Vía Libre

DOSSIER

El Estado de los datos: del registro a la vigilancia

“El Estado de los datos: del registro a la vigilancia”

Autoría: Margarita Trovato

Dirección del proyecto: Beatriz Busaniche

Con el apoyo de la Fundación Heinrich Böll
Buenos Aires, junio de 2026

HEINRICH BÖLL STIFTUNG
BUENOS AIRES
Argentina | Uruguay | Paraguay

Vía Libre

ÍNDICE

Introducción 3

I. El Estado como acumulador de datos: de los registros civiles a la infraestructura de vigilancia 4

- La expansión biométrica
- Los datos en poder del Estado hoy

II. Datos inferidos, perfilamiento y decisiones automatizadas 6

- ¿Qué son los datos inferidos?
- Cómo se regulan en otras jurisdicciones

III. Argentina: el marco normativo vigente y sus límites 9

- Ley 25.326: protección insuficiente
- Débiles controles
- La necesidad de una reforma normativa

IV. La normativa que habilita la vigilancia: reformas al sistema de inteligencia y fuerzas de seguridad (2024-2025) 13

V. El Gemelo Digital Social: un caso hipotético que ilustra riesgos concretos 15

- Qué implicaría el programa
- Los problemas que este programa concentra

Conclusión 18

Introducción

En este informe analizamos qué puede hacer hoy el Estado argentino con los datos personales de la ciudadanía y qué protecciones existen frente a ese poder, en un contexto mediado por el uso de tecnologías.

Partimos de una descripción del ecosistema de datos que el Estado argentino acumula hoy, para luego abordar la cuestión de los datos inferidos. ¿Qué son? ¿Cómo se protegen? Hacemos un recorrido por los marcos normativos de protección de datos y sus debilidades, y a continuación repasamos algunas reformas recientes que habilitan el aumento de la vigilancia, con el objetivo de caracterizar y entender el escenario en el que se despliegan hoy tecnologías para el procesamiento de datos, y los riesgos asociados en términos de derechos humanos de los y las ciudadanas.

El documento se nutre de dos informes previos de Fundación Vía Libre que constituyen su base analítica, a los que remitimos para profundizar en sus respectivas temáticas: *Protección legal de datos personales inferidos*[1], que analiza la categoría de datos inferidos y sus implicancias para los marcos normativos vigentes, y *Datos personales en poder del Estado*[2], que describe el régimen legal y las prácticas del Estado argentino en la materia. A la vez, para una lectura más detallada sobre las reformas al sistema de inteligencia y su impacto en derechos, que abordamos de forma resumida en este documento, recomendamos la lectura del informe elaborado por la Iniciativa para el Control Ciudadano del Sistema de Inteligencia, de la que formamos parte, *Estado del marco regulatorio de la inteligencia en Argentina*[3] (2025).

[1] Trovato, M., "Protección legal de datos personales inferidos", Fundación Vía Libre, 2023.
[2] Trovato, M., "Gestión de datos personales por parte del Estado" , Fundación Vía Libre, 2024.
[3] Iniciativa para el Control Ciudadano del Sistema de Inteligencia (ICCSI), "Estado del marco regulatorio de la inteligencia en Argentina", 2025.

I. El Estado como acumulador de datos: de los registros civiles a la infraestructura de vigilancia

El Estado argentino acumula datos personales desde mucho antes de que ese proceso tuviera nombre propio. Su función registral, entendida como la necesidad de conocer y contabilizar a la población para gobernarla, está en el origen mismo de su constitución como Estado moderno: primero a cargo de la Iglesia Católica, luego de las provincias, finalmente centralizada en el Estado Nacional a partir de las leyes de Registro Civil de la década de 1880 y, más adelante, con la creación del Registro Nacional de las Personas (RENAPER) en 1948. Desde su inicio, esa función implicó recolectar datos sobre nacimientos, muertes, matrimonios, y progresivamente también sobre filiación, identidad, huellas dactilares y fotografías. Dentro de este mandato, con los años fue cambiando de manera decisiva su escala, la tecnología disponible y, en consecuencia, el potencial de intrusión en la vida privada de la ciudadanía y la magnitud de los efectos en derechos de sus decisiones[4].

El punto de inflexión más visible es el Documento Nacional de Identidad: desde sus primeros orígenes en 1968[5], creó un número unívoco de identificación que se convertiría en la "clave primaria" con la que el Estado articula hoy docenas de bases de datos: el padrón electoral, el sistema tributario (CUIT), el previsional (CUIL), la tarjeta SUBE de transporte, la historia clínica digital, entre otras. El DNI es, en la práctica, la puerta de entrada a casi cualquier interacción con el Estado y, cada vez más, con el sector privado. Lo que empezó como un instrumento de identificación se volvió, gradualmente, la columna vertebral de una infraestructura de datos que ninguno de los ciudadanos que lo porta autorizó en esos términos.

