no se otorgan por ley. No se trata de un exceso de formalismo por el hecho que modifiquen el espíritu de una ley de mayor jerarquía, como la Ley de Seguridad Interior, sino que introduce reformas estructurales que amplían facultades y ameritan el debate legislativo. La justificación formal para eludir el tratamiento legislativo fue la "emergencia pública, económica, financiera y energética" a la que alude la Ley N° 27.742 ("Bases y Puntos de Partida para la Libertad de los Argentinos"), citada en cada uno de los decretos mencionados. Sin embargo los decretos no explicitan cuál es la relación entre las modificaciones propuestas y la "emergencia" que le delegó facultades extraordinarias al poder ejecutivo, es decir, no existe una fundamentación sobre cómo estos cambios en las fuerzas de seguridad podrían contribuir con la emergencia aludida.

2. **Competencias y definiciones ambiguas**

Los decretos utilizan una terminología amplia y vaga para definir las nuevas amenazas que se pretenden abordar, a la vez que eluden definiciones específicas sobre cursos de acción, permitiendo interpretaciones extensivas, que exceden el mandato legal que tienen estas fuerzas de seguridad. Conceptos como "criminalidad organizada", "actos delictivos complejos cometidos por organizaciones criminales", "riesgos de seguridad interior" y atribuciones sobre "delitos de su competencia" no tienen definiciones claras y permiten interpretaciones discrecionales sobre lo que la normativa habilita.

Por otra parte, la normativa parece desconocer el funcionamiento del sistema y las diferencias en las estructuras de inteligencia dentro de las propias fuerzas de seguridad. La PSA, por ejemplo, cuenta con áreas de inteligencia criminal que reportan a una superior, es decir, en el diseño orgánico existe una instancia de coordinación en materia de inteligencia. En el caso de la PFA, PNA y GNA, por su parte, la estructura se sostiene sobre distintos estados mayores con muchas superintendencias, y la cuestión de la inteligencia es asignada en reparticiones específicas en cada una de las fuerzas, pero no se encuentra centralizada. Es decir que cada superintendencia tiene un departamento de inteligencia propio que no reporta a uno superior.

En todo caso, el problema central de la competencia radica en la disociación con las leyes de inteligencia y de seguridad interior, donde se erige a la Dirección Nacional de Inteligencia Criminal (DINIC) como órgano superior de coordinación del sistema. Las definiciones ambiguas y la dificultad en el establecimiento de competencias y funciones entre las fuerzas, habilita su actuación por fuera de su ámbito legal, generando incompatibilidades entre las fuerzas que integran el sistema de inteligencia. El ejemplo más notorio de esta situación está presentado en el artículo 6.2 del decreto 383/25, que

habilita a la PFA a realizar actividades de inteligencia prohibidas por la ley de inteligencia, y que están reservadas para la SIDE. El mismo establece que la PFA tiene facultades para "efectuar tareas de inteligencia criminal, mediante la obtención, reunión, sistematización y análisis de la información referida a actividades criminales o riesgos que afecten la seguridad interior". En el supuesto afán de modernizar el sistema de inteligencia, una nueva ingeniería institucional debe responder a criterios de eficacia, y no solapar tareas que las fuerzas de seguridad tienen prohibido realizar por ley, ampliando su ámbito de actuación ante "riesgos que afecten la seguridad interior". Más aún, estas tareas de inteligencia criminal deberían estar coordinadas (y controladas) por el Ministerio Público Fiscal.

3. Problemas en la técnica legislativa y lagunas

A la cuestión de las definiciones ambiguas se suma un problema fundamental relacionado con la definición del concepto de "inteligencia" a secas y, en particular, con el uso indistinto de actividades disímiles como son "inteligencia criminal" e "investigación criminal". Los decretos no cuentan con un glosario, ni parece haber una estandarización del lenguaje técnico empleado, de manera que no resulta claro qué tipo de actividad podría realizarse por fuera de los límites de la investigación judicial. La falta de delimitación conceptual tiene como consecuencia la habilitación "legal" de tareas de inteligencia que podrían realizarse mediante intervenciones judiciales. En otros pasajes, la opacidad de la redacción amerita aclaraciones que el texto legal no provee, o bien, con especificaciones incompletas. A modo de ejemplo, el inciso 5 del artículo 6° del decreto 383/25 establece la posibilidad para la PFA de tener acceso a "información y bases de datos públicas con el fin de llevar adelante "de manera justificada" tareas de investigación o de inteligencia criminal. La pregunta aquí es cómo y quién establece esa justificación, más allá que luego el decreto aclara "que se deberá cumplir con la normativa de protección de datos personales", no lo hace con respecto a la ley de inteligencia ni a la de seguridad interior.

