ANÁLISIS DECRETO 274/25

Datos personales, fines secretos: nuevas habilitaciones para la SIDE y la UIF

Vía Libre

Datos personales, fines secretos: nuevas habilitaciones para la SIDE y la UIF. Análisis del decreto 247/25 desde una perspectiva de privacidad.

Mayo 2025

Autoría: Margarita Trovato
Dirección del proyecto: Beatriz Busaniche

Realizado con el apoyo de la Fundación Heinrich Böll.

Vía Libre

HEINRICH BÖLL STIFTUNG
BUENOS AIRES
Argentina | Uruguay | Paraguay

Introducción

La protección de los datos personales es hoy uno de los principales desafíos que enfrentan las democracias contemporáneas, en un contexto marcado por el crecimiento exponencial de la capacidad estatal y privada para recolectar, almacenar, procesar e intercambiar información sensible sobre la vida de las personas. En este escenario, el rol del Estado es doble: por un lado, debe proteger activamente los derechos fundamentales frente a eventuales abusos en el tratamiento de datos; por el otro, en tanto actor que también procesa y comparte información, tiene la obligación de hacerlo conforme a estándares rigurosos de legalidad, transparencia, necesidad y proporcionalidad.

El Decreto 274, dictado en abril de 2025 por el Poder Ejecutivo con el objetivo de optimizar la política de prevención de lavado de activos y la financiación del terrorismo, siguiendo recomendaciones del Grupo de Acción Financiera Internacional (GAFI), introduce modificaciones sustantivas en el funcionamiento de la Unidad de Información Financiera (UIF) y en el régimen de intercambio de información con otros organismos del Estado y sujetos obligados en general. Al mismo tiempo, sin justificación, reubica toda la política de ciberseguridad en el seno de la Secretaría de Inteligencia del Estado (SIDE).

Todas estas modificaciones importan una expansión significativa de las capacidades estatales, fundamentalmente de su posibilidad de injerencia en la privacidad de la ciudadanía. Ninguna fue incorporada desde una perspectiva de derechos, respetuosa de los estándares internacionales que deben guiar y limitar la actuación del Estado, especialmente cuando se trata de facultades tan intrusivas.

En este documento analizamos, en términos generales, el decreto y nos proponemos analizar con mayor profundidad lo referido al intercambio y cesión de datos personales, contrastándolo con el marco normativo vigente en materia de protección de datos (específicamente la Ley Nacional de Protección de Datos Personales nro. 25.326) y con los principios generales y estándares internacionales que deben regir. Lo hacemos, además, con la preocupación de la otra gran modificación que este decreto introduce: toda la cuestión relativa a la ciberseguridad en manos de una agencia de inteligencia.

Es importante resaltar que esta norma se inscribe en un contexto de lagunas normativas y falta de controles en el tratamiento de datos personales en general, lo cual incrementa su riesgo. Sobre este tema publicamos un informe desde la Fundación Vía Libre en 2024, “Gestión de datos personales por parte del Estado”, cuya lectura en extenso recomendamos para complementar el presente análisis. Allí realizamos un diagnóstico detallado sobre las debilidades del marco normativo y formulamos propuestas para una reforma estructural del régimen de protección de datos con perspectiva de derechos.

Con el mismo enfoque nos ocupamos en este documento de examinar las modificaciones introducidas por el decreto y de evaluar sus implicancias. Nos preocupa el aumento de facultades con el grado de discrecionalidad, opacidad y falta de controles democráticos que este decreto importa. Son necesarias reformas normativas con relación al marco de protección de datos personales, así como sobre la gobernanza de infraestructuras críticas e implementación de mejores medidas de ciberseguridad, pero no en el sentido de este decreto.

A continuación presentamos nuestras observaciones.

El Estado recolecta y trata permanentemente datos de los ciudadanos para el ejercicio de sus funciones. Sin embargo, la información recolectada es cada vez más sensible y usada con distintas finalidades, que se amplían constantemente y son, en muchos casos, intrusivas.

El informe aborda, desde una perspectiva histórica y de derechos humanos, la recolección y gestión de datos personales por parte del Estado en Argentina para identificar sus usos a lo largo del tiempo, estudiar el marco regulatorio y proponer las reformas necesarias para proteger el derecho a la privacidad.

Disponible acá.