La expansión biométrica

El avance de la tecnología profundizó (y sigue profundizando) la estructura de datos en poder del Estado. A partir de 2009 el DNI incorporó datos biométricos, a través del Decreto 1766/2011 y su modificatorio 243/2017. En 2011 se creó el Sistema Federal de Identificación Biométrica (SIBIOS), una base de datos de este tipo de todos los argentinos, con el objetivo declarado de facilitar la identificación a través de cámaras en la vía pública, aunque sin controles suficientes. Como señalamos en su momento[6], los sistemas de identificación biométrica incrementan la capacidad del Estado en materia de vigilancia intrusiva, en parte por la facilidad para interoperar con tecnologías de bases de datos. El riesgo no era solo teórico: los datos del RENAPER empezaron a ser

[4] Para profundizar más en la evolución de este proceso, que delineamos en la presente sección, recomendamos la lectura del capítulo 1 del informe "Gestión de datos personales por parte del Estado".
[5] Decreto-ley 17.671 de 1968, de "Identificación, Registro y Clasificación del Potencial Humano Nacional", aún vigente.
[6] Estado de vigilancia generalizado en Argentina | FUNDACIÓN VÍA LIBRE, mayo de 2012.

cedidos a otros organismos para fines que excedían ampliamente las finalidades originales con las que habían sido recabados.

Un caso lo ilustra con precisión. El sistema de reconocimiento facial implementado por la Ciudad Autónoma de Buenos Aires se nutre de la base biométrica del RENAPER a través de un convenio interjurisdiccional. En 2022 salió a la luz que desde la Ciudad se habían solicitado casi 10 millones de datos biométricos al RENAPER, cuando la cantidad de prófugos que el sistema procuraba identificar era de aproximadamente 40.000. La finalidad declarada del sistema y el uso real de los datos no guardaban ninguna proporción razonable. Fue la consecuencia previsible de, entre otras cosas, un diseño sin controles sobre el destino de los datos una vez cedidos[7].

Los datos en poder del Estado hoy

Hoy, con el avance tecnológico y bajo marcos normativos que analizaremos en las secciones siguientes, el Estado nacional concentra volúmenes inmensos de datos personales de los y las ciudadanas. Las finalidades para las que los acopia ya no tienen que ver únicamente con su función registral originaria sino con la administración de un espectro amplio de políticas públicas.

A través de sus distintos organismos, dispone de información sobre la identidad y biometría de cada habitante (RENAPER), su situación patrimonial y tributaria (ARCA), su situación laboral y previsional (ANSES), sus movimientos migratorios (DNM), su actividad de transporte (SUBE), sus datos de salud (obras sociales y hospitales públicos), su trayectoria educativa y sus antecedentes judiciales y policiales, entre otros. A eso se suma, como veremos a continuación la posibilidad de acceder a información sobre actividad en redes sociales, metadatos de comunicaciones y, a través de inferencias, construir perfiles que van mucho más allá de lo que cada persona proveyó directamente, con muy pocas limitaciones. La pregunta es qué puede hacer el Estado con todo eso, bajo qué reglas y con qué controles.

[7] Ver Por qué se suspendió el sistema de reconocimiento facial de la Ciudad de Buenos Aires - Chequeado, abril 2022. Referido en el informe "Gestión de datos personales por parte del Estado", pág. 11.

II. Datos inferidos, perfilamiento y decisiones automatizadas

Hasta aquí hemos descripto lo que el Estado recolecta directamente: aquello que la ciudadanía le provee con consentimiento en el marco de sus interacciones con distintos organismos. Pero hay una segunda capa de información, invisible para los titulares, que transforma radicalmente el panorama. Se trata de los datos que pueden ser inferidos sobre todos nosotros sin que siquiera tengamos conocimiento y las decisiones que se toman en base a ellos.

¿Qué son los datos inferidos?

Los datos inferidos son aquella información relativa a una persona identificada o identificable que no es provista directamente por su titular, sino creada a partir del análisis (en general automatizado) de datos existentes. También han sido definidos como los generados a través de "una operación intelectual que incluye comparación o deducción" o como "la derivación de información, datos, presunciones o conclusiones a partir de hechos, evidencia u otra fuente de información o datos".[8]

Lo que estas definiciones comparten es el énfasis en tres características: 1) los datos inferidos no son provistos por su titular, 2) son creados por quien procesa los datos originales; y 3) se construyen a partir del análisis de grandes volúmenes de información. En otras palabras, alguien toma datos sobre una persona (muchas) y produce a partir de ellos información nueva que esa persona nunca cedió, y de la que generalmente no tiene conocimiento. Esa información, además, tiene carácter persistente: puede quedar almacenada indefinidamente y servir de base para análisis futuros, posiblemente del mismo tipo estadístico.