4. Ausencia de controles, límites y transparencia para la recolección y uso de información

Siguiendo con la cuestión de las bases de datos del párrafo anterior, los decretos otorgan facultades amplias para el acceso a base de datos públicas, y la solicitud de acceso a bases privadas, con fines de inteligencia criminal. En este sentido, faculta a la PFA y la PSA a organizar bases de datos, archivos, sistemas de información y solicitar acceso a bases privadas, como también al SPF, con justificación en tareas de investigación o inteligencia criminal. Es pertinente aclarar que SPF no está capacitado para realizar tareas de investigación criminal, función que se encuentra muy alejada de la custodia de personas privadas de su libertad, más aún si para ello requiere la consulta de bases de datos, lo que permitiría suponer que es una hipótesis de delito fuera de su ámbito de competencia. Asimismo, vale mencionar como antecedente su participación en las tareas de inteligencia ilegal sobre funcionarios, empresarios y sindicalistas detenidos en Ezeiza entre 2017 y 2019

a través del área de Análisis de la Información, conocida como la dirección de Inteligencia del SPF o el "Área 50"[11].

Sobre este punto, resulta importante destacar la falta de controles internos y la ausencia de mecanismos de transparencia. Las normas no especifican la trazabilidad de la obtención de información, ni sobre el registro obligatorio de bases de datos, así como tampoco mencionan mecanismos de auditoría sobre las tareas de inteligencia criminal. En términos operativos, tampoco establece la obligación de desarrollar protocolos de actuación que regulen cómo se accede, utiliza, almacena o comparte información de inteligencia, incluso con organismos internacionales o entre países. Y mucho menos habilita criterios de acceso a la información compatibles con la ley de acceso vigente.

5. Ciberpatrullaje

Se autoriza la vigilancia de espacios digitales públicos sin orden judicial previa ni controles judiciales obligatorios, y sin la exigencia de una hipótesis delimitada previamente. Adicionalmente, no se definen concretamente cuáles serán herramientas, alcances, parámetros de búsqueda o tiempos de almacenamiento de la información recolectada. En los casos de PSA y GNA la vigilancia digital parece justificarse como una tarea de prevención del delito sobre campos de actuación existentes, aunque vagamente definidos (como "acciones criminales" o "terroristas" o "en contra de derechos y garantías de los ciudadanos"). En cambio, la modificación reglamentaria sobre la estructura orgánica del SPF implica una modificación, de hecho, sobre funciones preventivas que esta fuerza nunca se encargó de realizar. De nuevo aquí, bajo la excusa de modernizar las tareas de las fuerzas de seguridad, se le incorpora a través de un decreto, una función que el SPF no tenía, con relación a la realización de tareas preventivas o de investigación, por fuera del contexto de sus establecimientos de detención.

Cualquiera sea el caso, debe considerarse que ninguno de los decretos establece con claridad cómo deben ser los procesos de trabajo de este ciberpatrullaje, es decir, la cuestión operativa. Una reforma que pretenda modernizar las fuerzas de seguridad para adaptarla a los desafíos del presente, debería establecer criterios claros para la elaboración de protocolos específicos de actuación para evitar justamente la autonomía de policías y fuerzas de seguridad "saliendo" a buscar, de manera aislada, conductas posiblemente delictivas en fuentes abiertas, sin ningún tipo de directiva superior o de articulación con el Ministerio Público Fiscal. O también la posibilidad de que las autoridades políticas den órdenes o directivas que impliquen un perfilamiento ilegal o discriminatorio. El diseño reglamentario en este punto da lugar a la ampliación del poder de vigilancia para objetivos que no están necesariamente asociados a fenómenos de criminalidad compleja, sino a delitos de baja preparación y ostensiblemente visibles al ojo policial o bien, hacia objetivos políticos ilegítimos, amparados en la vaguedad de las definiciones conceptuales ya descriptas.

[11] Para más información ver, por ejemplo, Bertoia, L. (10/05/2022), "Espionaje en Ezeiza: la Justicia requirió información sobre el IRIC", Página/12.