DERECHO A LA PRIVACIDAD. PRINCIPIOS BÁSICOS

Como punto de partida, es importante recordar cuáles son los principios que rigen -o deberían regir- la recolección y tratamiento de información personal, conforme la legislación nacional y los estándares internacionales. Nos referimos, principalmente, a la ley 25.326 que, a pesar de tener ya más de 20 años y haber quedado desactualizada con respecto a los usos y procesos actuales, sigue siendo la norma nacional que rige la materia. En el plano internacional, tanto la jurisprudencia como la normativa de la Unión Europea (fundamentalmente el Reglamento General de Protección de Datos - RGPD) suele ser el paradigma para impulsar mejores estándares y ponderar la protección adecuada de derechos en el contexto de reformas como la presente.

En una mirada integral, los principios que deben regir la regulación de datos personales para asegurar un tratamiento ético, seguro y respetuoso de los derechos a la privacidad, intimidad y autodeterminación informacional incluyen:

- **Legalidad:** todo tratamiento de datos debe tener una base jurídica válida y no puede realizarse de manera arbitraria.
- **Consentimiento libre, expreso e informado:** como principio general, la recopilación y tratamiento de datos debe contar con la aprobación expresa del titular, salvo en casos muy excepcionales que deben interpretarse de forma restrictiva y procurando un equilibrio entre el interés público que fundamenta el tratamiento de los datos y la protección de los derechos individuales. Veremos más adelante que en la legislación argentina las excepciones son vagas y por lo tanto permiten ser aplicadas en detrimento de la protección de derechos
- **Finalidad:** los datos deben ser utilizados únicamente para las finalidades específicas para las cuales se recopilaron, y estas finalidades deben estar claramente informadas a los titulares. Si cambiaran o se ampliaran, un nuevo consentimiento deberá ser requerido (Recogido en los arts. 4, 6 y 11 de la ley).
- **Limitación en el uso y conservación:** Como desprendimiento del punto anterior, los datos no deben recopilarse, tratarse ni conservarse por fuera de la finalidad original, lo cual incluye hacerlo sólo por el tiempo necesario (art. 4 de la ley).
- **Minimización de datos:** solo deben recabarse y tratarse los datos estrictamente necesarios para cumplir con la finalidad prevista, limitando el tratamiento a la cantidad mínima indispensable. Este principio no se encuentra previsto de manera taxativa en nuestra ley pero sí en el RGPD, art. 5.
- **Proporcionalidad:** el grado de injerencia en la privacidad debe ser proporcional y pertinente con respecto al objetivo legítimo que se persigue; no se justifica la recolección ni tratamiento que resulte desmedido en relación con el fin declarado.
- **Seguridad y confidencialidad:** el tratamiento de datos debe realizarse con medidas que protejan la confidencialidad, integridad y disponibilidad de la información, minimizando riesgos de filtraciones o accesos no autorizados. Es responsabilidad del Estado implementar medidas técnicas y organizativas adecuadas para esto; responsabilidad que se vuelve particularmente relevante en la medida en que aumenta el volumen de datos tratados.

- **Derechos del titular:** los y las ciudadanas deben tener control sobre sus datos, pudiendo ejercer, de mínima, derechos básicos como acceso, rectificación, cancelación y oposición (conocidos como "ARCO"), y brindar (o no) su consentimiento en caso de cesión o uso distinto a la finalidad original.
- **Independencia y autonomía de las autoridades de aplicación:** las autoridades encargadas de supervisar y hacer cumplir estas normas deben ser independientes e idóneas y contar con recursos y facultades suficientes para garantizar la protección efectiva de los derechos.

Estos principios conforman el marco básico para una protección efectiva de los datos personales y derechos humanos siendo especialmente rigurosos en el contexto de avances tecnológicos y expansión del tratamiento de datos por parte del Estado que rige en estos tiempos[1].

LA CESIÓN DE DATOS PERSONALES

En función de estos principios, vale detenernos en la cuestión de la cesión de datos personales[2].

El art. 11 de la ley 25.326 establece que *"Los datos personales objeto de tratamiento sólo pueden ser cedidos para el cumplimiento de los fines directamente relacionados con el interés legítimo del cedente y del cesionario y con el previo consentimiento del titular de los datos, al que se le debe informar sobre la finalidad de la cesión e identificar al cesionario o los elementos que permitan hacerlo"*. Pero, a la vez, habilita una serie de excepciones al requisito del consentimiento, eje fundamental del tratamiento de datos personales. Por un lado, prevé excepciones en general, por ejemplo, cuando la información tratada no implique una intrusión arbitraria en la esfera personal (nombre, DNI, domicilio, etc.) o cuando provenga de fuentes públicas, entre otras, pero incluye una particularmente problemática: exime del consentimiento aquellos datos que *"Se recaben para el ejercicio de funciones propias de los poderes del Estado o en virtud de una obligación legal"* (art. 5, inc. b). La formulación es tan amplia que puede tornarse sumamente abusiva; puede funcionar como una ventana a usos discrecionales, excesivos y sin justi-

1 Para ampliar información sobre estos principios, los estándares internacionales, el estado actual de la normativa argentina y en qué sentido deberían impulsarse reformas, nos remitimos al documento "Gestión de datos personales por parte del Estado de la Fundación Vía Libre" (2024) antes referido.