Las inferencias funcionan principalmente como base para dos tipos de procesos. El primero es el perfilamiento o *profiling*: el uso de datos personales para evaluar determinados aspectos personales de una persona física, en particular para analizar o predecir aspectos relativos al rendimiento profesional, situación económica, salud, preferencias personales, intereses, fiabilidad, comportamiento, ubicación o movimientos. El segundo es la asignación de puntajes o *scoring*: la traducción de ese análisis en un número que resume a una persona para los fines de quien lo construyó. Como dijimos, ambos procesos son habitualmente invisibles para quien los protagoniza.

Un ejemplo que grafica con claridad los riesgos en el contexto argentino fue el anuncio en 2018 en la provincia de Salta de la implementación de un sistema que permitiría

[8] Las definiciones corresponden, respectivamente a: Wachter, S. and Mittelstadt, B., "A right to reasonable inferences: Re-thinking data protection law in the age of big data and AI", *Columbia Business Law Review*, 2019; European Court of Justice, sentencia del 1 de agosto de 2022, caso C-184/20; California Consumer Privacy Act (CCPA), art. (r). Todas abordadas en el capítulo 1 del informe "Protección legal de datos personales inferidos".

predecir embarazos adolescentes sobre mujeres individualizadas[9]. El Laboratorio de Inteligencia Artificial Aplicada de la UBA-CONICET analizó la metodología y encontró serios errores técnicos y conceptuales, datos de base sesgados e inadecuados, y señaló el riesgo de decisiones incorrectas de política pública. Pero más allá de los errores técnicos, el caso planteó una pregunta de fondo: ¿qué impactos tiene en la vida de una niña que el Estado la catalogue como "predestinada" a quedar embarazada, sin que ella pueda conocer esa categorización ni, en consecuencia, discutirla o impugnarla?. Obviamente implica una afectación directa a la privacidad, pero el impacto en derechos es más amplio: desde la autodeterminación informativa hasta, eventualmente, vulneraciones en el derecho a la educación, a la igualdad y no discriminacion, a la autonomía, a la salud, entre otros.

Vemos que el riesgo aumenta en tanto estas inferencias son, actualmente, el fundamento de decisiones con impacto directo en derechos: quién accede a un plan social, quién es identificado como riesgo de seguridad, qué candidatos electorales son considerados "amenazas". Más aún, las decisiones suelen ser tomadas en el marco de los mismos procesos que infieren estos datos, es decir de manera automatizada. Cabe ahí preguntarse el nivel de revisión humana sobre las prescripciones de los *software* utilizados, que muchas veces es poco significativa o insuficiente.

Cómo se regulan en otras jurisdicciones

Si bien no existe aún una legislación modelo que regule los datos inferidos en todas sus dimensiones de manera exhaustiva, varios ordenamientos jurídicos han dado pasos relevantes en esa dirección.[10]

La ley más avanzada en este punto es la californiana *Consumer Privacy Act* (CCPA, 2018), que incorporó explícitamente los datos inferidos como parte de su definición de información personal y los considera datos personales cuando conforman un perfil sobre un consumidor. En 2022 el Procurador General de California precisó que las inferencias generadas por una empresa sobre un consumidor son información personal bajo la CCPA y deben divulgarse a pedido del consumidor.

En el ámbito europeo, el RGPD reconoce los datos inferidos bajo el paraguas de los datos personales, aunque con importantes lagunas. El Tribunal de Justicia de la Unión Europea sostuvo que inferencias basadas en categorías especialmente protegidas deben recibir la misma protección que esos datos sensibles. El Reino Unido, por su parte, no restringe su definición de datos personales a información fáctica: incluye opiniones e inferencias en la medida en que se relacionen con un individuo e importen a su identificación.

---

[9] Para más información sobre el caso y sus derivaciones ver Sternik, I., "La inteligencia que no piensa", Diario Página/12, abril 2018, y el informe "Protección legal de datos personales inferidos", pág. 25.

[10] Para más información sobre las distintas jurisdicciones y un análisis más profundo de las que aquí mencionamos, ver el capítulo 4 del informe "Protección legal de datos personales inferidos".

Así, las regulaciones internacionales más avanzadas reconocen que lo que debe ser protegido no es solo la información que una persona entrega, sino también la información que otros construyen sobre ella. La Ley 25.326 no los reconoce de manera expresa, lo que se vuelve especialmente problemático cuando el responsable del tratamiento es el propio Estado.

