Informe

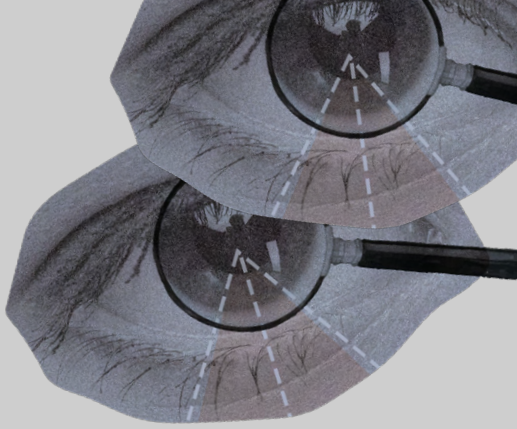
Gestión de datos personales por parte del Estado

Fundación Vía Libre

Abril 2024.

Autoría: Margarita Trovato
Dirección del proyecto: Beatriz Busaniche
Asesoramiento: Enrique Chaparro
Diseño editorial: Alexia Halvorsen

Índice



Introducción

Identificar a los y las ciudadanas es fundamental dentro de una sociedad organizada: desde la provisión de servicios públicos hasta objetivos de seguridad nacional, lo cierto es que la función registral le permite al Estado conocer a su población y elaborar políticas públicas que aseguren el cumplimiento de sus obligaciones. Sin embargo, veremos que a lo largo del tiempo la recolección y tratamiento de esa información personal por parte de organismos públicos fue utilizada con distintas finalidades, cada vez más amplias y, en muchos casos, más intrusivas; muchas veces como consecuencia del avance tecnológico que permite no sólo el análisis de información más íntima (datos biométricos, de salud, por ejemplo) sino también el procesamiento simultáneo de datos que aisladamente pueden parecer inocuos pero en conjunto no lo son. Como contracara, son frecuentes las noticias en los medios de comunicación sobre filtraciones o vulneraciones a la seguridad de las bases de datos del Estado.

En el contexto tecnológico actual, compartimos a diario información propia como domicilio, número de documento, profesión, miembros que integran la familia, estudios cursados, existencia de cuentas bancarias, afiliación o pertenencia a algún partido político, creencias religiosas, etc. Todos estos datos son susceptibles de ser recopilados en archivos o bancos de datos, "con la potencialidad de ser utilizados con fines discriminatorios o simplemente en forma indebida o -lo que es peor- de manera abusiva. Además, si estos datos se entrecruzan pueden arrojar un perfil completo de la persona, es decir, una verdadera "radiografía" del individuo (...)"[1].

Ahora combinemos esta información con el hecho de que el Estado recolecta y trata permanentemente -en principio de manera legítima- datos de los ciudadanos para el ejercicio de sus funciones. Surgen entonces preguntas válidas sobre la forma en que los administra: ¿cuáles son los límites en su manejo? ¿Cómo se garantiza la seguridad y confidencialidad de esa información?¿Qué salvaguardias existen para los titulares de esos datos? ¿Cuál es la protección a la privacidad, tanto individual como colectiva?

[1] Basterra, M., *Protección de Datos Personales*, 1º Ed., Buenos Aires: Ediar; México: Univ. Nac. Autónoma de México – UNAM, 2008, pág. 26.

Para abordar estos interrogantes partimos de la base de la privacidad como derecho fundamental que el Estado debe no sólo abstenerse de vulnerar sino también garantizar activamente. Es que "El simple hecho que se generen y reúnan datos relativos a la identidad, la familia o la vida de una persona ya afecta a su derecho a la privacidad, pues a través de esas acciones, la persona pierde en cierta medida el control sobre una información que podría poner en riesgo su vida privada" [2].

En este sentido se dijo que "No se puede afirmar que esta vasta estructura de actividad colectiva administrada por las autoridades públicas o por cuerpos de voluntarios ayudados por dineros públicos, ha sido hostil a la libertad. Por el contrario, ha incrementado la libertad de millones de individuos extendiendo el campo de actividades abierto a ellos (...) existen otros enemigos de la libertad además del Estado, y que es en efecto, por medio del Estado que los combatimos", pero que no por eso podemos presumir que cada ampliación de los actos del Estado fuera favorable a la libertad. "Si el Estado interviene en el control de la vida personal y familiar, (...) si establece un sistema de espionaje sobre la vida privada de sus ciudadanos y requiere constantes registramientos con propósitos múltiples, tales acciones son claramente opuestas a la libertad. Por ello, entendemos que la ampliación de la esfera de actividad del Estado es sólo admisible en tanto no implique una invasión de las libertades públicas (expresión del pensamiento, domicilio, correspondencia, reunión, salir del país, etcétera) o una irrazonable restricción de los demás derechos individuales (...)"[3].

Es esencial, en este marco, ponerle límites a la actividad del Estado con respecto a los datos personales de los ciudadanos, sin por esto considerar incorrecta, poco ética o contraria a las libertades públicas la existencia de un Estado que planifique y ejecute políticas acorde a las necesidades de la sociedad y se valga para eso de información sobre ella. Lo que sostenemos, en cambio, es la importancia de preservar los derechos esenciales de los ciudadanos y entonces contar con un andamiaje jurídico fuerte que regule la actuación estatal en este sentido y lo obligue a tratar esos datos con la mayor seguridad posible.

Por eso, cuando hablamos de proteger el derecho a la protección de datos entendemos que se trata de asegurar el equilibrio de poderes, así como la

[2] El derecho a la privacidad en la era digital, 2018, A/HRC/39/29, extracto de los párrs. 6 y 7.
[3] Gordillo, A. A., *Tratado de Derecho Administrativo: Parte General*, 2004, pág. 92. Con cita a Robson, W. A., *The Welfare State,* Londres, 1957

participación democrática en los procesos de información y comunicación, “a través de la disciplina los sistemas de obtención, almacenamiento y transmisión de datos”[4]. Veremos entonces a lo largo de este informe cuál fue la función originaria del Estado respecto al uso y tratamiento de datos y en qué situación se encuentra hoy, cuál es el marco regulatorio y cuáles son sus falencias de diseño y aplicación y, finalmente, abordaremos la cuestión de la autoridad de control, esencial en el escenario que describimos.

[4] Basterra, M., “La Garantía Constitucional de Habeas Data. Lineamientos Generales de la Ley de Protección de Datos Personales”, 2016, pág. 13. Con referencia a Pérez Luño, A., E., "Los derechos humanos en la sociedad tecnológica", AA.VV, *Libertad informática y Leyes de Protección de Datos Personales,* Ed. CEC, Madrid, España, 1989, p. 139.

01.

El Estado como generador de datos

El Estado como generador de datos

i. Evolución histórica: del registro civil al RENAPER

La función registral es una de las esenciales de cualquier Estado, especialmente si nos situamos en la etapa de construcción de una Nación (veremos luego cómo esta función primigenia se extiende y amplía a lo largo del tiempo). Su organización y planificación sería impensable sin una política de identificación y registro por parte del Estado, que permita dar cuenta de su población. En Argentina esta responsabilidad la fueron encabezando distintos sectores a lo largo de la historia. En un primer momento era una tarea propia de la Iglesia Católica, que anotaba en sus libros parroquiales datos como nacimiento, matrimonio y defunción de los ciudadanos[5]. Estuvo luego a cargo de las provincias y, finalmente, con la laicidad del Estado, compartida entre éstas y la Nación, a raíz de las leyes nº 1565 de 1884 y nº 2393 de 1888, de creación del Registro Civil de la Ciudad de Buenos Aires y los Territorios Nacionales y de Matrimonio civil respectivamente, que centralizaron en el Estado Nacional la inscripción y el registro de los datos fundamentales (nacimiento, matrimonio y defunción). Así el Estado comenzó paulatinamente a hacerse cargo del registro de los datos vitales de la población, como "un paso más en la consolidación del Estado moderno argentino luego de la sanción de la Constitución Argentina en 1853, que es la que rige hasta el día de hoy, y de la sanción del Código Civil"[6].

En los años subsiguientes, los problemas de fraude electoral que vivió la Argentina impulsaron la sanción de las leyes nº 8129 de Enrolamiento de

[5] Para más información sobre el tema, ver art. Frescura Toloza, D. E., "Debates públicos en torno a la creación del Sistema Federal de Identificación Biométrica (SIBIOS): tensiones entre seguridad y privacidad", XIII Jornadas de Sociología, Facultad de Ciencias Sociales, Universidad de Buenos Aires, Bs. As., Argentina, 2019, sección 1.2, pág. 8 y ss.; y Poder Ciudadano, "Acceso al Documento Nacional de Identidad y derechos básicos en la Ciudad Autónoma de Buenos Aires y Provincia de Buenos Aires. Principales puntos críticos detectados y acciones de incidencia propuestas desde la sociedad civil", julio de 2007, sección 2.1, p. 5 y ss.

[6] Frescura Toloza, Op. Cit., p. 9.

Ciudadanos, nº 8130 de Padrón Electoral y, finalmente, en 1912 la conocida como "Ley Sáenz Peña", la nº 8871, que al establecer el sufragio masculino universal, secreto y obligatorio para todos los ciudadanos hizo manifiesta la necesidad del Estado nacional de contar con un sistema de registro propio. Así fue creada la Libreta de Enrolamiento de Ciudadanos, con doble función: permitía acceder al Padrón Electoral a la vez que garantizaba el cumplimiento del servicio militar obligatorio[7].

Ya durante la primera presidencia de Juan Domingo Perón, en 1948 se creó a través de la ley nº 13.482 el Registro Nacional de las Personas (RENAPER), dependiente del Ministerio del Interior, con la misión de registrar y certificar la identidad de todos sus ciudadanos[8], como respuesta estatal definitiva a la incorporación de las oleadas migratorias. Como explica Frescura Toloza, "La identificación se debía llevar a cabo ante una dependencia del RENAPER, mediante la asignación de una matrícula con un número exclusivo e inmutable. La misma debía registrar datos individuales como nombre y apellido completos, fotografías, impresiones dactiloscópicas, descripción de señas físicas, antecedentes penales, contravencionales y policiales, etc." (pág. 9). Así, su misión era "registrar y certificar la identidad de todas las personas de existencia visible de nacionalidad argentina o que se hallen en jurisdicción argentina o se domicilien en ella (...)" y para ello debía identificar e inscribir a las personas, clasificar sus datos para que puedan ser utilizados por privados y/o autoridades públicas con fines militares, electorales u otros y realizar las actividades estadísticas necesarias para asegurar el censo permanente de las personas (cfr. art. 2).

Sobre esta base llegamos al dictado del decreto-ley nº 17.671 de **"Identificación, Registro y Clasificación del Potencial Humano Nacional"** de 1968, firmado durante el gobierno de facto de Juan Carlos Onganía. Aún vigente, ese decreto derogó la ley previa para dotar de mayores competencias al RENAPER y dio origen a nuestro actual Documento Nacional de Identidad (DNI). Incorporó el registro de datos dactiloscópicos y abrió la puerta a nuevas tecnologías de identificación biométrica[9]. En otras palabras, creó un nuevo dato personal de los habitantes: un número unívoco que sería luego la puerta de entrada a derechos y

[7] Poder Ciudadano, Op. Cit., p. 6

[8] Vale mencionar que en simultáneo tuvo origen la Libreta Cívica, que posibilitó el acceso al sufragio de las mujeres en condición de igualdad con los hombres.