2 En este apartado ofrecemos un breve repaso de cómo se encuentra hoy reglamentada la cesión de datos personales, pero nos remitimos al documento nos remitimos al documento "Gestión de datos personales por parte del Estado de la Fundación Vía Libre" (2024) antes referido, donde lo abordamos en profundidad y elaboramos recomendaciones para futuras modificaciones. Especialmente recomendamos en este punto la lectura de los capítulos 2.III y 3.

ficación por parte de los responsables del tratamiento, en este caso el Estado. A modo de ejemplo, podemos pensar que se trata de "obligaciones legales" aquellas impuestas por la Ley de Inteligencia Nacional nº 25.520 en lo concerniente a interceptación de comunicaciones- agencias con las ahora la UIF podrá intercambiar información discrecionalmente, como veremos más adelante.

Por otro lado, el propio art. 11 prevé una excepción específica del consentimiento del titular en el caso de la cesión de datos: cuando se realice *"entre dependencias de los órganos del Estado en forma directa, en la medida del cumplimiento de sus respectivas competencias"*. En otras palabras, un paraguas casi absoluto para el intercambio intra-estatal de información personal sin ninguna restricción. Si bien la doctrina y la jurisprudencia precisaron en alguna medida el alcance de esta norma y recordaron la importancia de la interpretación restrictiva, en los hechos funciona como una habilitación casi total.

La recolección de datos por parte del Estado no sólo es legítima sino también necesaria en ejercicio de sus objetivos básicos, desde su función registral hasta el diseño de políticas públicas en distintas áreas. Lo mismo sucede con su intercambio: tiene sentido suponer que un servicio social ofrecido por el Estado sea más eficiente en tanto se pueda dirigir mejor, por ejemplo. Pero no debería poder hacerlo en cualquier circunstancia ni incondicionalmente. Sin embargo, el límite que prevé la ley a la obtención de datos por parte del Estado y su eventual cesión es ambiguo: si bien las excepciones son contadas y deberían ser interpretadas de forma taxativa, lo cierto es que supuestos como el de la cesión lícita dentro del Estado sin consentimiento cuando se realice en cumplimiento de sus competencias, puede ser interpretado de forma amplia y abusiva. Lo mismo sucede con el concepto de *"fines directamente relacionados con el interés legítimo del cedente y del cesionario"* que, si bien por regla general deben ser complementados con el consentimiento del titular, es poco claro a qué se refiere y puede ser interpretado de maneras invasivas de la privacidad.

Nos preguntamos entonces qué sucede cuando combinamos el principio de finalidad que rige la recopilación y el uso de datos personales que puede hacer el Estado con el principio general del consentimiento, pero también con las excepciones a éste que habilita la ley cuando los datos *"se recaben para el ejercicio de funciones propias de los poderes del Estado o en virtud de una obligación legal"* (art. 5, inc. b), o cuando sean cedidos *"en cumplimiento de sus competencias"* (art. 11.3.c): ¿Puede el Estado recopilar datos en ejercicio de "sus funciones", cualquiera éstas sean, sin consentimiento del titular? ¿Puede, luego, transferirlos o cederlos dentro de su estructura sin mayores limitaciones que sus competencias funcionales? ¿Son "sus funciones" una finalidad en sí misma?

La respuesta debería ser no: las funciones del Estado y/o sus obligaciones legales como base para exceptuar el consentimiento deben ser acotadas y precisas. También debe serlo la finalidad o el propósito por el que el Estado decide recopilar esos datos en ejercicio de sus funciones. Pero la Ley de Protección de Datos Per-

sonales es genérica y la jurisprudencia escasa[3].