III. Argentina: El marco normativo vigente y sus límites

Hasta aquí describimos dos procesos que corren en paralelo: el Estado argentino acumula cantidades crecientes de datos personales, y la tecnología amplía la capacidad de construir inferencias sobre esos datos y automatizar decisiones en base a ellos. Abordaremos ahora el marco normativo, fundamentalmente la Ley 25.326 (2000) en el que se desarrollan estas actividades.

Ley 25.326: protección insuficiente

En el escenario que venimos describiendo, la Ley 25.326 de Protección de Datos Personales del año 2000, creada como espejo de una directiva europea ya derogada, tiene dos problemas principales: por un lado, no contempla explícitamente los datos inferidos ni las decisiones automatizadas. Como vimos, los datos inferidos presentan características que los distinguen de los "datos personales" en sentido estricto (entendidos como aquellos primarios, que brinda activa o pasivamente el titular) y, por lo tanto, en una interpretación restrictiva pueden quedar por fuera del alcance de esta norma.

Por otro lado, en su formulación actual esta ley permite cesiones entre distintos organismos del Estado de manera casi absoluta. En el contexto de proliferación de sistemas de IA y generación masiva de inferencias para perfilamientos y toma de decisiones automatizadas, esta habilitación resulta alarmante.

Veamos: la ley sí establece, siguiendo estándares internacionales, un conjunto de principios que deben regir cualquier tratamiento de datos. Entre otros, el respeto a la finalidad (los datos recabados para un fin no pueden usarse para otro distinto); proporcionalidad y minimización (sólo deben recolectarse los datos necesarios para el fin declarado); consentimiento informado del titular; y acceso a la información sobre qué datos se tienen y para qué. Vale recordar que la ley reconoce también categorías de datos sensibles (entre ellos los relativos a origen racial o étnico, opiniones políticas, convicciones religiosas, salud y vida sexual) que merecen protección reforzada.[11]

Sin embargo, es sumamente amplia en sus excepciones a estos principios. En particular, para la actuación estatal, prevé excepciones muy generales al requisito de consentimiento. Sus arts 5.2.b, 11.3.b y 11.3.c., de la ley 25.326 permiten que el Estado ceda entre sus dependencias datos de los ciudadanos para finalidades distintas as las que fueron recabadas (excepción al principio general de finalidad), sin informar ni pedir un nuevo consentimiento al titular, en la medida en que sea necesario para "el ejercicio de funciones propias del Estado" o en virtud de una "obligación legal". Esta excepción es el principal punto de tensión en la materia: representa en un cheque en blanco para cualquier uso estatal de datos personales.

[11] Ley 25.326, arts. 4, 5, 7 y 11. Para más información ver el capítulo 2 del informe "Gestión de datos personales por parte del Estado".

Sobre las excepciones previstas por estos artículos, recientemente se pronunció la CSJN en el caso "Torres Abad"[12], declarándolas inconstitucionales por ser contrarias a la protección al derecho a la privacidad en los términos en que lo protegen la Constitución Nacional y los tratados internacionales de derechos humanos a los que Argentina otorga jerarquía constitucional.

Entendió que las reglas del consentimiento y el conocimiento son necesarias para la garantía del derecho a la autodeterminación informativa, derivado de la privacidad, y que, como cualquier limitación a derechos, sus excepciones deben ser razonables, proporcionales y no alterarlos sustantivamente. Además, deben ser necesarias para la prosecución de un fin legítimo. La ley, en su formulación actual, no cumple con estos parámetros: "(...) debido a la amplitud con que la ley 25.326 diseñó las excepciones bajo examen, los entes estatales estarían exentos, virtualmente en todos los casos, de cumplir con la exigencia del consentimiento. Aunque la norma parece delimitar la dispensa con la condición de que los órganos deben actuar en ejercicio de funciones propias del Estado y 'en la medida del cumplimiento de sus respectivas competencias', simplemente no es posible imaginar en qué casos no lo harían (...). No se advierte qué interés legítimo justificaría permitir al Estado que organice un sistema de almacenamiento y tráfico de datos personales sin el conocimiento de sus titulares; sin importar qué tipo de organismos públicos intervienen, cuál es la naturaleza de la información involucrada, el tipo de interés público comprometido o el grado de afectación que se produzca en la privacidad de los afectados. (...) no parecen justificadas ni proporcionadas para proteger 'un interés superior' (...)". (cons. 14).

Así, concluyó que el problema no es la interpretación de la norma sino su formulación: las excepciones, tal como están contempladas ahora, son irrazonables y desproporcionadas, y virtualmente dejan sin efecto el derecho a la privacidad y sus derivados. En consecuencia los declaró inconstitucionales.