[9] "En la sede central del Registro Nacional de las Personas se llevarán por lo menos ficheros patronímicos, numéricos y dactiloscópicos según el sistema argentino Vucetich u otro que en el futuro aconseje la evolución de la técnica", art. 7. Para más detalles ver Frescura Toloza, Op. Cit., p. 9.

políticas públicas mucho más amplias que la identificación, pero también un factor más de intromisión en la privacidad.

Esta ley le agrega competencias al Estado Nacional, a través del RENAPER, para cuestiones relativas al momento político en que se sanciona, y de hecho lo hace con una lógica castrense también propia del gobierno militar de la época. Por ejemplo, especifica que la clasificación y procesamiento de la información de identificación relacionada con el "potencial humano" debe servir a dos objetivos: por un lado, como insumo para las decisiones gubernamentales sobre política demográfica; por otro, son "necesarios para realizar una adecuada administración del potencial humano; posibilitando su participación activa en los planes de defensa y de desarrollo de la Nación" (cfr. art. 2.b, incs. 1 y 2). **Vemos así cómo se va reorientando la política de identificación y la lógica con que se procesan esos datos: el fin último ya no es sólo la construcción registral de la Nación sino también su desarrollo y participación en la defensa del país.** Y es ahí donde se cristaliza la razón de Estado propia de un gobierno militar como el que sanciona esta ley, donde la identificación de sus habitantes no busca (solo) la mejor administración de los recursos y acceso a derechos, sino el fortalecimiento militar, defensivo, y en términos de "capital" humano productivo para estos objetivos. De hecho, la entonces Ley Nacional de Defensa (nº 16.970 de 1966, contemporánea al dictado del Decreto-Ley que estamos analizando) adjudicaba directamente a las autoridades en esta materia "Planear y coordinar la movilización del potencial humano y los recursos de la Nación" (art. 13.e).

La ley vigente de Defensa Nacional nº 23.554 de 1988, producto del consenso democrático luego de la última dictadura y que deroga la anterior mencionada, ya no lo menciona dentro de sus competencias. Hoy en día está explicitado que el propio Ministerio de Defensa complementa al RENAPER específicamente en el procesamiento de los datos del "potencial humano" **que hace a las fuerzas armadas,** debiendo "Entender en el registro, clasificación y distribución del potencial humano destinado a la reserva de las Fuerzas Armadas y en el fomento de las actividades y aptitudes de interés para la defensa." (art. 19.8, Ley de Ministerios nº 22.520).

Las facultades originales del RENAPER y las que incorpora el decreto-ley de 1986 responden de forma directa al paradigma político de cada momento: primero, a las necesidades de una Nación en plena conformación, y luego propio de un régimen militar en un contexto geopolítico bipolar y en diálogo con la Ley de Defensa vigente en ese tiempo. Sin embargo, la norma sigue igual, con el mismo

título que incluye el concepto de "potencial humano" y la disposición sobre el objetivo de defensa nacional.

ii. El uso de los datos por parte del Estado hoy. EL DNI como signo distintivo y el uso de biometría

Si bien el marco normativo es el mismo, en la práctica la cuestión del tratamiento de datos personales por parte del Estado se fue expandiendo en dos sentidos. En primer lugar, la identificación y el uso de los datos se fue ampliando hacia otras funciones estatales, desde políticas de prevención en seguridad e investigación de delitos hasta diseño de políticas sociales y de la organización del Estado para asegurar derechos y libertades. Recordemos, además, que el DNI es un dato creado por el Estado y es obligatorio.[10] Según la propia ley, es el único idóneo para acreditar la identidad de las personas. No sólo materializa el derecho a la identidad sino que además se requiere para cualquier interacción con el Estado, para trabajar legalmente en el país y para poder hacer transacciones privadas, como las bancarias. Es una clave primaria que identifica a cada ciudadano en el padrón electoral, en el sistema de transporte (la tarjeta SUBE que se usa para pagar el boleto es personal[11]), en el mundo laboral (a través del número único de identificación laboral -CUIL- o tributaria -CUIT-, entre otros[12]. De hecho, las políticas públicas orientadas a disminuir las desigualdades -acceso al trabajo registrado, planes sociales, salud, educación, vivienda, etc.-, no aceptan a personas sin DNI[13].

[10] Vale aclarar que no todos los países cuentan con un único documento identificatorio para todos sus ciudadanos.
[11] Desde Fundación Vía Libre advertimos desde su implementación sobre las amenazas que implicaba para privacidad (ver, por ejemplo, https://www.vialibre.org.ar/con-sube-si-vas-a-pagar-mas-caro-el-fin-de-la-privacidad/). Recientemente se anunció que, si bien no es obligatorio que cada ciudadano registre su SUBE (es decir que la asocie con su número de DNI) a partir de abril de 2024 quienes no lo hayan hecho abonarán más el pasaje: "aplicándose a partir de dicha fecha, a quienes no posean una tarjeta SUBE nominalizada, una tarifa diferencial sobre el tramo que le correspondiere abonar." (Resol. 1/24 del Ministerio de Infraestructura - Secretaría de Transporte, Anexo I, p. 5). Medidas como esta implican de hecho un incremento en el seguimiento estatal y un aumento en la vulneración de la privacidad, dado que no existe otro medio para abonar el pasaje.
[12] Siri, L., "El Documento Nacional de Identidad Argentino: una 'caja negra' y una política de veridicción", III Simposio Internacional LAVITS Vigilancia, Tecnopolíticas y Territorios 13, Río de Janeiro, Brasil, mayo de 2015, pág. 2
[13] Poder Ciudadano, Op. Cit., pág. 22.

Obviamente para todas estas cuestiones es necesaria la cooperación e intercambio de datos entre el RENAPER y otros organismos de la administración pública[14].

De hecho, "según una información del diario 'La Nación' del 3 de febrero de 2002, la Argentina era el país con mayor cantidad de registros pues coleccionaba más de 600 millones de huellas, cuando el FBI sólo tenía 50 millones. Allí también se denunciaba la cantidad de dinero público que se prometía a las empresas (Siemens, Ciccone, Sagem) que lucrarían con la obtención de información y la expedición de distintos tipos de documentos. Este no es un tema menor pues tales empresas serán las beneficiarias más inmediatas de la aplicación de tecnologías que no veo en qué pueden mejorar la condición humana. Tampoco en relación a la seguridad (...) no impedirán actos terroristas por mayor tecnología que implementen."[15]. Es fundamental, entonces, contar con regulaciones suficientes sobre cuál y cómo debe ser el uso que haga de ellos el Estado, en pos de salvaguardar la privacidad de los ciudadanos.

En segundo lugar, el avance tecnológico permitió importantes transformaciones en la identificación y gestión de los datos, pero también mayor vulnerabilidad en términos de privacidad y seguridad. Veremos en el apartado siguiente un ejemplo concreto de esta cuestión pero lo cierto es que la incorporación de tecnologías de vigilancia siguió aumentando en los distintos gobiernos de turno y de los distintos niveles territoriales. El caso del reconocimiento facial en la Ciudad de Buenos Aires es un ejemplo paradigmático. Como se ha afirmado, "Con los avances tecnológicos, las políticas públicas de identificación, registro y clasificación del 'potencial humano nacional' se hicieron más eficientes y efectivas. De ficheros almacenados que podían ser revisados por una persona a requerimiento específico se pasó a información digitalizada en sistemas informáticos de almacenamiento y verificación."[16].

En este escenario, sobre los datos recabados y aquellos presentes en los documentos de identificación hubo sucesivas modificaciones a la norma. Sin pretender exhaustividad, en orden cronológico podemos mencionar la autorización para el uso de tecnologías digitales para la identificación y la emisión del DNI[17] en

[14] Incluso con actores privados. El RENAPER provee, por ejemplo, la autenticación de identidad de una persona a través de datos biométricos para aplicaciones móviles de organismos públicos y empresas privadas.
[15] Anitua, G. I., "'¡Identifíquese!' Apuntes para una historia del control de las poblaciones", en Courtis, C. (comp.), *Desde otra mirada. Textos de teoría crítica del Derecho*, Bs. As., Ed. Eudeba, 2009, pág. 22, nota al pie 76.
[16] Asociación por los Derechos Civiles (ADC), "El Estado recolector. Un estudio sobre la Argentina y los datos personales de los ciudadanos", septiembre de 2014.
[17] Decreto 1501/09.

2009, que pasó a incluir "una fotografía digital del rostro de la persona de frente, una huella digitalizada del dígito pulgar derecho y la firma también digitalizada. Asimismo, posee un código de barras de dos dimensiones, el cual contiene datos biográficos y biométricos cuya lectura permite certificar su autenticidad."[18] En un sentido similar, en 2011[19] se estableció la emisión del pasaporte electrónico con un chip RFID con los datos biométricos y biográficos de su portador, emitido por el RENAPER.

En esta línea se implementó por decreto el mismo año el Sistema Federal de Identificación Biométrica (SIBIOS)[20], una base de datos biométricos de todos los argentinos, independientemente de que sean buscados o no por las fuerzas de seguridad, cuyo objetivo declarado fue facilitar la identificación a través de las cámaras ya existentes en la vía pública, para facilitar la persecución del delito y profundizar las medidas de seguridad. En otras palabras, la identificación ya no está dada por la huella digital y la fotografía sino por los datos biométricos. En un principio los usuarios eran las fuerzas de seguridad nacionales (Policía Federal, Policía de Seguridad Aeroportuaria, Gendarmería y Prefectura), la Dirección Nacional de Migraciones y por supuesto el RENAPER. A través del decreto se propuso la adhesión de otras jurisdicciones y en 2017 se dictó otro donde se invitó a organismos dependientes de los Poderes Ejecutivo o Judicial nacional, provinciales y de la CABA a adherirse al sistema SIBIOS "con miras a que puedan formular consultas biométricas en tiempo real".

En 2014 se profundizó esta línea política de identificación personal con el anuncio del entonces Ministerio del Interior y Transporte de un nuevo documento de identidad, que consistiría en "una tarjeta inteligente multipropósito que permitiría unificar no solo datos biométricos y domiciliarios, sino también los de ANSES (es decir, la oficina que gestiona los aportes a la seguridad social) y los de SUBE [tarjeta para el transporte]. La comodidad que tendría para el ciudadano el nuevo sistema no fue el único argumento esgrimido en su momento por el ministro. También se refirió a una eventual 'prevención del delito'"[21]. Esto es un problema en términos de privacidad, como veremos a continuación, y de seguridad: "si alguien logra vulnerarlo, no solo podría usurpar identidades, sino también acceder y usar como guste la información relacionada con salud, educación, trayectos en transporte público o consumo. Y aunque fuera una tecnología totalmente segura, implica un

[18] Frescura Toloza, Op. Cit., p. 10
[19] Decreto 261/11.
[20] Decreto 1766/2011 y su modificatorio 243/2017.
[21] Siri, L., pág. 4

hito más en una tendencia creciente por parte del Estado a la recolección y análisis de datos utilizables para la vigilancia total de la ciudadanía."[22]. Si bien en aquel momento finalmente no se avanzó con el nuevo DNI anunciado, fue una cuestión de tiempo. Desde 2022 se anunció la incorporación del chip y QR a los nuevos Documentos emitidos y en noviembre de 2023 se hizo oficial por disposición del RENAPER[23] el nuevo diseño y lo que contendrán.