Es en este marco que se dicta el Decreto 274/2025. Sin límites claros al intercambio de información dentro del Estado, con excepciones legales ambiguas y sin un criterio interpretativo jurisprudencial contundente, se permite la cesión de cualquier tipo de dato personal, sin reparar sobre la finalidad original con la que se recabó, la sensibilidad que puede revestir, la legitimidad (o no) de su futuro uso, o la falta de mecanismos de control. Es posible pensar que en algunos casos las cesiones se puedan justificar por la eficiencia en la gestión pública –suele ser frecuente el argumento de no duplicar esfuerzos- pero de ninguna forma debe ser la regla general, sin evaluar el costo en términos de derechos. El intercambio de información indiscriminado con los organismos de inteligencia, por ejemplo, es un claro ejemplo de los riesgos que mencionamos. Esta práctica debería, en todo caso, estar respaldada por un análisis de necesidad, proporcionalidad y seguridad, a fin de que solo se compartan los datos indispensables para cumplir con un fin público específico y legítimo, cosa que no sucede a nivel normativo ni se exige en este Decreto para la práctica, como veremos a continuación.

EL DECRETO: TRES CAMBIOS PRINCIPALES

En este escenario, el 16 de abril de 2025 el Poder Ejecutivo emitió el Decreto 274/25[4] modificando algunas cuestiones sustantivas del funcionamiento de la UIF y de la organización del Estado en torno a la prevención del lavado y el conjunto de misiones que tiene atribuidas la Unidad. 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 pretensión de exhaustividad, podemos encontrar en términos generales tres

3 Existen diversos casos donde se disputa el límite de las excepciones a estas cuestiones, algunos actualmente en litigio judicial. El más relevante resulta la sentencia de Cámara en el caso "Torres Abad" (pendiente ante la CSJN) que exige interpretación restrictiva de las excepciones y justificación estricta en caso de ampararse en ellas. También recuerda que el marco internacional, como el RGPD y los Principios de la OEA, exigen demostrar proporcionalidad y necesidad. La misma postura mantuvo en sus resoluciones recientes la Dirección Nacional de Protección de Datos Personales (DNPDP) de la Agencia de Acceso a la Información Pública.

4 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.

grandes aspectos que se modifican sobre la UIF y/o la política de prevención de los delitos mencionados.

En primer lugar, a través de su art. 10 elimina la facultad de querellar de la UIF, que había sido incorporada por el decreto n° 2226 del 2008. Bajo el pretexto de "optimización" de los recursos estatales y reducción de estructuras supuestamente duplicadas, deja esta actividad en cabeza del Ministerio Público Fiscal. Si bien excede el objetivo de este documento, y por lo tanto no profundizaremos en este aspecto, sí es importante resaltar que fortalecer las facultades judiciales del organismo era una de las recomendaciones del propio GAFI.

En segundo lugar, basándose en la necesidad de asegurar una "*adecuada protección de la información sensible y privada de los ciudadanos de la Nación, así como de los datos de importancia estratégica del Estado Nacional*", especialmente luego de recientes "*ciberataques de distinta magnitud en virtud de la vulneración de sus mecanismos de defensa informáticos"*, insiste en "*direccionar de manera eficiente los esfuerzos de los organismos especializados*" y desarrollar auditorías de seguridad informática en el sector público para establecer condiciones mínimas y las medidas necesarias a implementar. Sin mayor argumentación que ésta, el Decreto en consecuencia centraliza toda la política de ciberseguridad en la Secretaría de Inteligencia del Estado (SIDE), específicamente en su Agencia Federal de Ciberseguridad (AFC).

Recordemos que esta agencia, creada por el Decreto de Necesidad y Urgencia 614/24, reglamentado por el Decreto 615/24, es un órgano dentro de la SIDE "con competencia sobre la ciberdelincuencia, las infraestructuras críticas y objetivos de valor estratégico tecnológicos y de la información" (art. 17 del decreto, 8ter de la Ley Nacional de Inteligencia nro. 25.520 que modifica). Con este objetivo, la norma le da funciones confusas y vagas, entre ellas "interceptar comunicaciones" privadas y recolectar, adquirir y procesar "toda información relevante para el Sistema de Inteligencia Nacional" -algo que según la ley en su formulación anterior la Agencia de Inteligencia no podía realizar por sí misma- sin detallar a qué se refiere, de qué forma lo debe hacer, bajo qué parámetros, con qué controles, qué haría con la información obtenida ni por cuánto tiempo la debe almacenar. No deja en claro siquiera si es necesaria la autorización de un juez, cuestión que sí preveía la ley anteriormente. Estas competencias de por sí son riesgosas para el derecho a la privacidad, a la libertad de expresión y a la autodeterminación informativa de todas las personas, que se encuentran así en un estado de sospecha permanente, peligroso y desproporcionado. Más aún teniendo en cuenta que tampoco reforzaron en esa oportunidad los controles parlamentarios ni independientes: más bien se debilitaron. Y avanzar en facultades que implican tal intromisión sin prever mecanismos de contralor, auditoría y/o rendición de cuentas resulta impropio del sistema republicano y democrático, basado en la división de poderes y el control de los actos públicos como principios elementales de gobierno.