Si bien este tipo de declaración aplica sólo al caso concreto, es un buen punto de partida para exigir una actuación estatal acorde a esta interpretación e insistir en la reforma de la ley en este sentido.

Débiles controles

Los efectos de las deficiencias normativas se vuelven más preocupantes en la medida en que los organismos de control no son robustos.

El órgano de aplicación de la ley es hoy la Dirección Nacional de Protección de Datos Personales, ubicada dentro de la Agencia de Acceso a la Información Pública (AAIP). Este diseño institucional presenta dos problemas de distinto tipo. El primero es de estructura: concentrar en un mismo organismo el control del acceso a la información pública y la protección de datos personales implica poner bajo un mismo techo dos lógicas que con frecuencia se contrapone; en la práctica la protección de datos quedó subordinada a la agenda de acceso a la información. El segundo problema es de

[12] CSJN, "Torres Abad, Carmen c/ EN-JGM s/Habeas Data", Expte. No 49.482/2016/CA1, sentencia del 30 de abril de 2026.

independencia: la AAIP opera en la órbita de la Jefatura de Gabinete de Ministros, y su titular es designado y removido exclusivamente por el Poder Ejecutivo, sin intervención del Senado y sin exigencia de idoneidad específica en la materia. Esto es menos independencia que la que preveía la redacción original de la ley, que contemplaba un organismo descentralizado con autonomía funcional.

A estos problemas de diseño se suman los de implementación. La escasa prioridad política asignada a la protección de datos personales se tradujo históricamente en presupuestos magros y capacidades técnicas insuficientes. Hasta ahora "nunca una dependencia estatal responsable de alguna base de datos fue objeto de una inspección por parte de la DNPDP (...). El Estado siempre evitó la facultad sancionatoria de un órgano de control débilmente empoderado para dictar sanciones contra dependencias jerárquicamente iguales o, en general, superiores".[13]

Frente a casos de público conocimiento, como los incidentes que dieron lugar a filtraciones de información por parte de organismos públicos[14], o la presencia de empresas cuyas prácticas irían en detrimento de la privacidad, el accionar de la AAIP fue magro. Apenas comunicados expresando preocupación o anunciando el inicio de investigaciones de las que no se informó nada más, ni a nivel público ni como respuesta a pedidos de información particulares[15].

Este panorama se complejiza en tanto en 2024 se restringió por decreto el acceso a información pública, herramienta clave para el control ciudadano. Si bien la ley 27.275 sobre la materia prevé mecanismos para que la ciudadanía pueda saber qué hace el Estado con sus datos, el decreto 780/24 restringió el universo de información considerada pública, debilitando ese canal de fiscalización.[16]

---

[13] Asociación por los Derechos Civiles (ADC), "El Estado recolector. Un estudio sobre la Argentina y los datos personales de los ciudadanos" (2014), pág 8; referido en el capítulo 4 del informe "Gestión de datos personales por parte del Estado".

[14] Los casos son frecuentes. Por ejemplo, en octubre de 2021 se conoció que la base de datos del RENAPER había sufrido una vulneración de seguridad donde se extrajo información de los documentos nacionales de identidad como foto y número de trámite (ver Filtración del Renaper: difunden datos sensibles de 60.000 argentinos y piden cerca de 17 mil dólares por todos los DNI). Para más información ver el capítulo 3 del informe "Gestión de datos personales por parte del Estado".

[15] Nos referimos a casos como los de WorldCoin, la empresa que ofrece escanear el iris a cambio de una contraprestación económica, o las filtraciones recientes de bases de datos estatales de manos de la empresa SudamericaData. En el primero, la AAIP inició una investigación en 2023 y su último informe público, avisando que seguía en proceso, fue en 2024 (Avanza la investigación de la AAIP sobre WorldCoin y el uso de datos personales | Argentina.gob.ar). Sobre el segundo, informó en diciembre de 2025 el inicio de investigaciones, sin actualizaciones posteriores (La AAIP inició una investigación de oficio ante presunta filtración masiva de datos personales | Argentina.gob.ar). Sobre este caso desde FVL le requerimos información pública sobre el avance de esos procesos, que fueron contestados de manera negativa alegando la reserva de las actuaciones.

[16] Para más información ver, Un decreto no puede limitar el acceso a la información pública | FUNDACIÓN VÍA LIBRE, septiembre 2024.

La necesidad de una reforma normativa

A las debilidades institucionales se suma la obsolescencia de la norma. La Ley 25.326 fue calcada de una directiva europea de 1995 que ya fue reemplazada. No contempla la inteligencia artificial, las inferencias ni las decisiones automatizadas. El proyecto de reforma que circuló en Argentina excluía expresamente la portabilidad de datos inferidos e incluía excepciones amplias y vagas por razones de "seguridad pública" que, como señalamos, el Estado tiende a usar sin justificación suficiente.