6. El contexto de las reformas

En este punto en particular resulta necesario vincular nuevamente lo que los decretos dicen y el contexto en el que emergen. La ampliación de facultades policiales, la opacidad de la terminología empleada y la ausencia de los controles necesarios, no puede leerse de manera aislada sino en el marco de una utilización del poder policial en particular, y punitivo en general, por parte del poder ejecutivo para controlar el clima político y desalentar fuerzas políticas, sociales, sindicales, etc, opositoras. Por esta razón, una lectura de estas reformas reglamentarias sobre las fuerzas de seguridad junto al Plan de Inteligencia ya mencionado, permite proyectar un panorama aún más opaco, cuyo foco parece orientarse hacia la supresión de disidencias y activismo en derechos. Vale recordar, la ampliación de categorías de "amenazas" del PIN mencionadas anteriormente, como "ideología exacerbada", "terrorismo anarquista", "extremismo religioso" o "separatismo indígena". En este contexto, además de la vigilancia y el control, estas reformas podrían contribuir a la represión de determinados actores políticos y de la sociedad civil que el gobierno califica como antagónicos, a partir de la creación de escenarios artificiales de conflicto.

IV. CIBERSEGURIDAD: CENTRALIZACIÓN EN LA SIDE

EL DECRETO 274/25

En abril del 2025 el Poder Ejecutivo dictó el Decreto 274/25[12] modificando algunas cuestiones sustantivas del funcionamiento de la Unidad de Información Financiera (UIF) y las misiones que tiene atribuidas, así como sobre la organización del Estado en torno a la prevención del lavado.

Según el propio texto, la necesidad de estas modificaciones responde a la "eficientización" del Estado, la búsqueda de unificar procesos que puedan implicar facultades duplicadas y el cumplimiento de las recomendaciones periódicas emitidas por el GAFI para Argentina, en el marco de la lucha contra el narcotráfico y lavado de activos. Sin embargo, sin explicar cuál es la vinculación con este objetivo, en el mismo decreto se desplazó toda la agenda de ciberseguridad del Estado -hasta ahora dispersa en distintas agencias de la Administración Pública- a la órbita de la Secretaría de Inteligencia del Estado (SIDE).

TRES CAMBIOS PROBLEMÁTICOS

En detalle, el decreto modifica tres aspectos fundamentales en cuanto a la organización del Estado y sus facultades en esta materia:

[12] Se trata de un decreto delegado en los términos del art. 76 de la Constitución Nacional. Tal como se cita en los considerandos del propio decreto, éste es posible (en lugar de una ley formal del Congreso) gracias a las facultades delegadas que le otorgó la "Ley Bases". Sin embargo, habilita al PEN a "modificar o eliminar" competencias, mientras que en este caso se están aumentando.

1. Eliminación de la facultad de querellar de la UIF (art. 10)

Bajo el pretexto de la "optimización" de recursos y reducción de estructuras duplicadas, deja la actividad de querella exclusivamente en cabeza del Ministerio Público Fiscal. Va a contramano de las recomendaciones del GAFI, que indicaba el fortalecimiento de las judiciales del organismo como una acción prioritaria para la transparencia institucional[13].

2. Centralización de la política de ciberseguridad en la SIDE

A partir de este nuevo decreto (art. 7), toda la política de ciberseguridad del Estado queda bajo el ala de la Agencia Federal de Ciberseguridad (AFC).

Esta agencia fue creada dentro de la SIDE por DNU 614 y su reglamentario 615/24, modificatorios de la Ley de Inteligencia. Le dieron competencias generales sobre “la ciberdelincuencia, las infraestructuras críticas y objetivos de valor estratégico tecnológicos y de la información" (DNU 614, art. 17), entre ellas recolectar, adquirir y procesar "toda información relevante para el Sistema de Inteligencia Nacional", incluyendo la posibilidad de interceptar comunicaciones, sin detallar a qué se refiere, de qué forma, bajo qué parámetros, con qué controles, qué hace con la información obtenida, por cuánto tiempo la almacena ni aclarar expresamente si es necesaria autorización judicial (que la ley en su formulación anterior sí preveía).

El decreto 274 le da a la AFC competencias sobre otras cuestiones relativas a ciberseguridad que, hasta ahora, estaban dispersas dentro de la Administración Pública. A modo ilustrativo, incluyen: la creación de un nuevo Comité de Ciberseguridad (que hasta ahora estaba en la órbita de Jefatura de Gabinete de Ministros); la dirección del Centro Nacional de Respuesta a Incidentes Informáticos (CERT.AR); la elaboración de planes y programas destinados a fortalecer la ciberseguridad, entender en el monitoreo y respuesta de los incidentes informáticos del Sector Público Nacional y de las infraestructuras críticas nacional; colaborar en la promoción de planes, programas y proyectos de innovación tecnológica y científica en materia de ciberseguridad, etc.