A esas competencias ahora se le suman todas aquellas relativas a la ciberseguridad (art. 7 del decreto, modificatorio del 8ter de la Ley 25.520 de Inteligencia) incluyendo, a modo ilustrativo, 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.

Sin pretensión de exhaustividad, 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.

Se trata de un conjunto de facultades que implican -o pueden implicar- una intromisión grande en la vida de los y las ciudadanas, que pasarán a permanecer en secreto, en tanto éste parece ser la regla en cualquier organismo dependiente de la SIDE. Más allá de la idoneidad que puedan tener técnicamente los funcionarios a cargo, de ninguna manera la política de ciberseguridad de una nación debería quedar bajo un manto de opacidad. A la vez, 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.

En efecto, especialistas en el campo de ciberseguridad y la experiencia comparada indican que la creación de un área de estas características bajo la órbita de una agencia de inteligencia refuerza la ineficacia de la política de ciberseguridad al confundir sus objetivos, teñirla de secreto e impedir que se garantice una buena coordinación con las áreas e instituciones que deben proteger sus infraestructuras, por lo que esta tarea no debería recaer en único organismo. 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[5].

En el mismo sentido, vuelve a crear dentro de la AFC el Comité de Ciberseguridad, que hasta ahora pertenecía a la órbita de la Secretaría de Innovación y, por problemas en su diseño e integración, no se había logrado unificar voluntades políticas que permitieran avances sustantivos. Si bien puede ser un paso en el sentido correcto unificarlo dentro de un mismo organismo rector, de ninguna manera éste puede ser la SIDE, con la opacidad y falta de trazabilidad que lo caracteriza. Lo mismo sucede con el traspaso del CERT a su órbita, que lo desnaturaliza por completo: ¿Quién puede pensar que incentiva las denuncias de incidentes o vulnerabilidades que el organismo a cargo sea la Agencia de Inteligencia? En el camino quedó la Dirección Nacional de Ciberseguridad, dependiente de Jefatura de Ga-

5 Para más información sobre esta cuestión, las competencias de la AFC y, en general, la reforma de la SIDE hecha por DNU 614, recomendamos ICCSI, “Comentarios sobre la reforma del sistema de inteligencia”, diciembre 2024.

binete, 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.

Como dijimos, lo cierto es que el decreto no explica de manera directa por qué la centralización en la AFC/SIDE: parece más responder a una decisión por conveniencia política que técnicamente fundada.

En tercer lugar, y es esta la cuestión nos ocupa fundamentalmente en esta ocasión, el decreto en cuestión amplía en gran medida los supuestos en los que la UIF puede intercambiar información, incluyendo personal[6], sin ninguna salvaguarda. Aumenta la posibilidad de recolectar y tratar datos sin incorporar mayores controles que aseguren la protección de la privacidad en los términos en que indican las normas, tal como desarrollaremos a continuación.

LAS NOVEDADES SOBRE INTERCAMBIO DE INFORMACIÓN

En concreto, el decreto en cuestión incorpora nuevos supuestos en los que se habilita, e incluso promueve, el intercambio de información de la UIF con distintos actores, tanto estatales como privados, nacionales e internacionales, sin establecer limitaciones en el tratamiento 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, como describimos al principio de este documento), lo cierto es que el nuevo decreto lo hace de manera extremadamente amplia y vaga, sin agregar salvaguardas acordes o imponer límites que aseguren la protección de derechos.

Desde sus considerandos plantea que, en pos de eficientizar la lucha contra el terrorismo, *"(...) resulta también necesario realizar las modificaciones pertinentes a fin de administrar el flujo de información recibida por los órganos especializados en la materia, a efectos de que los recursos operativos se concentren en el análisis y procesamiento de la información relevante para la mejor obtención de los objetivos perseguidos."*. Veamos en detalle:

6 Entendemos por "información personal" o "datos personales" como toda aquella información relacionada con una persona identificada o identificable.

1) Se le deja de exigir judicializar la información que recaba, sin importar su tenor, contenido y/o de quién provenga.