El uso de biometría por parte del Estado es presentado generalmente como un gran avance, entendiendo que la correcta identificación de las personas sería la base de las políticas de seguridad pública y constitución de una Nación[24]. Si bien es cierto que tiene aspectos positivos, también incorpora nuevos riesgos, en lo que aquí nos concierne respecto a la privacidad y protección de datos personales. En el caso de SIBIOS, los problemas son variados.

Tal como afirmamos en aquella oportunidad[25], "Los sistemas nacionales de identificación y otros métodos similares de centralización de datos personales incrementan la capacidad del Estado en materia de vigilancia intrusiva. Junto con la recolección simultánea de identificadores biométricos, tales como rostros digitalizados, se crea una capa adicional de seguimiento que es aún más intrusiva y peligrosa. Como en el caso argentino, las tecnologías biométricas son esencialmente individualizantes y pueden interoperar fácilmente con tecnologías de bases de datos, permitiendo que violaciones extendidas de la privacidad sean sencillas y más dañinas. (...) La base en sí es un foco de ataque importante para estafadores de toda índole.". Veremos a lo largo de este informe que la Ley de Protección de Datos personales plantea límites pero también excepciones para la actividad estatal en este sentido, que deberían interpretarse de manera restrictiva- aunque esto no siempre sucede.

En aquel mismo comunicado agregamos que "Lo que queda claro es que se revierte la presunción de inocencia. Todas las personas son fichadas por las dudas, todos somos presuntamente delincuentes, todos debemos estar bajo control. En nombre de la seguridad pública, la Argentina ha impulsado políticas de vigilancia masiva incluyendo un monitoreo generalizado de los espacios públicos (...). De esta manera, SIBIOS no sólo amenaza la privacidad de los ciudadanos y el derecho a la protección de sus datos personales, sino que también involucra una seria amenaza a

[22] Ibidem, pág. 5.
[23] Dirección Nacional del Registro Nacional de las Personas, Disposición 1255/2023. Ver específicamente Anexo III sobre las medidas de seguridad.
[24] Frescura Toloza, Op. Cit., pág. 14 con cita a Thill (2011) y Janices (2011).
[25] Ver https://www.vialibre.org.ar/estado-de-vigilancia-generalizado-en-argentina/, 10 de mayo de 2022.

los derechos civiles y políticos." Además, al igual que la mayoría de la normativa sobre estos asuntos, fue creado por decreto, acotando la posibilidad de debate público.

Parte de estas preocupaciones se confirmaron poco después: en efecto los datos fueron cedidos para fines distintos a los previstos. En 2013 el padrón electoral incorporaba fotos de los electores provistas por el RENAPER y por una falla de seguridad, el sistema permitía descargarlas mediante un código de programación del sitio web oficial[26]. Otro ejemplo claro es el escándalo por presunto espionaje en el marco del uso del sistema de reconocimiento facial de prófugos que implementó la Ciudad Autónoma de Buenos Aires en 2019, que se nutre justamente de las bases de datos biométricos del RENAPER a través de un convenio interjurisdiccional.[27] A raíz de la prueba producida en la causa judicial donde se analiza la constitucionalidad del sistema, salió a la luz en el año 2022 que desde la Ciudad se habían solicitado casi 10 millones de datos, mientras que la cantidad de prófugos que procura encontrar este sistema es de aproximadamente 40.000[28]. Es imposible suponer que la finalidad con la que fueron recabados esos datos de forma alguna sea compatible con -de mínima- su ingreso frecuente e indiscriminado por parte de la Policía de la Ciudad.

Según una parte de la doctrina el consentimiento de los titulares no aplica cuando los datos son recolectados por el Estado o cedidos entre sus dependencias si se realiza en virtud de una obligación legal y/o en cumplimiento de sus competencias. Esta es la interpretación literal y más amplia de los arts. 5 y 11 de la ley de Protección de Datos Personales. Veremos a lo largo de este documento que, según los estándares nacionales e internacionales, las interpretaciones a la excepción del consentimiento deben ser restrictivas para garantizar la privacidad. Es que este tipo de recolección masiva e innecesaria de datos es contraria a los principios de minimización y proporcionalidad que deberían regir para ser armónicos con el derecho a la intimidad, por el nivel de intrusión estatal que implica y por la cantidad de poder acumulado que le significa. Pensemos, por ejemplo, qué hubiera

[26] Para más información sobre este caso, advertido por la Fundación Vía Libre y cuestionado judicialmente por la Asociación por los Derechos Civiles (ADC), ver ADC, Op. Cit., Cap. IV.
[27] Para más información sobre el sistema, el caso judicial y lo que allí se reveló ver, entre otros, "Un escándalo en Buenos Aires revela los peligros del reconocimiento facial", Revista Wired, 15/09/2023. Disponible en https://es.wired.com/articulos/escandalo-en-buenos-aires-revela-los-peligros-del-reconocimiento-facial.
[28] Para más información ver https://www.cels.org.ar/web/2022/04/el-ministerio-de-seguridad-de-la-ciudad-busco-informacion-biometrica-de-7-millones-de-personas-de-manera-ilegal/

pasado si este sistema hubiera sido adoptado por o estado vigente durante un gobierno militar de facto.

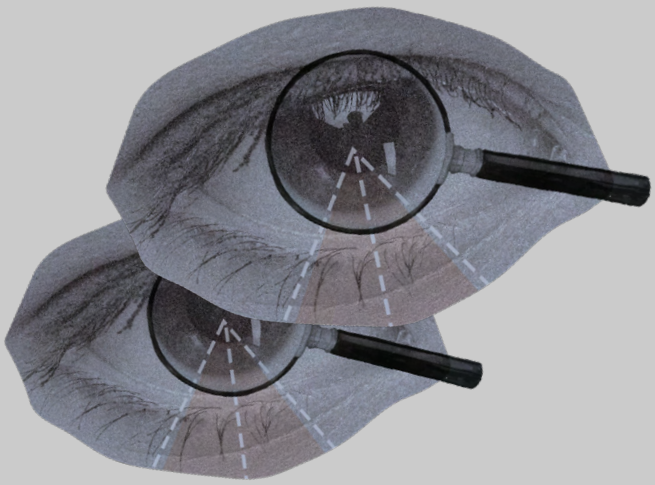
Las experiencias en el mundo también permiten evaluar críticamente la incorporación de estas tecnologías de identificación de modo indiscriminado. Por ejemplo, en el Reino Unido en 2010 el gobierno debió cancelar la creación de una tarjeta de identidad para todos los ciudadanos y a destruir todos los datos biométricos que contenían; en Francia en el año 2012 se declaró inconstitucional una ley para crear un DNI biométrico por vulnerar la privacidad y libertades públicas, señalando que vulnera derechos fundamentales vinculados a la privacidad y a las libertades públicas de los ciudadanos[29]. En ambos casos fue esencial la oposición de la ciudadanía.

Así, vemos que el RENAPER en particular[30], y el Estado en general, recolecta y crea datos personales -así como elementos biométricos que incluso están incorporados hoy en nuestros DNIs- y que la identificación que genera es la puerta de entrada a cualquier contacto con el Estado y al acceso a derechos. A la vez, si bien originalmente tuvo que ver con la función registral de una Nación en construcción, se fue ampliando y hoy permite una política de vigilancia indiscriminada sobre los ciudadanos, sobre la que tienen poco conocimiento y capacidad de control. Esto implica, por un lado, un **deber agravado de seguridad sobre esas bases de datos** por parte del Estado; por otro, la necesidad de **límites normativos claros** sobre qué puede hacer con ellos y funcione entonces como suficiente para proteger el derecho a la privacidad de todos los habitantes.

[29] Frescura Toloza, Op. Cit., notas al pie 18 y 19.
[30] Al igual que al momento de su creación, sigue ubicado en la órbita del Ministerio del Interior. Esto fue ratificado por el nuevo Presidente de la Argentina a través del DNU 8/2023, modificatorio de la Ley de Ministerios, art. 17.9.

02.

Los datos personales en poder del Estado. El deber ser.



Los datos personales en poder del Estado. El deber ser.

i. El marco constitucional y legal de protección de datos personales

Hasta aquí, destacamos que el Estado hoy ya no se limita a recolectar y utilizar datos personales únicamente para llevar adelante su función registral. En cambio, los trata también para planificar y ejecutar políticas públicas, para lo cual genera perfilamientos, predice comportamientos, analiza ubicaciones, etc. De hecho, las autenticaciones de identidad con tecnología de reconocimiento facial en aplicaciones móviles se realizan cotejando con la base de datos del RENAPER, sean de organismos públicos o empresas privadas (bancos, por ejemplo). Y viceversa: el Estado muchas veces se nutre de datos provenientes del sector privado para profundizar la planificación, control y/o ejecución de esas políticas públicas. Es que "La rápida evolución tecnológica y la globalización han planteado nuevos retos para la protección de los datos personales. La magnitud de la recogida y del intercambio de éstos ha aumentado de manera significativa. La tecnología ha transformado tanto la economía como la vida social y es de pública notoriedad que tanto las empresas privadas como las autoridades públicas utilizan datos personales en una escala sin precedentes a la hora de realizar sus actividades, asimismo las personas físicas difunden un volumen cada vez mayor de información personal a escala mundial."[31]. Como dijo en algún momento la ex canciller de Alemania Ángela Merkel, los datos son la materia prima del mundo moderno[32].

Pero la recolección, almacenamiento y tratamiento masivo son evidentemente un problema en términos de privacidad. **El Estado no debería recopilar más datos que los estrictamente necesarios para la política pública que lleva a cabo:** vimos que esa política estatal ha cambiado con el tiempo y se ha

[31] Masciotra, M., "Protección de datos personales y su integración en el marco de los derechos humanos", Sistema Argentino de Información Jurídica (SAIJ), 2018, pág. 11.
[32] Declaraciones publicadas por el Diario "El País", Madrid, 25.1.2018

extendido a cuestiones sociales pero, en cualquier contexto, si la retención de datos es una herramienta necesaria, entonces debe ser sobre la cantidad mínima indispensable para eso, con la debida transparencia de cara a los titulares y en cumplimiento de los estándares de seguridad, siempre recordando que son ellos y no el Estado los titulares de los datos. Durante los últimos años nos encontramos con el uso excesivo y desproporcionado de datos personales para políticas estatales que, si bien pueden representar un fin noble, son sumamente invasivas y no cuentan con las salvaguardas suficientes para estar disponiendo y compartiendo información tan íntima. A modo de ejemplo, podemos mencionar brevemente la problemática ley nacional nº 27.706 sancionada en marzo de 2023, que crea el Programa Federal Único de Informatización y Digitalización de las Historias Clínicas, donde se manifiestan los dos aspectos que mencionamos: se trata de información extremadamente sensible que no debería ser objeto de cierto tipo de intercambio o cesión y, si lo fuera, debería serlo con consentimiento informado por parte de los titulares y los más altos estándares de seguridad para garantizar la debida confidencialidad. Nos referiremos a la cuestión de seguridad de la información en el capítulo 3.ii. de este informe.