Esto es problemático en varios sentidos. En términos generales, la política de ciberseguridad debería estar separada de la inteligencia, y contar con estándares mínimos de transparencia, supervisión técnica y auditoría externa, que este Decreto no contempla. Las competencias listadas son claros ejemplos del gran abanico de responsabilidades que pasa a tener un organismo de la SIDE en términos de política pública de ciberseguridad. Así, el decreto centraliza funciones críticas y potencialmente muy intrusivas en un organismo opaco y sin controles. No explica de manera directa por qué: parece más responder a una decisión por conveniencia política que técnicamente fundada.

La experiencia comparada indica que ubicar ciberseguridad en el ámbito de la inteligencia resulta ineficaz: confunde objetivos, reduce la profesionalización, coloca toda actividad bajo un manto de secreto, e impide garantizar buena coordinación con otras

[13] Acción prioritaria “d” de la evaluación del GAFI a la República Argentina, diciembre 2024.

áreas que deben proteger sus infraestructuras. Si bien es necesario que Argentina cuente con una agencia que proteja la infraestructura crítica, definitivamente no resulta recomendable que se encuentre bajo dependencia de la SIDE, organismo caracterizado por el secreto, regido por la Ley de Inteligencia y cuyos cuadros técnicos no se especializan en este campo[14]. Si realmente se busca tornarla estratégica, requiere ser pensada y discutida bajo una lógica distinta a la de la prevención de amenazas en los términos que lo hace la SIDE.

A la vez, el decreto vuelve a crear dentro de la AFC el Comité de Ciberseguridad y traspasa a su órbita el CERT: ¿quién puede pensar que incentiva las denuncias de incidentes o vulnerabilidades informáticas que el organismo a cargo de recepcionarlas e investigarlas sea la Secretaría de Inteligencia? O, por ejemplo, ¿acaso es posible considerar que este sea el organismo idóneo para hacer capacitaciones de buenas prácticas en la materia para el resto de la Administración Pública? En el camino quedó la Dirección Nacional de Ciberseguridad, dependiente de Jefatura de Gabinete, que si bien el decreto no disuelve tampoco incorpora al nuevo esquema; al día de hoy está casi vacía de funciones y sin director designado.

3. Ampliación de supuestos para tratar e intercambiar información: mayor vigilancia.

Si bien el tratamiento y protección de datos personales excede el objetivo de este documento, es importante destacar que este decreto modifica de manera problemática el régimen respecto al tratamiento de información sensible entre la UIF y organismos tanto nacionales -entre ellos de inteligencia y FFSS- como extranjeros, en dos sentidos:

a. Elimina la obligación de control judicial sobre la información que trata la UIF, sin importar su tenor, contenido y/o de quién provenga (art. 1.1 del decreto). Si esto lo analizamos a los ojos del DNU 614 y su reglamentario 615, veremos que la AFC ya tenía una serie de competencias ambiguas y amplias que le permitían una autonomía importante con respecto al Poder Judicial, a quien ya no debe pedir autorización ni informar en los mismos casos que antes de la reforma.

b. Amplía el universo de sujetos con los que puede intercambiarla sin prever nuevas limitaciones, salvaguardas ni instancias de control (cfr. arts. 1.2 y 2 del decreto), y amplía el intercambio de información a los propios sujetos obligados, es decir aquellos que tienen el deber de informar a la UIF (art. 3). Esto representa una autorización explícita a intercambiar información con organismos de inteligencias, fuerzas de seguridad, fuerzas armadas, migraciones, entre otras, sin necesidad de justificar qué datos se recabarán, para qué fines y con qué parámetros de eliminación luego. Choca con principios rectores de la protección de datos personales, como el de consentimiento, *minimización de los datos* o el de *finalidad*, pero también con la prohibición de ciertas causales para realizar inteligencia (art. 4 de la ley 25.520). Además, el decreto extiende el secreto sobre

[14] Para más información ver ICCSI (2024), "Comentarios sobre la reforma del sistema de inteligencia".

este intercambio: al ser confidencial, ¿cómo se asegurará la protección de datos personales? ¿Quién será la autoridad de control sobre el uso de esos datos?

Si bien puede ser una facultad necesaria en algunos casos (y de hecho la ley original que crea la UIF ya preveía facultades en este sentido), no debería hacerse forma tan vaga y sin garantías en términos de derechos. Haciendo una lectura integral de las modificaciones de este artículo, la UIF podrá disponer de la misma información que la SIDE y los organismos que componen el Sistema Nacional de Inteligencia, en secreto y sin intervención judicial. Mucho menos control ciudadano.