El art. 1 del decreto 274/2025 modifica las competencias de la UIF (art. 13 de la ley 25.246) en varios sentidos problemáticos. En el inciso 1, que refiere a la posibilidad de la UIF recibir, solicitar y archivar la información, aclara que estos datos "*podrán ser utilizados en el marco de una investigación o para su análisis estratégico para identificar las tendencias y patrones relacionados con el lavado de activos, financiamiento del terrorismo y financiamiento de la proliferación de armas de destrucción masiva.*". Así, a diferencia de la formulación anterior de la ley, ya no se exige judicialización de la información que recaba ni que se haga dentro del marco de una causa existente. Esto implica una disminución de las garantías en torno a la obtención y posibles usos de esa información, mayor discrecionalidad y menor control judicial. Sucede al mismo tiempo que, como vimos, aumenta la competencia de la SIDE (a través de la AFC) en los casos que impliquen cuestiones relativas a ciberseguridad. 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 -como desarrollamos más arriba- que le permitían una autonomía importante con respecto al Poder Judicial, a quien ya no debe pedir autorización en los mismos casos que antes de la reforma del año 2024. Vale agregar que, en este mismo sentido, aquella norma habilitó también los órganos del Sistema de Inteligencia Nacional a centralizar sus respectivas bases de datos, a cargo de funcionarios del mismo Sistema, con "el fin de facilitar su explotación y propiciar su fusión e integración con otras fuentes de información"(art. 24, modificatorio del 16 quinquies de la ley 25.520).

Así, en una lectura conjunta, el panorama es complejo: no sólo aumenta notablemente el universo de sujetos con el que la UIF puede intercambiar información casi sin restricciones (en función de las amplias excepciones de la Ley de Datos Personales que detallamos anteriormente), sino que además disminuyen los posibles controles judiciales, especialmente de aquella que la UIF y/o la AFC decidan no judicializar, sobre un conjunto muy amplio de información sumamente sensible.

Lo mismo sucede al final del último párrafo del inciso 3 de este artículo, que deja a discreción de la UIF poner información que considere relevante -si la hubiera- a disposición del Ministerio Público Fiscal. Nuevamente vemos la opción de judicializar o dar intervención a las autoridades judiciales con respecto a la información solicitada, sin siquiera establecer parámetros mínimos o criterios a seguir para reducir la posible arbitrariedad de esa decisión, ni exigir una justificación por parte de la administración. Dicho de otro modo y 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.

2) Amplía el universo de sujetos con los que la UIF puede intercambiar información, incluyendo organismos de inteligencia, sin contemplar límites ni incorporar salvaguardas y/o instancias de control.

El mismo art. 1 del decreto, en su art. 2 refiere al análisis *"los actos, actividades y*

operaciones" relacionados con la prevención que tiene como mandato la UIF. La ley en su formulación anterior la habilitaba a celebrar acuerdos para el intercambio de información "con otras entidades y/o autoridades públicas nacionales, provinciales y/o municipales" (art. 14.14), tal como mencionamos anteriormente. El decreto ahora incorpora, además, la posibilidad de que, en ese marco, la UIF pueda *"requerir, recibir e intercambiar información (...) con otras entidades públicas que desarrollen actividades de inteligencia, información o prevención, resguardando el carácter secreto, a tenor de lo dispuesto en esta ley, cuando la UIF estime que aquella pueda permitir a las autoridades receptoras enfocarse en los casos o en la información que considere relevante. En caso de corresponder, la UIF pondrá los elementos de convicción obtenidos a disposición del Ministerio Público Fiscal, para el ejercicio de las acciones pertinentes, como así también para coordinar acciones conjuntas."* (sobre este último párrafo nos referimos en el punto anterior: el problema de la discrecionalidad para informar a autoridades judiciales).

Esta disposición se complementa con el artículo 2 del decreto, que modifica el artículo 14 de la ley, referido a las facultades de la UIF, donde agrega un nuevo inciso: *"17. Intercambiar información con otros organismos o entidades públicas con facultades de inteligencia o investigación cuando la UIF estime que la información puede permitir a las autoridades receptoras enfocarse en casos o resultar relevante en la materia de lavado de activos, de financiación del terrorismo o de financiamiento de la proliferación de armas de destrucción masiva. La información brindada por la UIF conlleva la obligación de guardar secreto conforme lo establecido en el artículo 22 de la presente ley".*