Una reforma de la Ley 25.326 debería reconocer explícitamente los datos inferidos como datos personales, prever derechos y garantías frente a las decisiones automatizadas, actualizar las excepciones para el Estado para que sean tasadas y precisas -en línea con la decisión de la CSJN en Torres abad- y dotar a la autoridad de aplicación de independencia y autonomía respecto del Poder Ejecutivo. Además, previsiones de este tipo se condicen con el contenido del Convenio 108 y su Protocolo modificatorio 108+ (próximo a entrar en vigencia) ratificados por Argentina, que establecen la obligación internacional de reconoce el derecho a recibir una explicación suficiente sobre los procesamientos de datos propios.

IV. La normativa que habilita la vigilancia: reformas a los organismos del sistema de inteligencia y fuerzas de seguridad (2024-2025)

Mientras el marco de protección descripto en la sección anterior era ya insuficiente, reformas normativas en 2024 y 2025 sobre inteligencia y vigilancia expandieron simultáneamente el poder informacional del Estado en una dirección opuesta. Por un lado, el marco de protección se debilita: la autoridad de aplicación carece de independencia, la norma es vaga y obsoleta, el acceso a la información se restringe. Por otro, las habilitaciones para la vigilancia se expanden: más datos concentrados en más organismos, menos controles judiciales, más secreto, categorías de amenaza que pueden alcanzar a periodistas, activistas, organizaciones sociales, candidatos electorales o cualquier persona que exprese disidencia[17].

En primer lugar, el Sistema de Inteligencia Nacional fue modificado dos veces por decreto en este período. El DNU 614/24 y su reglamentario 615/24 sentaron las bases institucionales sobre las que se construyeron las modificaciones posteriores. El DNU 941/25 profundizó y consolidó una serie de reformas, introduciendo cambios estructurales en competencias, controles y facultades de la SIDE.

Desde la perspectiva del tratamiento de datos personales, las consecuencias son concretas y graves. El DNU 941/25 obliga a una serie de organismos públicos y a gobiernos de distintas jurisdicciones a compartir sus bases de datos con la SIDE, sin respeto a los principios de consentimiento, finalidad ni minimización que exigen la ley 25.326 y los estándares internacionales. No establece procedimientos para la trazabilidad de la información, ni límites, ni mecanismos de control, ni una política de seguridad de la información. Por el contrario, centraliza la información en la SIDE y la autoriza a compartir esa información (incluso datos sensibles) con agencias de inteligencia extranjeras sin autorización ni control judicial[18].

A esto se agrega un elemento que atraviesa todo el decreto y agrava sus disposiciones: el secreto como regla general. El DNU 941/25 declara todas las actividades de inteligencia como "encubiertas" por definición. Esta presunción generalizada de secreto tiene un efecto directo sobre el régimen de protección de datos: las garantías de la Ley 25.326 (como los derechos básicos de acceso, rectificación, cancelación, oposición) se vuelven prácticamente inoperables cuando el organismo que trata los datos puede ampararse en el secreto para no responder, especialmente en el marco de la reforma

[17] Para ampliar la información de esta sección recomendamos la lectura del informe de la ICCSI "Estado del marco regulatorio de la inteligencia en Argentina", de diciembre de 2025 (elaborado previo a la publicación del DNU 941 del 31/12/25).
[18] Arts. 14-17 del DNU 941/25 que incorporan los nuevos arts. 10 quater, quinquies, sexies y septies a la ley 25.520.

del decreto 780 reglamentario de la Ley de Acceso a la Información Pública al que nos referimos anteriormente.

Este marco normativo es importante leerlo a la luz de la orientación política actual: la Política de Inteligencia Nacional de 2025, en el mismo sentido que las filtraciones del Plan de Inteligencia que existieron durante el mismo año, definen el concepto de "amenaza" de una manera tan amplia que habilita la vigilancia política, social y cultural de sectores que históricamente fueron objeto de inteligencia ilegal. En este sentido, es especialmente relevante para el análisis de este documento la conexión entre esa vigilancia y los datos personales que el Estado ya tiene. Como ejemplo, los datos del RENAPER, de ARCA, de ANSES, de Migraciones, de las bases judiciales y policiales (además de las inferencias que pueden construirse sobre ellos) son la materia prima de los perfiles que el aparato de inteligencia puede elaborar sobre cualquier persona que entre en alguna de las categorías objeto de vigilancia o inteligencia. Las reformas que habilitaron la concentración de esos datos en la SIDE no son separables de la orientación política de su uso.