V. INTELIGENCIA: EXPANSIÓN PRESUPUESTARIA Y FONDOS RESERVADOS

En un contexto de "motosierra" y ajuste general, el presupuesto de seguridad e inteligencia sigue aumentando. Tanto en la proyección del presupuesto para el año próximo como a través de distintas partidas que se fueron asignando por decreto en los últimos meses, se advierte la decisión política de financiar estas agendas sobre otras. Hay que tener en cuenta, además, que la SIDE y la actividad de inteligencia pueden recibir partidas secretas, por lo que tampoco es posible saber con exactitud cuántos recursos reciben ni en qué se gastan.

Esto funciona muchas veces como incentivo para incorporar en la órbita de la SIDE actividades de inteligencia criminal en las que intervienen también las fuerzas de seguridad federales. Es el caso, por ejemplo, del flamante Centro Nacional Antiterrorismo, creado en octubre de 2025 mediante el decreto 717/2025. Se trata de una decisión del Poder Ejecutivo, que crea un nuevo organismo con funciones compartidas con el Ministerio de Seguridad. Nuevamente bajo la retórica de la "lucha contra el terrorismo" otorga competencias vagas y amplias, y asigna recursos para su ejecución. En este sentido, sujeta su financiamiento a la SIDE, habilitando así el financiamiento discrecional a través de partidas reservadas, sin trazabilidad ni rendición de cuentas.

SOBRE LOS FONDOS RESERVADOS

Los "fondos reservados" están previstos para el Sistema de Inteligencia en la ley 25.520 pero, como se trata de presupuesto secreto sobre el que no hay obligación de registro, se gasta discrecionalmente y su único control es *ex post* por parte de la Comisión Bicameral, debería ser un monto mínimo indispensable para el funcionamiento de las actividades que realmente requieren ser financiadas en secreto y no la regla general. De hecho, el decreto 331/23, anexo II (que sigue vigente según el art. 8 del decreto 615/24, reglamentario del DNU 614), exige que sean sólo para gastos excepcionales cuando su publicidad pueda afectar "el normal desarrollo de las actividades de inteligencia, poniendo en riesgo la defensa nacional o la seguridad interior", y prevé que el resto de las operaciones deben regirse por el presupuesto ordinario y controlarse según la ley de administración financiera 24.156.

En otras palabras, el financiamiento a través de fondos reservados debería suceder únicamente de manera excepcional, cuestión que en esta gestión no se respeta. De hecho, en 2024 el Congreso rechazó el DNU 656 que ampliaba de manera desproporcionada el monto que iba a recibir la SIDE bajo este concepto.

PRESUPUESTO 2025/26

Según información disponible[15], el presupuesto total consolidado de la SIDE para 2025 fue de más de $80.000 millones, y a mediados de año ya había ejecutado cerca del 46% del total. Esta cifra representa casi el doble de lo gastado por el organismo durante 2024.

Los aumentos se realizaron a través de readecuaciones presupuestarias dispuestas por el Poder Ejecutivo unilateralmente, a través de (DNU) y Decisiones Administrativas -es decir, eludiendo el debate parlamentario-, y los fondos reservados representaron un porcentaje alto.

Por ejemplo, mediante el DNU 186/2025 (marzo) se dispuso una ampliación total de $7.300 millones, con $1.625 millones destinados a gastos reservados. Por su parte, mediante la Decisión Administrativa 10/2025 (mayo) se redirigieron $25.250 millones a la SIDE, de los cuales más de $8.000 millones se dispusieron como gastos reservados. Así, el total de gastos reservados asignados se estima en, por lo menos, $25.465 millones en lo que va del año. Finalmente, en la misma línea, el 2 de diciembre el Ejecutivo asignó $26.117.900.000 extra a la SIDE, a través del Decreto 849/2025[16].

Los aumentos suceden sin mayores justificaciones, a través de retóricas vacías. Dentro de la misma lógica opaca que caracteriza a las actividades de inteligencia y, en especial, la asignación de fondos reservados, pretextos como “la lucha contra el terrorismo” funcionan como paraguas amplio para evitar la transparencia sobre grandes asignaciones de recursos, que debería ser especialmente estricta en un contexto de ajuste fiscal extremo.