Hay aquí, al menos, tres problemas: por un lado, la autorización explícita a intercambiar información con, por ejemplo, organismos de inteligencias, fuerzas de seguridad, fuerzas armadas, migraciones, entre otras, con el nivel de sensibilidad que la información recolectada a través de estas actividades implica. En tanto el principio que rige es la minimización de datos y por lo tanto siempre las autorizaciones para recolectarlos debe interpretarse de forma restrictiva, podía discutirse hasta ahora el alcance del artículo 14.14 de la ley, es decir con qué tipo de entidades públicas podía la UIF celebrar estos acuerdos; luego de esta reforma queda expresamente abierta la puerta. Lo mismo el análisis en función de los principios que deben regir la cesión de información entre organismos del Estado que estudiamos anteriormente: ¿Acaso la UIF mantendrá la finalidad original con que fueron recopilados esos datos por fuerzas de seguridad, cuando su objetivo institucional es diferente? ¿Hasta qué punto pueden extenderse interpretativamente las excepciones de los arts. 5 y 11 de la Ley de Protección de Datos Personales? Esta norma no es ni siquiera mencionada por el decreto en cuestión. Sin embargo, es posible inferir que otorga estas facultades a la UIF bajo el amparo de la excepción al consentimiento de los titulares cuando la cesión de información entre organismos del Estado se haga *"para el ejercicio de funciones propias (...) o en virtud de una obligación legal"* (art. 5) o *"en la medida del cumplimiento de sus respectivas competencias"* (art. 11), es decir como una habilitación absoluta, en sentido opuesto a la interpretación restrictiva que debe regir. Ni siquiera justifica qué datos se recabarán, para qué fines exactos ni qué límites o salvaguardas se establecerán para evitar un uso excesivo o abusivo.

En segundo lugar, la nueva norma extiende el secreto sobre este intercambio: al ser confidencial, ¿Cómo se asegurará el principio de finalidad y la renovación del consentimiento, por ejemplo? ¿Quién será la autoridad de control? ¿La misma Comisión Bicameral de Fiscalización de Organismos y Actividades de Inteligencia, en vez de la Agencia, que es hoy autoridad de aplicación de la Ley de Datos Personales?

Y por último, aunque en este mismo sentido, esta ampliación no trae aparejados nuevos mecanismos de control (o alguna clase de "fortalecimiento" de los existentes) ni de protección, todavía más importantes al tratarse de información confidencial. Como ya dijimos, debería haber límites claros en el manejo de datos personales por parte del Estado, especialmente en lo que respecta al consentimiento y la finalidad específica del tratamiento de datos, siempre regidos por un análisis de necesidad, minimización y proporcionalidad, que el decreto no realiza, contraviniendo los principios fundamentales en materia de protección de derechos. Al mismo tiempo, la autoridad de aplicación de la Ley de Protección de Datos Personales es la Agencia de Acceso a la Información Pública, que no tiene especificidad temática en la materia, carece de autonomía real del Poder Ejecutivo y no es siquiera invocada en el decreto en cuestión. Parecería que todo el contralor recaerá en la mencionada Comisión Bicameral del Congreso, que funciona en secreto.

Recordemos, finalmente, que la opacidad que suele revestir las cuestiones de inteligencia, y que la reforma de la SIDE a través del DNU 615 y su reglamentario 614 de 2024 profundiza, se inscribe en un contexto de creciente repliegue del Estado en términos de información pública, que da respuesta cada vez a menos solicitudes de acceso a información pública[7]. Esta tendencia se consolidó con el decreto 780 de septiembre de 2024, que reforma en sentido regresivo la reglamentación de la Ley 27.275 de Acceso a la Información Pública, restringiendo principios generales y reduciendo en la práctica las posibilidades de ejercer el derecho de acceso. Este escenario es contrario a lo que indican los estándares internacionales en la materia, que hacen hincapié en la rendición de cuentas y la posibilidad de control ciudadano sobre políticas o medidas de gobierno que resulten especialmente intrusivas o riesgosas en términos de derechos".

3) Se amplía el intercambio de información a los propios sujetos obligados, es decir, aquellos que tienen el deber de informar a la UIF.

El art. 3 del decreto agrega al art. 21 de la ley 25.246 que los sujetos obligados *"podrán intercambiar la información recabada a los fines de la debida diligencia del cliente y de la administración del riesgo de lavado de activos, financiación del*

7 Sobre esta tendencia ver, por ejemplo, "Acceso a la Información Pública: cada vez hay más pedidos, pero menos respuestas", el Auditor, 30/05/2025, disponible en https://elauditor.info/transparencia-y-participacion/acceso-a-la-informacion-publica--cada-vez-hay-mas-pedidos--pero-menos-respuestas-_a6834601edd148f87355b4a7a

terrorismo y financiamiento de la proliferación de armas de destrucción masiva, siempre que medie el consentimiento del titular de los datos y se asegure la protección de los datos personales y el deber de guardar secreto, de conformidad con la normativa que dicte la UIF". Si bien es expresa la mención al consentimiento, no deja de ser preocupante la habilitación genérica teniendo en cuenta a) la sensibilidad de los datos, b) el amplio universo de sujetos obligados (desde entidades crediticias hasta proveedores de servicios de activos virtuales, administradoras u operadoras de juegos de azar, empresas aseguradoras, etc) pensando en la cantidad y diversidad de información personal que recaban, y c) la vaguedad de las excepciones al requisito del consentimiento que permite la Ley de Protección de Datos Personales, tal como vimos antes.