En simultáneo, también fue aumentando el poder de vigilancia de las Fuerzas de Seguridad federales. Mediante resoluciones ministeriales, en 2024 se formalizó el ciberpatrullaje (vigilancia de espacios digitales públicos) y se creó la Unidad de IA Aplicada a la Seguridad (UIAAS)[19], que le da a las fuerzas un conjunto de facultades amplias, en muchos casos de dudosa legalidad, a las que se les incorpora la posibilidad de ser ejercidas a través de IA, sin mayores precisiones sobre qué significa, con qué controles, con qué limitaciones, utilizando qué software, etc. En la misma línea, en 2025 el Ejecutivo dictó reformó a través de una serie de decretos[20] las estructuras orgánicas de las fuerzas federales, con el objetivo de "modernizarlas" frente al avance tecnológico. El resultado es una serie de facultades amplias para el acceso a bases de datos públicas y la solicitud de acceso a bases privadas con fines de inteligencia criminal, y para realizar ciberpatrullaje sin orden judicial previa y sin mayores precisiones o requisitos. sin definir herramientas, parámetros de búsqueda ni tiempos de almacenamiento de la información recolectada.

[19] Resoluciones 428 y 710/24 del Ministerio de Seguridad de la Nación, respectivamente. Para más información ver Ni artificial ni inteligencia, vigilancia ilegal | FUNDACIÓN VÍA LIBRE, julio de 2024.
[20] Decretos 383/25 (PFA), 454/25 (GNA), 455/25 (SPF), 456/25 (PSA) y 457/25 (PNA).

V. El Gemelo Digital Social: un caso hipotético que ilustra riesgos concretos

En las secciones precedentes describimos un conjunto de habilitaciones para el Estado argentino: desde concentrar datos de distintos organismos en la SIDE hasta construir inferencias sobre esas bases y vigilar la actividad digital de la ciudadanía sin orden judicial, siempre bajo un manto de secreto.

En este marco, el Gobierno Nacional anunció en mayo de este año por la red social "X" un programa denominado "Gemelo Digital Social"[21]. Al momento de elaboración de este informe no hay aún ningún acto público que lo cree formalmente o lo operativice, y por lo tanto no sabemos su alcance ni tenemos más información al respecto que el anuncio comunicacional. Sin embargo, hecha esta aclaración, el análisis del programa nos sirve para ilustrar el tipo de procesos que se pueden llevar adelante a partir de las habilitaciones que fuimos recorriendo, sea con este programa o con otro eventualmente.

Qué implicaría el programa

Según la información disponible, el programa consistiría en procesamiento de grandes volúmenes de información, entrecruzando e integrando distintas bases de datos: policiales, biométricas, financieras, de redes sociales, etc. En otras palabras, se trata del montaje de una infraestructura de toma de decisiones a través de inferencias, en los términos que describimos más arriba. Según el anuncio oficial[22], el software permitiría "ordenar, describir, predecir y prescribir", facilitando así la toma de decisiones en políticas públicas. Así como quedan dudas sobre la implementación por la falta de información disponible, también el anuncio deja muchas preguntas sobre el funcionamiento concreto: ¿la toma de decisiones será automatizada? ¿Cuál es la instancia de revisión humana? Quien va a decidir, ¿conoce el proceso de producción de la información, es decir la lógica algorítmica con la que el software llega al output? ¿Cuál será el proceso de discusión de esas decisiones? ¿Dónde se alojarán los datos producidos y quién garantizará su seguridad?

Es importante aclarar que, al tratarse de inferencias, posiblemente la información que surja de estos modelos no sea tratada como datos personales en sentido estricto y, en consecuencia, los titulares no sean notificados ni puedan discutirla. ¿Cómo se puede discutir ser incluido en una categoría cuando uno no lo sabe? ¿Cómo se puede corregir el "perfilamiento" sin conocerlo? De hecho, oficialmente se informó que no se utilizarían datos personales para el funcionamiento del programa. ¿Y si se trata de inferencias?

En cualquier caso, la circulación indiscriminada de datos dentro del Estado viola los principios de consentimiento y de finalidad de manera directa. Los datos del RENAPER fueron recabados para identificar a la persona en la función registral del Estado; los de

[21] Tweet del 22/05/2026 de la cuenta oficial de Presidente de la Nación, Javier Milei
[22] Tweet del 27/05/2026 de la cuenta oficial de la Ministra de Capital Humano, Sandra Pettovello.

ANSES, para gestionar sus aportes previsionales; los de Migraciones, para registrar sus movimientos. Ninguno fue recabado para construir un perfil predictivo de política social.

El uso en los términos planteados colisiona con la Ley de Protección de Datos Personales, la intimidad y la autodeterminación informativa, pero también genera un riesgo enorme para el goce de otros derechos. Cabe preguntarnos qué pasa si, además, se usara para otras finalidades: pensemos, por ejemplo, política criminal en base a perfilamientos elaborados con todo este caudal de datos. ¿Qué pasa con el derecho de defensa?