Partimos entonces de la base de que, si bien pueden ser necesarias y tener un objetivo legítimo, la posesión y tratamientos de datos personales por parte del Estado son una intromisión en la **privacidad e intimidad de las personas**[33]. Se trata de derechos con el máximo reconocimiento interno, en la Constitución Nacional y leyes nacionales, e internacional, en diversas Convenciones y Tratados, cuyo objetivo es "proteger a la persona de la intrusión de otras en una determinada esfera de reserva personal"[34], de larga trayectoria y recogido en el artículo 19 de la Constitución Nacional. Podemos entenderlos como "la facultad que tiene cada persona de disponer de una esfera, espacio privativo o reducto inderogable de libertad individual, que no puede ser invadido por terceros –ya sea que se trate de particulares o del propio Estado– mediante intromisiones que pueden asumir diversos signos."[35]

---

[33] A los efectos de este informe, trataremos los conceptos de "privacidad" e "intimidad" como análogos y/o los utilizaremos de forma indistinta, tal como lo hace parte de la doctrina, la jurisprudencia y la propia CSJN (Fallos 306:1892).

[34] *Diario de Sesiones de la Convención Constituyente de la Ciudad de Buenos Aires de 1996*, Ciudad Autónoma de Buenos Aires, Editorial Jusbaires, 2016, T. 2, p. 548. Citado en Basterra, M., "Derecho a la intimidad, privacidad y confidencialidad en la Ciudad Autónoma de Buenos Aires", en *Constitución de la Ciudad Autónoma de Buenos Aires. Edición Comentada*, Editorial Jusbaires, CABA, 2016.

[35] Ekmekdjian, Miguel Ángel, *Tratado de Derecho Constitucional*, Buenos Aires, Editorial Depalma, 2005, T. II, p. 375, citado en Basterra, M., Op. Cit., p. 143.

Es que, indefectiblemente, la **privacidad** no sólo es un derecho en sí misma, sino que funciona además como condición para el ejercicio de otros. Sobre el derecho a la vida privada, la Corte Interamericana de Derechos Humanos[36] tiene dicho que "La protección a la vida privada abarca una serie de factores relacionados con la dignidad del individuo, incluyendo por ejemplo la capacidad para desarrollar la propia personalidad y aspiraciones, determinar su propia identidad y definir sus propias relaciones personales. (...) La efectividad del ejercicio del derecho a la vida privada es decisiva para la posibilidad de ejercer la autonomía personal sobre el futuro curso de eventos relevantes para la calidad de vida de la persona. La vida privada incluye la forma en que el individuo se ve a sí mismo y cómo decide proyectarse hacia los demás, y es una condición indispensable para el libre desarrollo de la personalidad"[37]. Es fundamental, en este sentido, contar con herramientas jurídicas que aseguren su protección y promuevan su vigencia de forma amplia.

Con el paso del tiempo y la evolución de la tecnología, este derecho fue ampliándose. Hoy ya no es entendido sólo como la ausencia de información propia en manos de terceros, sino que incluye también la capacidad de control sobre esa información: "(...) el derecho a la intimidad no podía seguir considerándose simplemente la ausencia de información acerca de nosotros en la mente de los demás (el 'déjenme solo'), **sino que debía adquirir el carácter de un control sobre la información que nos concerniera"[38].**

Llegamos así a otro derecho esencial: **la autodeterminación informacional[39],** entendida como el derecho de cada persona a decidir por sí misma sobre la publicidad, divulgación y uso de sus datos personales, también es condición para el ejercicio de otros derechos y por lo tanto debe ser estrictamente garantizada. Es que se trata de "(...) reconocer a las personas una serie de facultades jurídicas que se les atribuyen precisamente para enfrentar las extralimitaciones (...) y que puedan evitar

[36] Para más información sobre la regulación de distintos sistemas regionales de DDHH sobre el derecho a la privacidad, ver Maqueo Ramírez, M. S., Moreno González, J. y Recio Gayo, M, *"Protección de datos personales, privacidad y vida privada: la inquietante búsqueda de un equilibrio global necesario"*, Rev. Derecho (Valdivia) vol.30 no.1, 2017. Disponible en http://dx.doi.org/10.4067/S0718-09502017000100004

[37] Corte IDH, Caso Artavia Murillo y Otros vs. Costa Rica, Sentencia de Fondo (Excepciones Preliminares, Fondo, Reparaciones y Costas), 2012, párr. 143.

[38] Molina Quiroga, E., "Protección de datos personales como derecho autónomo. Principios rectores. Informes de solvencia crediticia. Uso arbitrario. Daño moral y material", 2003, publicado en SAIJ.

[39] Este derecho fue reconocido como tal por primera vez por el Tribunal Constitucional Federal Alemán en 1983 en una sentencia sobre el censo: *BVerfG*, fallo del Primer Senado de 15 de diciembre de 1983, 1-BvR-209/83, § 1-215. Disponible en inglés en https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/EN/1983/12/rs19831215_1bvr020983en.html.

que de su mal uso lesionen bienes o derechos constitucionales como la intimidad y los derechos conexos."[40].

En tanto los datos personales permiten identificar a la persona a la que el dato pertenece y, en consecuencia, también a establecer conductas y prácticas que sólo mediando su expresa voluntad deberían trascender la esfera de su intimidad, es que encontramos al derecho a la autodeterminación informativa como fundamento de la protección de datos personales[41].

En este contexto, es indispensable la protección jurídica a través de normas que otorguen garantías a los ciudadanos y operen como frenos para la recolección y tratamiento abusivos, especialmente por parte del Estado.

Veamos cómo funciona en Argentina. Con la reforma constitucional de 1994 se consagró la protección de datos personales en el máximo nivel normativo: por un lado, se incorporaron con la misma jerarquía tratados internacionales de derechos humanos que incluyen entre sus previsiones el derecho a la privacidad e intimidad que no sólo implican la obligación de los Estados de protegerlo sino que, además, refuerzan su importancia como garantías básicas a asegurar en el sistema argentino.

Por otro lado, además de prever estas garantías en sus arts. 18 y 19, se reguló expresamente la protección de datos personales en el art. 43, que codifica la acción idónea para su reclamo. Establece que "Toda persona podrá interponer esta acción [refiere a la acción de amparo] para tomar conocimiento de los datos a ella referidos y de su finalidad, que consten en registros o bancos de datos públicos, o los privados destinados a proveer informes, y en caso de falsedad o discriminación, para exigir la supresión, rectificación, confidencialidad o actualización de aquéllos. No podrá afectarse el secreto de las fuentes de información periodística." Vemos así que esta disposición constitucional sienta las bases para la protección de la privacidad y la seguridad de la información de los ciudadanos, dotándolos de mecanismos para asegurarlas.

Establece en general el marco de protección de los datos personales frente tanto al Estado, contenidos en "bancos de datos públicos", como aquellos en manos de privados. A los efectos de este informe nos centraremos en el primer caso. En

[40] Castillo Córdova, L., *Comentarios al Código Procesal Constitucional,* tomo II, Ed. Palestra, Perú, 2006, p. 975, citado en Orrego, A. C., "Una aproximación al contenido constitucional del derecho de autodeterminación informativa en el ordenamiento jurídico peruano", en *Anuario de Derecho Constitucional Latinoamericano, año XIX,* Bogotá, 2013, p. 317. disponible en https://biblioteca.corteidh.or.cr/tablas/r32202.pdf

[41] Basterra, M., *Protección...* Op. Cit., pág. 29. Con cita a Pizzolo, C., "Tipología y protección de datos personales. El sistema establecido en la ley 25.326 y la legislación comparada", JA, 2004-II, p. 1439.

este sentido, vale recordar que la CSJN precisó poco después de su sanción el alcance de la ley con respecto a la información personal en poder estatal, definiendo como "banco de datos públicos" todos aquellos pertenecientes "a organismos del Estado, incluso y en especial, los reservados con carácter secreto", incluyendo así a fuerzas de seguridad y organismos de inteligencia, salvo que justifiquen adecuadamente la procedencia de alguna excepción[42].

Es que, según explica Gelli , "En efecto, como bien lo señalara en su intervención el convencional Juan Pablo Cafiero, en un principio, la preocupación por incorporar la garantía del hábeas data a la Constitución Nacional, giró en torno a la necesidad de proteger a las personas frente al contenido de los registros y asientos que de ellas pudieran efectuar los organismos de seguridad del Estado. La historia de la represión ilegítima en la Argentina, recrudecida en la década de los setenta, gravitaba con el peso de la violación de las garantías personales en el ánimo de los convencionales constituyentes, quienes procuraron poner remedio, en el futuro, a eventuales quebrantamientos de los derechos humanos. La obtención de certeza acerca de lo que el Estado conocía y asentaba sobre las personas, constituyó una prioridad para la seguridad de todos. (...) La instrumentación del hábeas data como remedio a tales situaciones de desaparición forzada de personas, perfilaba un instituto jurídico sin duda singular, un instrumento llamado a condicionar el secreto de Estado sin por ello desproteger a éste ni tampoco a las sociedad."[43]. Esta historización se condice con el hecho de que las normas de identificación estatal de personas fueran (y sigan siendo) de épocas militares, mostrando de qué manera el instituto del habeas data está ligado a la trayectoria política y social de la argentina. A la vez, su lógica es la misma que impera frente a un Estado democrático: la necesidad de establecer límites y parámetros en el manejo de los datos que, muchas veces de manera legítima, recolecta y/o infiere.

A través de esta acción, la legislación está protegiendo un abanico de derechos vinculados con la protección de datos personales: en palabras de la CSJN, el hábeas data es una garantía al mismo tiempo que un derecho en sí mismo[44]. Como explica la doctrina, "La norma constitucional, más que proteger los datos personales, comerciales, patrimoniales o sensibles, está resguardando una multiplicidad de

[42] CSJN. "Ganora, Mario E. y otra s/ habeas corpus" (1990), Fallos 322:2139. Voto Dr. Fayt, cons. 6 y 7. Cfr. Gelli, M. A Gelli, M. A., *Constitución de la Nación argentina: comentada y concordada*, Ed. La Ley, 2º ed., Bs. As., Argentina, 2004, pp. 413-415.

[43] Gelli, Op. Cit., pág. 407. Con cita a Cafiero, J. P., Convención Convencional Constituyente, 3a Sesión Ordinaria, 12 de agosto de 1994, págs. 4151/53.

[44] CSJN, fallo "Ganora Mario Fernando y Otra s/Habeas Corpus", 16/09/1999, cons. 11 y 12 del voto del Dr. Boggiano.

derechos sustantivos, tantos como pudieran verse afectados por la difusión, falsedad, o efecto discriminatorio del tratamiento de aquellos datos. El derecho a ser dejado a solas el derecho de mirada sobre lo que se registra de cada uno; el derecho a la identidad; a la imagen a la intimidad; a la seguridad personal y patrimonial; el derecho a la verdad; en fin, la lista parece inacabable"[45]. A la vez, no sólo se garantiza el acceso a los datos -condición de posibilidad del ejercicio de estos derechos- sino que también se permite ejercer "un control activo sobre los datos, a fin de supervisar no sólo el contenido de la información en sí, sino también aquello que atañe a su finalidad" por lo que "es evidente que se trata, a la vez, de un instrumento de control"[46].