VI. CONCLUSIONES

Las reformas impulsadas durante 2024 y 2025 configuran una transformación profunda y preocupante del sistema de inteligencia argentino. Lejos de modernizar las instituciones, estas medidas consolidan un aparato de vigilancia estatal que puede ser orientado al control político y social, sin desarrollo de mecanismos fuertes de control, en clara violación de la Ley de Inteligencia Nacional y de estándares internacionales de derechos humanos.

[15] Barón, P. (25/06/2025), “La SIDE esquiva la motosierra de Milei, duplica su presupuesto y lo lleva a más de $ 80.000 millones”, Clarín; Rosemberg, J. (05/05/2025), “El Gobierno decretó otro aumento en los fondos para la SIDE y una ampliación de gastos reservados”, La Nación.
[16] Davanna, C. (02/12/2025). “El Gobierno amplió fondos a la SIDE: el porcentaje que se destina a sueldos y los gastos más ‘llamativos’”, La Nación.

Estas reformas tienen un hilo conductor: expansión del poder de vigilancia, centralización de funciones en organismos de inteligencia, debilitamiento de controles democráticos y aumento del secreto. Este proceso no responde a necesidades técnicas sino a la decisión política de subordinar el sistema de inteligencia a los objetivos políticos del Poder Ejecutivo y al control de la disidencia.

El Plan de Inteligencia Nacional es el elemento central. Las categorías amplias y vagas que emplea funcionan como habilitadores de vigilancia sobre cualquier expresión disidente, violando frontalmente la ley 25.520 y reproduciendo lógicas de inteligencia ilegal incompatibles con la democracia.

La ampliación de facultades de inteligencia a las fuerzas de seguridad federales, realizada mediante decretos sin debate parlamentario, agrava este panorama. La ambigüedad de las competencias otorgadas, la ausencia de protocolos claros y la habilitación de prácticas sin orden judicial, como el ciberpatrullaje, habilitan la vigilancia masiva y discrecional. En el mismo sentido, la centralización de la ciberseguridad en la SIDE y la modificación del régimen de intercambio de información entre estos organismos amplían exponencialmente esas posibilidades, permitiendo acceso a información sensible sin controles judiciales adecuados.

A la vez, el aumento presupuestario destinado a inteligencia en contexto de ajuste fiscal severo, especialmente de fondos reservados, evidencian la prioridad política asignada a estas agendas. Estas reformas se enmarcan en un contexto de restricción del espacio cívico y criminalización de la protesta. Impactan directamente en derechos fundamentales: libertad de expresión, protesta social, participación política, privacidad, igualdad y presunción de inocencia.

Frente a este escenario, resulta imprescindible la acción coordinada de múltiples actores. Sin embargo, el Congreso no ejerce sus funciones de control, ni el Poder Judicial investiga las denuncias de inteligencia ilegal.

Las reformas de 2024 y 2025 nos sitúan en un camino peligroso que es urgente revertir para sostener los límites legales y acuerdos democráticos. Las noticias de los últimos tiempos[17] solo muestran organismos de inteligencia cruzados por las internas políticas, con cada vez más fondos, competencias y discrecionalidad pero desprofesionalizado y con falencias evidentes para cumplir su misión legal de defender el interés nacional.

[17] Al momento de cierre de este documento se hizo pública la noticia de una nueva Política de Inteligencia Nacional, en los términos del Título IV de la ley 25.520. Si bien excede el período de análisis abordado aquí, en una primera lectura advertimos la continuidad de muchos de los riesgos que habíamos identificado en función del PIN. En este sentido, resulta relevante avanzar en su análisis y monitoreo permanente.

SOBRE ICCSI

La Iniciativa Ciudadana para el Control del Sistema de Inteligencia (ICCSI) es un espacio destinado al seguimiento, impulso y promoción del funcionamiento efectivo de los mecanismos de control sobre el sistema de inteligencia de nuestro país.

Esta iniciativa representa una respuesta de la sociedad civil a la necesidad de construir un espacio comprometido con la democratización de los organismos de inteligencia, en particular, a través del impulso de políticas destinadas a mejorar los controles internos y externos del sistema, cuya efectividad es de vital importancia para el buen funcionamiento del Estado de derecho y las instituciones democráticas.

www.iccsi.org.ar

INTEGRANTES

ILSED
Instituto Latinoamericano de Seguridad y Democracia

Vía Libre 25 años

CELS
CENTRO DE ESTUDIOS LEGALES Y SOCIALES

ICCSI

INICIATIVA CIUDADANA PARA
EL CONTROL DEL SISTEMA
DE INTELIGENCIA