Esto se conecta directamente con otra duda que queda pendiente: cómo se controlaría y cuáles serían los mecanismos de auditoría. A su vez, se abren en este punto preguntas sobre los proveedores y la dependencia de ellos (conocida como "vendor lock-in") cuando el propio comprador (el Estado en este caso, y su infraestructura de datos) queda atada a los sistemas propietarios de un único proveedor privado, bajo regulaciones de otro país y con secreto comercial que impide el acceso independiente.

Más aún, sucede en el contexto de expansión de las big tech y el desembarco en nuestra región. Pensemos por ejemplo el caso de Palantir Technologies, una empresa estadounidense que desarrolla plataformas de análisis de grandes volúmenes de datos con aplicaciones tanto en el sector civil como en el militar y de inteligencia, cuyo fundador se instaló recientemente en la Argentina y se reunió con el presidente. Su trayectoria internacional en materia de derechos humanos es objeto de críticas documentadas[23] por lo que su llegada representa, de mínima, una potencial amenaza a los derechos de la ciudadanía en el marco que venimos describiendo.

Los problemas que concentra

Como vemos, un programa del tipo de Gemelo Digital ilustra la convergencia de problemas en distintas dimensiones.

En materia de datos personales, advertimos el cruce sin consentimiento ni finalidad compatible, los datos sensibles procesados masivamente, la ausencia de evaluación de impacto previa. Sobre decisiones automatizadas, las inferencias como base de políticas que afectan derechos sin revisión humana ni mecanismo de impugnación. Con respecto a los controles (o la falta de ellos), el secreto comercial, la opacidad algorítmica y los organismos de control debilitados. Finalmente, y como corolario, en materia de vigilancia estatal y privada: la misma infraestructura que procesa datos para política social puede, si el proveedor tiene productos de inteligencia y el Estado tiene las habilitaciones descriptas, ser orientada hacia la vigilancia política. Esto tiene un efecto directo en la libertad de expresión y sus derivadas (prensa, reunión, protesta), que puede derivar en el auto-silenciamiento ("chilling effect").

[23] Para más información sobre Palantir, su despliegue en otros países y los riesgos locales recomendamos la lectura del informe "Caso Palantir en Argentina" de Amnistía Internacional Argentina.

Hay que ser claros en que la tecnología no es el problema en sí mismo. El cruce de bases de datos estatales puede ser una herramienta legítima si se hace con base legal clara, evaluación de impacto previa publicada, auditoría independiente del algoritmo, revisión humana de las decisiones que afectan derechos individuales, garantías sobre la soberanía de los datos y las decisiones estatales, y con un proveedor cuya trayectoria en materia de derechos humanos sea razonablemente compatible con esos objetivos. Ninguno de esos elementos parece prevalecer en este escenario.

Conclusión

El recorrido de este documento permite trazar un cuadro de situación concreto. El Estado argentino concentra volúmenes inmensos de datos personales, tiene habilitaciones legales para construir inferencias sobre ellos y tomar decisiones automatizadas, y cuenta con un marco normativo de protección que es insuficiente, está desactualizado y se erosionó aún más con las reformas recientes. Los mecanismos de control son débiles o están debilitados, escenario que se vuelve aún más crítico frente al secreto (de Estado o comercial) en el que ocurren estas actividades. El resultado es una asimetría de poder muy fuerte entre el Estado y la ciudadanía: se amplía el poder informacional del Estado sobre las personas, al tiempo que se reducen los mecanismos que permitirían contenerlo y cuestionar sus efectos.

Los derechos afectados son variados y pueden superponerse. La privacidad y la autodeterminación informativa se ven comprometidas cuando una persona no puede conocer ni cuestionar los perfiles que el Estado construye sobre ella. La vigilancia masiva tiene un efecto inhibitorio sobre la libertad de expresión, de prensa y de asociación, incluso antes de que se concrete ninguna acción concreta sobre el vigilado. Los sistemas de perfilamiento invierten la presunción de inocencia al categorizar a las personas por lo que podrían hacer. Y las decisiones automatizadas sobre derechos (acceso a planes sociales, identificación como riesgo, sometimiento a vigilancia intensificada) son opacas y no tienen instancias de discusión accesibles.

¿Con qué garantías se llevan adelante estos programas? ¿Con qué controles? ¿Cuánto poder y soberanía mantiene el Estado sobre los datos y el proceso de toma de decisiones? La tecnología no es neutral ni un problema en sí misma. El punto es cómo se entrena, para qué se usa, cómo se audita.

Vía Libre

vialibre.org.ar