Si bien seguramente existan circunstancias que limiten los derechos de los titulares en función de la necesidad o "conveniencia social" del Estado de registrar o darle determinado tratamiento a datos personales de la población, deberán siempre regirse por el marco y las limitaciones establecidas por la ley. Tal como veremos más adelante, los organismos estatales sólo podrán recabar datos personales cuando resulten necesarios para el ejercicio de sus funciones y con el consentimiento del titular de los datos, salvo que proceda alguna excepción, en cuyo caso deberán justificarla adecuadamente. Esto se vincula directamente con los principios generales del derecho administrativo que determinan que el Estado sólo puede hacer aquello para lo que se encuentra expresamente habilitado (al revés de las personas físicas que podemos realizar todo aquello que no esté prohibido). Dicho en otras palabras, no sólo es necesario el consentimiento del titular sino que normativamente el Estado debe tener **permitida de manera expresa la facultad de recabarlos y tratarlos[47].**

Esta previsión fue luego reglamentada y desarrollada con mayor profundidad a través de la Ley Nacional de Protección de Datos Personales nº 25.326 del año 2000, que complementa en este sentido al Decreto-Ley 17.671/68 de identificación de las personas por parte del Estado. En términos generales, entre otras novedades[48], y además de jerarquizar este derecho otorgándole una regulación

[45] Gelli, Op. Cit., pág. 418.
[46] CSJN, "Urteaga, Facundo Raúl c/ Estado Nacional - Estado Mayor Conjunto de las FF.AA. s/ amparo-ley 16.986", 15/10/1998, cons. 13, del voto del Dr. Petracchi.
[47] En este sentido, nuestro ordenamiento se asemeja al sistema europeo que establece "que cualquier actividad relativa al procesamiento de datos personales está prohibida, salvo cuando está permitida, a diferencia de la legislación estadounidense que se sustenta en que todo está permitido, salvo lo que está prohibido.". Ver Masciotra, M., Op. Cit., pág. 3.
[48] Para una exposición breve sobre su contenido, ver Bastera, M., "La Garantía...", Op. Cit., y Gelli, M. A., Op. Cit, pp. 421 y 422.

específica, es importante destacar que establece principios generales sobre el consentimiento de los titulares, las condiciones del tratamiento de los datos y su conservación; explicita los derechos que asisten a los titulares (de información, acceso, rectificación, supresión y oposición); precisa la vía administrativa y judicial de exigibilidad del derecho a la protección efectiva de los datos personales y los derechos que de ella se derivan, a través del habeas data (que en la Constitución Nacional estaba sólo como una especie de la acción de amparo); exige el registro de los bancos de datos, establece un contralor sobre ellos y dispone sanciones administrativas y penales frente a incumplimientos; y crea la autoridad de aplicación, que abordaremos en el capítulo 4 de este informe. A la vez, tiene algunos puntos problemáticos sobre los que nos explayaremos a continuación: deja algunas lagunas sin resolver y plantea regímenes de excepción amplios, fundamentalmente para el consentimiento para la obtención o cesión de datos personales, o el tratamiento de datos sensibles.

Si bien fue un avance necesario y positivo al momento de su sanción, en las más de dos décadas transcurridas desde su entrada en vigencia, la protección de la información personal en nuestro país ha sido bastante deficitaria: en la práctica se ha hecho muy poco en defensa del derecho a la privacidad de las personas ante intromisiones estatales o privadas. Este déficit se relaciona tanto con falencias del marco legal como con falta de voluntad política (parte de lo cual abordaremos en el apartado 4 al reflexionar sobre la autoridad de aplicación). Sobre las primeras, se advierte, por un lado, la falta de previsión de una autoridad con suficiente independencia -tal como veremos más adelante-; por otro, por la obsolencia que ya caracteriza a la ley 25.326. Es que se basa, casi textualmente, en la Directiva europea 465 del año 1995 que fue objeto de un largo período de discusión y, aunque ciertos principios fundamentales permanecen invariables, la evolución técnico-económica de 40 años requiere respuestas normativas más adecuadas a los tiempos. Así lo entendió la Unión Europea cuando en enero de 2012 encomendó el actual Reglamento General de Protección de Datos (2016)[49].

De hecho, la evolución tecnológica incorporó nuevos desafíos y prácticas que exceden las previsiones de nuestra ley e imploran una más actualizada. Hubo numerosos proyectos de reforma presentados en el Congreso Nacional; a la fecha de elaboración de este informe aquel presentado por el Poder Ejecutivo en junio de

[49] Para más información sobre el proceso europeo remitimos a las observaciones que presentamos desde la Fundación Vía Libre en ocasión de la candidatura de Fuentes como Director de la Agencia de Acceso a la Información Pública en marzo de 2021. Disponibles en https://www.vialibre.org.ar/wp-content/uploads/2021/03/Observaciones.AAIP_.FundacionViaLibre.pdf, pág. 3.

2023[50] fue ingresado a la Cámara de Diputados, y girado a las comisiones de Asuntos Constitucionales, Legislación General, y Presupuesto y Hacienda.

ii. Salvaguardas frente a su uso por parte del Estado. Consentimiento, principio de finalidad y sus límites

Uno de los puntos más problemáticos de la ley en su formulación actual es la regulación sobre los datos personales en poder del Estado y el uso que éste puede darles. En función de lo desarrollado, es clara la relevancia de la protección jurídica de los datos personales, entendiendo las garantías que deben regir su recolección y tratamiento y el principio general de limitar la acción Estatal sobre ellos para reducir al mínimo posible la intromisión en la privacidad. **Debemos enfocarnos entonces en dos ejes que hacen esta cuestión: por un lado el consentimiento del titular y, por otro, la finalidad del uso de su información por parte del Estado.**

Nos referimos en primer lugar **a la cuestión del consentimiento** porque es, como su nombre lo indica, la "acción" que exige la ley por parte del titular para que la obtención y tratamiento de sus datos personales sea lícito. Si bien existen excepciones a este requisito y se excluyen ciertas categorías de datos para el tratamiento aun cuando sí lo haya (aquellos sensibles, entre otros), es el consentimiento el criterio central para determinar la licitud de la obtención y tratamiento de datos personales, que deberá cumplir ciertas condiciones.

Veremos que la ley protege los datos personales a través de dos prohibiciones generales, de tratar y de ceder datos personales sin el consentimiento de los titulares, aunque las dos con un variado régimen de excepciones. Se ha afirmado en este sentido que "Ambas buscan impedir la explotación ilícita de los datos de los ciudadanos mediante un recurso que parece efectivo: darnos el poder de negarnos a que terceros exploten esos datos para fines con los que no estamos de acuerdo. Sin embargo, la ley que nos da ese poder también nos lo quita cuando queremos ejercerlo en contra de las acciones del Estado"[51] en la práctica.

[50] Nota de elevación al Congreso y proyecto disponibles en https://www.argentina.gob.ar/sites/default/files/mensajeyproyecto_leypdp2023.pdf
[51] ADC, Op. Cit., p.3.

En concreto, como regla general la ley exige en su art. 5 que el consentimiento para el tratamiento sea "libre, expreso e informado", por escrito o "por otro medio que permita se le equipare, de acuerdo a las circunstancias". Según la reglamentación de la ley (decreto 1558/2001), el consentimiento cumplirá estas condiciones cuando esté "precedido de una explicación, al titular de los datos, en forma adecuada a su nivel social y cultural, de la información a que se refiere el artículo 6 de la Ley". Refiere en este punto al derecho del titular que la ley consagra en el mencionado artículo a ser informado de diversas cuestiones al momento de recabar sus datos personales; entre otras, la finalidad para la que serán tratados y quiénes pueden ser sus destinatarios o clase de destinatarios (art. 6, inc. a). La reglamentación aclara también que el consentimiento puede ser revocado en cualquier momento (aunque sin efecto retroactivo), por lo que se vuelve aún más necesario el correcto ejercicio del derecho de información sobre el tratamiento de los datos.

A continuación la ley establece una serie de **excepciones**, es decir casos en los que el consentimiento no será necesario para que el tratamiento sea lícito, que deberán aplicarse siempre de acuerdo a los principios de proporcionalidad y necesidad, procurando un equilibrio entre el interés público que fundamenta el tratamiento de los datos y la protección de los derechos individuales. Refiere, por ejemplo, a aquella información como nombre, documento nacional de identidad, identificación tributaria o previsional, ocupación, fecha de nacimiento y domicilio (art. 5.b), en tanto no implicaría una intrusión arbitraria en la esfera personal. En todos los casos se deberá informar al titular el tratamiento de sus datos, en cumplimiento del deber general de información (arts. 5 y 6).

Pero, volviendo a las excepciones, resulta particularmente problemática la que prevé la ley en el inciso b: **no será necesario el consentimiento 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). La formulación es tan amplia que puede tornarse sumamente abusiva: es necesario entender a qué obligación legal refiere, si cualquier mandato estatal es válido para evitar obtener el consentimiento, en qué condiciones puede hacerlo, si lo mismo se aplica para cederlos a otros organismos estatales. En otras palabras, puede funcionar como una ventana a usos discrecionales, excesivos y sin justificación por parte de los responsables del tratamiento, en este caso el Estado. A modo de ejemplo, podemos pensar en que se trata de "obligaciones legales" aquellas impuestas la Ley de Inteligencia Nacional nº 25.520 en lo concerniente a interceptación de

comunicaciones o las obligaciones que impone a los licenciatarios de servicios de tecnologías de la información y comunicaciones la Ley Argentina Digital nº 27.078 (art 62 incs. g, h, i)[52].

En este punto es importante recordar que esta norma fue una copia casi textual de la entonces ley de España en la materia (Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal – "L.O.P.D.") que fue declarada inconstitucional poco tiempo después[53], pero la ley local no tuvo ninguna modificación en esa línea.

En un escenario de esta naturaleza, es fundamental asegurar la interpretación restrictiva de este tipo de excepciones. En este sentido, los Principios Actualizados sobre la Privacidad y la Protección de Datos Personales de la Organización de Estados Americanos (OEA)[54] sugieren que "en esos casos, la parte que recopile y trate los Datos debería demostrar que tiene una necesidad clara de hacerlo para proteger sus intereses legítimos o los de un tercero a quien puedan divulgarse los Datos. También se debería demostrar que hay un equilibrio entre los intereses legítimos de la parte que busque la divulgación y los intereses del Titular de los Datos.".

De hecho, parte de la doctrina especializada[55] sostiene que debe interpretarse siempre en consonancia con las previsiones de la ley sobre el tratamiento de datos personales "con fines de defensa nacional o seguridad pública por parte de las fuerzas armadas, fuerzas de seguridad, organismos policiales o de inteligencia" (art. 23), en tanto explicita en qué casos puede ser realizado sin consentimiento de los titulares y las condiciones en las que debe llevarse a cabo. Es que, según entiende, la excepción al consentimiento por tratarse de "una función propia" del Estado o "en virtud de una obligación legal" sólo procede para recopilaciones de datos con estos propósitos según los mandatos legales específicos de cada fuerza y en cumplimiento de una misión determinada (y no de manera genérica), y conservados

[52] Para más información ver Piccirilli y Quiroga, "Principios Nacionales e Internacionales en el marco de la Protección de Datos Personales. Deficiencias. Recomendaciones.", 15º Simposio Argentino de Informática y Derecho, 2015, pág. 6

[53] Fue declarada su inconstitucionalidad parcial en el año 2000. "Tribunal Constitucional de España. Pleno. Sentencia 292/2000, de 30 de noviembre de 2000. Recurso de inconstitucionalidad 1.463/2000. Ref. BOE-T-2001-332", disponible en https://www.boe.es/boe/dias/2001/01/04/pdfs/T00104-00118.pdf.