Por último, y con respecto a los tres conjuntos de cambios que prevé este decreto, es importante resaltar que no incorpora disposiciones sobre la seguridad de la información en cuestión, estándares mínimos para el resguardo de los datos ni para la prevención de filtraciones. Esto es particularmente importante dados los antecedentes de este tipo de incidentes con bases de datos públicas y privadas en Argentina, y se vuelve aún más necesario en tanto esta norma que aumenta la cantidad y sensibilidad de los datos tratados. Es imperante incorporar mecanismos de auditoría, trazabilidad, y respuesta ante incidentes, que de ninguna manera pueden quedar en el seno de la propia Secretaría de Inteligencia, como parecería ahora tener entre sus competencias la AFC.

CONCLUSIÓN

El Decreto 274/2025 implica una modificación de las competencias de la Unidad de Información Financiera (UIF): algunas las recorta -facultad de querellar- y otras las amplía -intercambio de información-. A la vez, traspasa toda la política de ciberseguridad a la Secretaría de Inteligencia del Estado, subsumiéndola en la confidencialidad y opacidad que caracteriza aquel organismo y alejándola del propósito estratégico que debería tener.

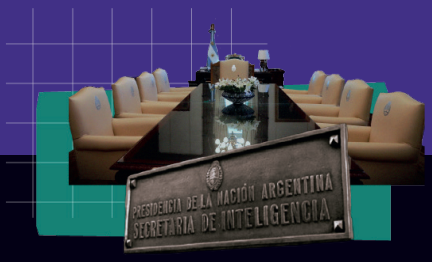
Aunque el decreto se enmarca formalmente en compromisos internacionales asumidos por el Estado en materia de prevención del lavado de activos y la financiación del terrorismo, lo cierto es que sus previsiones evidencian una tendencia preocupante hacia la expansión del poder estatal sin las correspondientes garantías normativas, técnicas e institucionales. Nos referimos, concretamente, al estado de vigilancia permanente bajo el que sitúa a la ciudadanía, fallando en el deber protección de los datos personales y vulnerando el derecho a la privacidad.

Habilita una lógica de cesión e intercambio de datos personales marcada por la discrecionalidad, la opacidad y la falta de control democrático, incluso sobre la información más sensible. Como remarcamos a lo largo de este documento, la inclusión explícita a organismos de inteligencia sin ninguna limitación es, de mínima, preocupante. No se le agrega ningún requisito de control, no se obliga a delimitar con precisión los fines del intercambio ni establecer criterios de minimización, necesidad o proporcionalidad. Esta omisión es particularmente grave si se considera el tipo de datos involucrados, recolectados por las propios organismos de inteligencia.

A la vez, esta habilitación se enmarca en el cese de la exigencia de que la información tratada por la UIF estuviera vinculada a investigaciones judiciales o debiera judicializarse. Este aumento de discrecionalidad del organismo sucede en un contexto más amplio de debilitamiento del control institucional, en tanto no se configura la Agencia de Acceso a la Información Pública como órgano rector, sino la Comisión Bicameral de Fiscalización de los Organismos de Inteligencia, que funciona en secreto.

Por último, el decreto no solo no establece nuevas salvaguardas frente al creciente tratamiento de datos personales por parte del Estado, sino que omite cualquier mención a estándares técnicos mínimos de seguridad de la información, a pesar de que los considerandos aluden a supuestas preocupaciones por recientes ciberataques. Peor aún, subsume toda la ciberseguridad al ámbito de la inteligencia, secreta. ¿Acaso es posible considerar que la SIDE sea el organismo idóneo para, por ejemplo, hacer capacitaciones de buenas prácticas en la materia para el resto de la Administración Pública?

El resultado es el control centralizado de información personal altamente sensible en organismos opacos y escasamente controlados. Dicho de otro modo, un desbalance entre el poder del Estado y los derechos de la ciudadanía, sin incorporar salvaguardas ni hacerse eco de los estándares internacionales sobre la materia. Mediante este decreto, se refuerza un diseño institucional orientado al control y la vigilancia más que a la protección de derechos.



Vía Libre

vialibre.org.ar