[54] Organización de Estados Americanos (OEA), "Principios Actualizados sobre la Privacidad y la Protección de Datos Personales", enero de 2022. Parte II, principio 2, pág. 34. Se trata de principios y recomendaciones que, si bien no son vinculantes, resultan rectores y de gran peso interpretativo para la región.

[55] Basterra, M., "El consentimiento del afectado en el proceso de tratamiento de datos personales", Lexis Nexis - número especial, 2004, p. 6 y ss.

únicamente por el tiempo que sea necesario para el cumplimiento estricto de los fines de recolección. Aclara además que, en tanto las leyes de deben interpretar en forma armónica y no analizando aisladamente sus previsiones, determinados datos -tales como la orientación sexual, origen étnico, datos referidos a la salud- sólo podrán ser autorizados al tratamiento si se aplica la disociación del dato, esto es sin que sea identificable la persona a la cual pertenece ese dato.

Esta limitación se debe a que, según explica Basterra, "Sólo con una interpretación restrictiva de la ley se logrará la efectiva protección del derecho a la autodeterminación informática[56]. En el caso particular deben darse los requisitos que la propia ley en la presente excepción establece para que no se transforme la misma en un 'arma de doble filo', cuando justamente el exceptuado puntualmente para recopilar datos sin consentimiento es el estado a través de los organismos específicos establecidos en la ley."[57]. Es cierto, además, que dada la opacidad que suele regir en estos ámbitos y la dificultad que representa asegurar la vigencia de las garantías legales en casos así, es fundamental restringir al máximo el alcance de la excepción.

Esto mismo entendió la Cámara Contencioso Administrativa Federal[58] al afirmar que "(...) la regla en materia de tratamiento de datos -según la Ley No 25.326- es el consentimiento del interesado y, las excepciones a ella, son las previstas en el artículo 5º de ese texto legal, que deben ser interpretadas de manera restrictiva.". A la vez, entendió que la excepción al consentimiento para el tratamiento de datos dado por el art. 5.2.b), es decir el ejercicio de funciones propias del Estado o cumplimiento de una obligación legal, debe entenderse de manera acotada con respecto a "objetivos que se vinculen con una finalidad de defensa nacional, seguridad pública o represión de delitos, tal como lo exige la doctrina especializada" y que "Debe advertirse, a la luz de la doctrina y la jurisprudencia comparada, que toda intrusión en la esfera de datos de una persona debe estar rigurosamente justificada con base legal, sin que proceda la invocación de excepciones genéricas que desnaturalicen ese derecho".

[56] Si bien la autora utiliza el término "autodeterminación informativa" y lo reproducimos textualmente para mantener la fidelidad de la cita, desde la Fundación Vía Libre preferimos referimos a este concepto como "autodeterminación informacional" o "relativa a la información personal" en tanto no se trata de algo que se informa sino de algo relativo a la información.
[57] Ibidem, p. 19.
[58] "Torres Abad, Carmen c/ EN-JGM s/Habeas Data", Expte. No 49.482/2016/CA1, sentencia del 03/07/2018, Cámara en lo Contencioso Administrativo Federal, Sala V. Cons. 9 y 10.

Para comprender la relevancia de requerir el consentimiento debemos introducir en paralelo otros principios rectores que rigen en materia de protección de datos personales y tienen que ver con lo "extraordinario" o de *última ratio* que debería ser su tratamiento y por lo tanto las salvaguardas que existen. En primer lugar nos referimos al **deber de minimización** para quien los recaba y procesa: implica que sean adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados.

En este sentido lo establece claramente el RGPD, que establece entre los principios del tratamiento de datos (art. 5) que sólo se pueden recolectar aquellos datos que sean estrictamente necesarios para el tratamiento, en el momento que vayan a ser tratados (no para el futuro) y ese tratamiento debe ser únicamente aquel relativo a la finalidad con que fueron recabados. Este conjunto de deberes -que recoge el RGPD pero se trata de un principio general en la materia- es lo que se conoce como *minimización de los datos.*

De aquí se desprende que cualquier tratamiento de datos debe hacerse con un criterio de **proporcionalidad,** es decir la premisa de que, en tanto la recolección y tratamiento de datos implica una vulneración a la privacidad, sólo debe realizarse sobre aquellos estrictamente **necesarios** para la finalidad buscada. Dicho de otro modo, el "uso" de datos -en este caso por parte del Estado- debe ser proporcional con el objetivo de la política pública que alimentan, y entonces tener una clara finalidad. Es ésta última la que determinará luego si los datos están o no correctamente cedidos entre las distintas dependencias, buscando que de ninguna forma el tratamiento (y por lo tanto la afectación a la privacidad) sea *desproporcionado* con respecto al objetivo original buscado.

De aquí se desprende que cualquier tratamiento de datos debe hacerse con un criterio de **proporcionalidad**, es decir la premisa de que, en tanto la recolección y tratamiento de datos implica una vulneración a la privacidad, sólo debe realizarse sobre aquellos estrictamente **necesarios** para la finalidad buscada. Dicho de otro modo, el "uso" de datos -en este caso por parte del Estado- debe ser proporcional con el objetivo de la política pública que alimentan, y entonces tener una clara finalidad. Es ésta última la que determinará luego si los datos están o no correctamente cedidos entre las distintas dependencias, buscando que de ninguna forma el tratamiento (y por lo tanto la afectación a la privacidad) sea *desproporcionado* con respecto al objetivo original buscado[59].

[59] Esta misma lógica será la que guiará el principio general de interpretación restrictiva de las excepciones justamente para asegurar el espíritu protector de la norma, que veremos más adelante.

Y entramos así en la segunda cuestión que funciona como límite claro al accionar estatal: aquella relativa al principio de finalidad. Este principio establece que los datos personales sólo pueden ser recabados y utilizados únicamente para los fines específicos y legítimos para los que fueron recolectados, que además debe ser explícito y de duración limitada[60]. Tiene una prevalencia importante en los estándares internacionales y las legislaciones regionales avanzadas en la materia. Por ejemplo, la regulación del Reino Unido[61] establece que los datos personales serán "recogidos con fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines", aclarando que no se considera incompatible cuando sea para fines de archivo en interés público, estadísticos o de investigación científica e histórica. El objetivo de esta limitación es "garantizar la claridad y transparencia en las razones para obtener los datos personales y que lo que se haga con ellos esté en línea con las expectativas razonables del caso. Funciona no sólo para ordenar la acción de los responsables del tratamiento sino también para asistir a los titulares en su derecho de información: entender cómo se usan sus datos, decidir si quieren compartirlos y hacer valer sus garantías cuando corresponda. Es fundamental para construir confianza pública en cómo se utilizan. De hecho, existen vínculos claros con otros principios, en particular los de equidad, legalidad y transparencia, en tanto promueve que el procesamiento sea justo, lícito y transparente. Y si utilizas datos con fines injustos, ilegales o 'invisibles', es probable que sea una violación de ambos principios" (art. 5.1.b, traducción propia).

En el mismo sentido, los Principios sobre privacidad de la OEA[62] establecen como principio fundamental para el tratamiento y conservación de datos personales su tratamiento y conservación limitados: por un lado, establecen que deben ser tratados y conservados solamente de una manera legítima que no sea incompatible con la finalidad para la cual fueron recopilados y, por otro, que no deben conservarse más allá del tiempo necesario para cumplir su finalidad y de conformidad con la legislación nacional correspondiente. Sobre la primera de estas cuestiones, es decir el principio de finalidad, agrega que el propósito debe ser debe ser determinado, específico, explícito y legítimo, de manera tal que el tratamiento y la conservación

[60] Access Now, "La creación de un marco para la protección de datos: una guía para los legisladores sobre qué hacer y qué no", 2018.
[61] Se trata de una regulación propia en materia de protección de datos personales, aunque muy similar al Reglamento General de Protección de Datos de la Unión Europea. Ver https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-protection-principles/a-guide-to-the-data-protection-principles/the-principles/purpose-limitation/
[62] OEA, Op. Cit., parte II, principio 4, pp. 41 y ss.

sean compatibles con las expectativas razonables de las personas (en la misma línea que lo regula el Reglamento General de Protección de Datos de la Unión Europea -RGPD-[63]). De esta manera, no deben tratarse ni conservarse datos que no sean compatibles con aquellas para las cuales se hayan recopilado, excepto con el conocimiento o consentimiento del titular o por mandato de la ley para, por ejemplo, fines de investigación o archivo históricos.

La legislación argentina también lo incluye. La ley 25.326 establece por un lado que "Los datos personales que se recojan a los efectos de su tratamiento deben ser ciertos, adecuados, pertinentes y no excesivos en relación al ámbito y finalidad para los que se hubieren obtenido" (art. 4, inc. 1) y, por otro, que "Los datos objeto de tratamiento no pueden ser utilizados para finalidades distintas o incompatibles con aquellas que motivaron su obtención" (art. 4, inc. 3). Incluso, la explicación de la finalidad deberá estar incluida entre la información brindada a los titulares al solicitar su consentimiento para recabar datos (art. 6) o, justamente, para su cesión (art. 11).

La doctrina es clara al respecto: "La recolección de los datos, debe responder a una finalidad o propósito predeterminado, que se identificará con el interés legítimo de quien recaba los datos para su tratamiento, propósito que no puede ser modificado sin contar con un nuevo consentimiento del interesado"[64]. A la vez, "Todos los datos que se recopilen deben ser adecuados, pertinentes y no excesivos en relación al ámbito y finalidad para la que fueron recogidos."[65].

En este sentido, el decreto 1558/2001 que reglamenta la ley especifica que "para determinar la lealtad y buena fe en la obtención de los datos personales, así como el destino que a ellos se asigne, se deberá analizar el procedimiento efectuado para la recolección y, en particular, la información que se haya proporcionado al titular de los datos". Agrega que, cuando la obtención de los datos es lograda por interconexión o tratamiento de alguna clase de bancos de datos, se debe "analizar la fuente de información y el destino previsto por el responsable o usuario para los datos personales obtenidos", es decir verificar su propósito original, y que "el dato que hubiera perdido vigencia respecto de los fines para los que se hubiese obtenido

[63] El Reglamento General de Protección de Datos (en adelante RGPD o GDPR, por sus siglas en inglés), es el principal instrumento jurídico de regulación y protección de datos personales de la UE y, a pesar de tener lagunas y aspectos perfectibles, es tomado muchas veces como modelo a nivel global por ser una de las legislaciones más avanzadas y con mejores estándares en términos de derechos humanos.

[64] Basterra, M., *Protección...*, Op. Cit., pág. 369, con cita a Travieso y Moreno, "La Protección de los datos personales y de los sensibles en la ley 25.326", LL, 14/7/2006, p.1.

[65] Ibidem.

o recolectado debe ser suprimido por el responsable o usuario sin necesidad de que lo requiera el titular de los datos.". Corresponde a la Dirección Nacional de Protección de Datos Personales, hoy dentro de la Agencia de Acceso a la Información pública, controlar de oficio o a pedido del afectado el cumplimiento de este precepto y aplicar sanciones si corresponde.

Así vemos que, según la norma, el Estado sólo puede recabarlos en la medida en que resulten necesarios y proporcionales para el ejercicio de sus funciones, con el **consentimiento** del titular en las condiciones antes descritas, **y no podrá utilizarlos con otros objetivos, salvo que medie un nuevo consentimiento del titular.** Sobre este punto es importante agregar que la prohibición funciona para todos los organismos del Estado, por lo que los datos tampoco podrán ser cedidos entre distintas dependencias si no se respeta la finalidad original con la que fueron recabados.

Sin embargo, es necesario complementar estas disposiciones con el artículo 11 de la ley, relativo específicamente a la **cesión** de datos -en la que profundizaremos en el próximo capítulo de este informe-. Refuerza 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", a la vez que presenta una serie de excepciones al requisito del consentimiento: que sea dispuesto por una ley especial (la de Acceso a la Información Pública, por ejemplo[66]), que se trate de los mismos supuestos en los que no se requiere consentimiento para el tratamiento (art. 5.2 antes desarrollado), que se realice entre dependencias del Estado "en forma directa, en la medida del cumplimiento de sus respectivas competencias", se trate de datos personales relativos a la salud y sea necesario por razones de salud pública, o si se disocia la información de modo que los titulares no sean identificables.

De esta manera, 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

[66] Así lo entendió la DNPDP en su dictamen en el caso "Pane, Juan Pablo c/ EN - Mo Desarrollo Social s/ amparo ley 16.986", expte. 15374/2020, con cita a previas al informe de la DNDP IF-2020-54444836-APN-DNPDP#AAIP y a la resolución de la AAIP RESOL-2020-231-APN-AAIP.

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, ya no sólo con el principio general del consentimiento para el tratamiento y la cesión sino, 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 es no: como dijimos, 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 es genérica y la evolución interpretativa no tan lineal. Existen numerosos casos donde se disputa el límite de las excepciones a estas cuestiones, algunos actualmente en litigio judicial.

iii. La necesidad de una reforma normativa sobre la cesión estatal

Si bien es clara la necesidad de contar con información para elaborar políticas públicas adecuadas, el tratamiento de datos por parte del sector público requiere de una regulación más extensa y precisa, con mayores salvaguardas y limitaciones[67].

[67] En este capítulo nos limitamos a la necesidad de reformas normativas sobre la cesión de datos entre organismos del Estado, pero desde la Fundación Vía Libre nos pronunciamos en repetidas oportunidades sobre una agenda más amplia de modificaciones e incorporaciones que deberían implementarse. A modo de ejemplo, en el capítulo 4 de este documento abordamos la necesidad de introducir cambios sobre la Autoridad de Aplicación y remitimos a los comentarios enviados al PEN durante la consulta pública por el último proyecto de ley presentado.

En este escenario consideramos fundamental y urgente reformar la legislación argentina sobre la cesión de datos entre organismos del Estado y la cuestión del consentimiento. Entre otras cuestiones, es indispensable restringir normativamente la ventana de arbitrariedad que habilitan las excepciones tal y como están redactadas actualmente. Con este objetivo, entendemos como lineamientos principales la necesidad de incorporar limitaciones para el tratamiento de datos personales, en especial cuando la base de legitimación sea el interés público; establecer pautas para la cesión de datos entre entidades públicas y entre éstas y empresas y sociedades del Estado, tanto para el caso de datos personales como para datos sensibles.

Con este objetivo, incluimos como anexo de este documento una propuesta de redacción para un artículo de ley que refleje estas previsiones, elaborado en octubre de 2023 en conjunto con la organización Access Now[68].

[68] https://www.accessnow.org/

03.

Uso y abuso de los datos personales por parte del Estado

Uso y abuso de los datos personales por parte del Estado

i. Cesión de datos entre oficinas del Estado. La postura de la AAIP y el caso Torres Abad

Naturalmente, el Estado obtiene permanentemente datos personales de los ciudadanos y ciudadanas. Como ya explicamos en los capítulos precedentes, constituye un paso esencial para la planificación y ejecución de políticas públicas de distinta índole bajo el supuesto de que cuanto más conozca a la población más precisas y acertadas serán las políticas

Sin embargo, esto no significa un cheque en blanco para recabar cualquier dato en cualquier situación, ni para cederlo sin más a cualquier área del Estado que pueda estar interesada[69]. Vimos ya que los límites generales tienen que ver con cuestiones fundamentales: por un lado, el consentimiento, obtenido en las condiciones que establece la ley; y, por otro, el respeto del principio de finalidad, es decir que cualquier actividad que realice el Estado con esos datos debe ser con apego a la finalidad con la que fueron obtenidos originalmente, salvo que medie un nuevo consentimiento.

Otro requisito esencial es la debida seguridad de la información que tiene en su poder, cuestión sobre la que profundizaremos más adelante.

Volviendo a los supuestos “esperables” de tratamiento de datos personales por parte del Estado, sabemos que pueden estar basados en obligaciones legales, interés público o simplemente el ejercicio del poder público para el cumplimiento de

[69] Por supuesto tampoco lo es para las transferencias al sector privado ni a otros Estados, pero en este trabajo nos centraremos en aquellas dentro del propio Estado Nacional argentino.

sus funciones. Como mencionamos, el art. 11 de la Ley 25.326 refiere a la cesión de datos, que puede ser entendida como "el traslado de todo o parte de una base de datos personales a otra basta de datos"[70]. De esta manera, "(...) cuando se cede un dato personal no se altera la titularidad del mismo, sino que simplemente se lo pone en conocimiento de otra u otras personas, por alguno de los procedimientos aptos a tal efecto, tales como la transferencia, la consulta, la transmisión o la interconexión. La transmisión de datos es la operación que más riesgos puede entrañar para los titulares de informaciones personales por cuanto implica su difusión más allá de los límites del archivo, registro o fichero en el que se encuentran almacenadas.".[71]

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** [distinto, por ejemplo, al acceso a información pública que no requiere ningún interés calificado] **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 que el consentimiento no es necesario, entre otros supuestos, cuando "Se realice entre dependencias de los órganos del Estado en forma directa, en la medida del cumplimiento de sus respectivas competencias". Así, el texto legal no agrega en este punto mayores requisitos para el tráfico de datos dentro del propio Estado Nacional.

Sin embargo, es indispensable interpretarlo a la luz del principio de finalidad en el uso de los datos recabados del art. 4 y los límites al requisito del consentimiento del titular del art. 5 para su obtención. Las excepciones deben ser interpretadas siempre con carácter restrictivo, en tanto el consentimiento "(...) es uno de los elementos determinantes para que sea lícita la recolección de datos o la fase del tratamiento del dato en el momento en que el consentimiento sea requerido"[72].

En otras palabras, así como el Estado no puede obtener cualquier dato sin consentimiento, tampoco es válida cualquier cesión de datos dentro del Estado, ni su uso por parte del receptor sin nuevo consentimiento del titular. Esto implica que no pueden ser cedidos o utilizados para fines distintos con la única justificación de, por ejemplo, el interés público.

---

[70] Palazzi, Pablo A.*, La protección de los datos personales en la Argentina: La let 25.326 de protección de datos persoanles y habeas data comentada y anotada con jurisprudencia,* Ed. Errepar, Buenos Aires, 2004, pág. 81

[71] Basterra, M., *Protección...*, Op. Cit., pág. 411.

[72] Ibidem, p. 412 y ss.

Esta posición también se fue consolidando a través de las decisiones de la Agencia de Acceso a la Información Pública que, como mencionamos, tiene en su órbita la **Dirección Nacional de Protección de la Datos Personales (DNPDP)** con competencia en la materia.

Esta última consolidó durante la última década su postura al respecto. Cuando fue preguntada por la pertinencia técnica de la cesión de datos solicitada por otros organismos estatales, entendió que debe hacerse siempre un análisis con cuatro pasos.

En primer lugar, estudiar la calidad del dato en el sentido del art. 4 de la ley, es decir verificar que no haya una prohibición legal para su tratamiento, que no esté especialmente protegido (por ejemplo, es el caso de los datos sensibles).

Una vez saldado, como segundo paso debe evaluarse **a) si es necesario y adecuado cederlo según el principio de proporcionalidad y b) si es pertinente hacerlo según la competencia de los organismos y la finalidad con que el dato fue recabado originalmente.** En este sentido la DNPDP entendió que "El **principio de finalidad** es determinante de la licitud de todo tratamiento de datos personales, y tiene una especial implicancia con el concepto de competencia del derecho administrativo, pues la competencia del organismo es la que determinará la finalidad a la que debe destinar el tratamiento de sus datos, y es un claro límite al tratamiento de datos personales por dicho ente. (...) se debe concluir que **la cesión de datos debe efectuarse siempre dentro del marco del ejercicio de las funciones propias (competencias) de los organismos (cedente y cesionario)** (...) y los datos a intercambiar sean los estrictamente necesarios para la finalidad prevista."[73]. En otra oportunidad[74] ahondó sobre este principio general explicando que la cesión sólo puede suceder en tanto sea **necesaria** para el cumplimiento de los fines relacionados con **el interés legítimo** del cedente y el cesionario (cuando se trata de dependencias públicas, éste se subsume en la competencia que legalmente se les haya atribuido) en línea con el art. 11 de la ley. En el mismo sentido, recalcando el principio de necesidad, recordó que "la cesión deberá contener solamente los datos estrictamente necesarios para que el cesionario pueda llevar adelante el tratamiento que declara al efectuar la petición (...)" por lo que **"deberá analizarse si los datos resultan necesarios, adecuados (principio de proporcionalidad) y pertinentes (principio de pertinencia) para la competencia del cesionario, lo que**

[73] Dictamen DNPDP N° 19/13 entre otros.
[74] Dictamen DNPDP N° 17/13.

implica verificar la calidad de los datos a ceder en relación con la competencia del organismo cesionario y la finalidad esgrimida para la requerir la cesión".

Finalmente, para completar el análisis, la DNPDP entendió que es necesario, como siguientes pasos, verificar que no se estén afectando derechos al momento de cederlo y que se cumplan los principios generales que deben regir siempre el tratamiento de datos para que sea lícito (inscripción en bancos de datos que cumplan con el estándar debido de seguridad y confidencialidad, la posibilidad del titular de ejercer sus derechos de acceso, rectificación, cancelación y/o oposición, etc.).

En este escenario es relevante destacar el caso conocido como "Torres Abad"[75], que se encuentra, al momento de redacción de este informe, pendiente de resolución ante la Corte Suprema de Justicia de la Nación. Iniciado en 2016, gira justamente en torno al uso de datos personales por parte de una entidad estatal distinta a la que los recolectó originalmente y con una finalidad diferente.

En aquel año, mediante la Resolución Nº 166 E/2016, se aprobó el Convenio Marco de Cooperación entre la Administración Nacional de Seguridad Social (ANSES) y la Secretaría de Comunicación Pública, mediante el cual la primera se comprometía a remitir periódicamente su base de datos a la segunda, dependiente de la Jefatura de Gabinete de Ministros, con el objeto de que instrumentara diversas políticas de comunicación pública para "mantener informada a la población". Al tomar conocimiento, la ciudadana Carmen Torres Abad inició una acción judicial con el objetivo de preservar la confidencialidad de la información brindada y que no se utilice para finalidades distintas a aquellas que tiene la ANSES[76].

Torres Abad entendió que el uso que quería hacer la Administración Pública de sus datos implicaba una "extralimitación" en tanto es necesario nuevamente el consentimiento si se trata de una finalidad distinta a la original, máxime cuando los datos cedidos no encuadran en ninguna excepción al consentimiento del titular. Por su parte, el Poder Ejecutivo sostuvo que los datos que pretendían cederse entre la ANSES y la Secretaría de Comunicación sí encuadraban en las excepciones de la ley al consentimiento por parte de los titulares, específicamente en las previsiones de los arts. 5.2.b (necesario para el ejercicio de una obligación legal) y 5.2.c. (datos

[75] "Torres Abad, Carmen c/ EN-JGM s/Habeas Data", Expte. No 49.482/2016/CA1. Actualmente pendiente de resolución ante la CSJN.

[76] Para más información sobre el recorrido judicial del caso ver https://palabrasdelderecho.com.ar/articulo/2076/El-Estado-no-puede-utilizar-sin-consentimiento-datos-personales-con-fines-de-propaganda-

nominativos: nombre, documento nacional de identidad, identificación tributaria o previsional, ocupación, fecha de nacimiento y domicilio).

En primera instancia la acción fue rechazada, pero la Cámara le dio la razón: ordenó a la ANSES que se abstuviera de ceder en el marco del convenio mencionado todos aquellos datos suyos que excedieran los referidos el art. 5.2.c de la ley.

Para arribar a esta conclusión hizo el siguiente razonamiento en torno a los argumentos del Estado: por un lado, para encuadrar en la excepción al consentimiento del titular por ser necesarios "para el ejercicio de funciones propias del Estado o en virtud de una obligación legal", debería tratarse de objetivos "que se vinculen con una finalidad de defensa nacional, seguridad pública o represión de delitos, tal como lo exige la doctrina especializada", en la misma línea que nos referimos anteriormente[77]. Sin embargo, en el caso de autos la oficina que los recibiría depende de Jefatura de Gabinete de Ministros, que no tiene ninguna competencia de este tipo, y las finalidades declaradas en la resolución que lo habilita tenían que ver únicamente con "mantener informada a la población" o "la identificación, evaluación y análisis de problemáticas o temáticas de interés en cada localidad del país". Así descarta la posibilidad de ampararse en esta excepción. Explica "Que la excepción que invoca la demandada, se refiere a datos de carácter personal que hayan sido recabados para el desempeño de funciones propias de la organización estatal. Se ha dicho que '[e]n la práctica, [ello] exime al Estado de obtener el consentimiento de los titulares de aquellos para proceder a las operaciones de tratamiento de los mismos, ya que la fórmula resulta tan amplia e imprecisa que no pone límites razonables a dichas operaciones' (PEYRANO, Guillermo F., Régimen legal de los datos personales y hábeas data, Buenos Aires, Lexis Nexis, 2002, pág.. 83). Es decir, que 'esta liberación 'en blanco' aparece como excesiva, por cuanto determinados datos personales y determinados organismos necesitan el consentimiento de los titulares de los datos para poder someter esos informes personales a ciertas operaciones de tratamiento. El consentimiento de la registración de ciertos datos personales, denunciándolos voluntariamente a ese efecto por el mismo titular, en forma expresa, libre e informada, no significa que dicho consentimiento se haya prestado para proporcionar o transferir esos datos a terceros o para su utilización con una finalidad distinta a la perseguida con la registración" (PEYRANO, Régimen legal... Op. cit., pág. 83)." (considerando IX del fallo).

[77] Basterra, M., "El consentimiento...", Op. Cit.

Con respecto al segundo argumento, sobre la prescindencia de un nuevo consentimiento por tratarse de datos para los que según la ley no hace falta, entiende que procede pero de manera limitada: es cierto que no es necesario obtener un nuevo consentimiento cuando se trate únicamente aquellos contemplados en el art. 5.2.c (nombre, apellido, etc.), pero este listado es taxativo y, por lo tanto, todos aquellos que no estén incluidos en el texto legal no pueden ser utilizados para otra finalidad sin volver a consultar al titular. En particular, en este caso se pretendía compartir información como números de teléfono y direcciones de correo electrónico, que exceden los mencionados.

Es así que la Cámara decide, entonces, impedir la cesión de datos sin nuevo consentimiento de la titular, excepto aquellos expresamente previstos en este artículo de la ley. **Es interesante destacar cómo a través de este razonamiento pone de relieve el principio de finalidad como rector de las cesiones entre organismos del Estado, a la vez que resuelve la cuestión del consentimiento a partir de la interpretación siempre restrictiva del alcance de las excepciones.**

El Estado apeló esta decisión y se encuentra hoy pendiente de resolución ante la CSJN. Sin embargo, ya se pronunció la Procuración General de la Nación recomendando a la Corte confirmar el fallo de Cámara. Es que entendió que, de lo contrario, se afectaría la autodeterminación informativa de los ciudadanos, es decir el derecho de cada uno a decidir por sí mismo sobre la publicidad, divulgación y uso de sus datos personales, que a su vez es condición para el ejercicio de otros derechos y por lo tanto debe ser estrictamente garantizado.

Nos interesa destacar que, para resolver, hace énfasis nuevamente en la necesidad de **interpretar de manera restrictiva las potestades que la ley en cuestión da al Estado frente a los ciudadanos,** especialmente en los supuestos que permite omitir el consentimiento de los titulares, y de **interpretarlas de manera armónica** con el resto del plexo normativo. En concreto sostiene que "una interpretación de dicha norma [*la excepción del art. 5.2.b sobre datos necesarios para el ejercicio de las funciones*] desvinculada del ordenamiento jurídico en el que se engarza podría llevar a pensar que el Estado puede efectuar el tratamiento de cualquier dato personal sin el consentimiento del titular, sin embargo, estimo que a la luz de la protección y garantía que la Constitución Nacional ha proporcionado al titular de los datos –como se expuso-, tal norma tiene que ser interpretada con criterio restrictivo y armonizada con el resto del bloque de legalidad."[78]. En este sentido, sostiene que debe ser interpretado en consonancia con el art. 11.3.c.

[78] Dictamen PGN, acápite V, p. 15.

(excepción al consentimiento cuando sea para cesiones entre organismos en el cumplimiento de sus competencias), recordando que esta disposición **busca proteger "(...) a las personas a las que se refieren los datos y no a las instituciones -públicas o privadas- que los registren o almacenen** (Fallos: 329:5239)"[79].

Este caso también resulta ilustrativo por el sentido de la argumentación del Estado. Es frecuente que la cesión indiscriminada aprovechando las ventanas que dejan las excepciones de la ley, se fundamente en una "eficientización" de los recursos. Dicho de otro modo, sería más "racional" optimizar los recursos (datos) que la Administración Pública ya tiene, aprovechándolos para distintos objetivos sin necesitar volver a recolectarlos o requerir el consentimiento de los titulares. Al contestar la demanda de Torres Abad, el Estado sostuvo que "(...) todos los órganos del Estado, independientemente de las competencias asignadas a cada uno de ellos, se interrelacionan y colaboran entre sí para lograr el fin común principal de la actividad administrativa del Poder Ejecutivo, esto es, ejecutar las leyes, gestionar para el bien común, atender al interés público y satisfacer las necesidades de la sociedad. No resultan compartimentos estancos ni extraños entre sí, de ahí que los órganos se conectan en virtud de las relaciones de jerarquía, subordinación y/o tutela" (pág. 29). También que la cesión de números telefónicos y direcciones de correo electrónicos era necesaria para "(...) una comunicación más eficiente y fluida con la población para acercar la información de manera más adecuada a los ciudadanos, de acuerdo a sus intereses y necesidades. Es decir, se podrá hacer llegar a cada ciudadano la información que le puede interesar recibir, de una manera más clara y directa, a un menor costo" (pág. 41), es decir con mayor eficiencia.

Sin embargo, la Cámara de Apelaciones fue contundente al rechazar de plano este tipo de argumento. Sostuvo textualmente: "En este contexto, resulta necesario advertir -en primer lugar- que los datos que la Administración pretende ceder (en concreto el número telefónico y la dirección de correo electrónico) se efectúa para llevar a cabo una finalidad distinta de aquella por la cual la ANSES recolectó esos datos. Es decir, que este último organismo puede requerir del interesado el número telefónico y su dirección de correo electrónico a los fines de llevar a cabo una eficiente comunicación con el administrado en relación con trámites administrativos (de naturaleza previsional) que lo involucran. En cambio, la cesión de esos datos a la Secretaría de Comunicación Pública tendría como fin, tal como está indicado en la resolución administrativa, lograr objetivos o finalidades distintas a las que

[79] Dictamen PGN, acápite V, p. 20.

oportunamente llevaron a la ANSES a requerirlos." (Cons. XI). Vemos claramente cómo hace primar el apego al principio de finalidad que establece la ley por sobre la "conveniencia" en términos de eficacia y "optimización de recursos", siempre con el objetivo de proteger los derechos de los ciudadanos.

Otro caso con una discusión jurídica similar es el que se encuentra actualmente tramitando ante la Cámara de Apelaciones del fuero Contencioso Administrativo Federal en torno a la **Decisión Administrativa nº 431/2020** del Jefe de Gabinete de Ministros de la Nación, dictada durante la emergencia sanitaria por COVID-19[80]. Esta disposición establece *el deber* de transferir, ceder o intercambiar entre las distintas dependencias de la Administración Pública Nacional "los datos e información que, por sus competencias, obren en sus archivos, registros, bases, o bancos de datos, con el único fin de realizar acciones útiles para la protección de la salud pública, durante la vigencia de la emergencia en materia sanitaria ampliada por el Decreto N° 260/20, con motivo de la pandemia por coronavirus COVID-19.". No requiere ningún consentimiento del titular de los datos que vayan a intercambiarse. Se ampara para esto tanto en el art. 5.2.b de la ley (cuando se recaben para el ejercicio de funciones propias de los poderes del Estado, o en virtud de una obligación legal) como en el art. 11.3.c (cesión en cumplimiento de respectivas competencias), amparándose en la obligación legal o facultades extraordinarias que le daría el contexto de la emergencia sanitaria al momento de su dictado. Como resultado termina habilitándose, entre otras cuestiones[81], que puedan hacerse cesiones de datos dentro del Estado para fines distintos a los que fueron recolectados, que el titular no sea informado de esa posibilidad al brindar los datos ni que se vuelva a solicitar su consentimiento al cederlos para que sean usados con otro propósito.

Vemos cómo el uso amplio de los supuestos excepcionales termina por desnaturalizar el espíritu restrictivo de la ley en cuanto al uso de datos por parte del Estado (de hecho parte del objetivo de la acción judicial relatada es la inconstitucionalidad de la excepción del art. 5.2.b en este caso). Esto se vuelve aún más grave si tenemos en cuenta que la disposición sigue vigente y no se eliminó ninguna base de datos creada a partir de las cesiones efectuadas. En este escenario, la Fundación Vía Libre se presentó *como amicus curiae* recordando

[80] "Andrade, Eliana y otro C/ EN - Jefatura de Gabinete de Ministros de la Nación – DECAD 2020/431 - Ley 25.326 s/ Amparo Ley 16.986", Expte. 18198/2023. Pendiente de resolución ante la Cámara Contencioso Administrativa Federal. Se trata de un caso inciado por el Observatorio de Derecho Informático Argentino (O.D.I.A.).
[81] Para más detalles ver punto VI. de la acción de amparo interpuesta.

las normas nacionales e internacionales aplicables al caso y los estándares interpretativos que deberían tenerse en cuenta.[82]

Finalmente, vale mencionar que en sentido similar se pronunciaron los tribunales de países con sistemas jurídicos similares. Es el caso, por ejemplo, del fallo del Tribunal Constitucional España que declaró inconstitucional la norma que admitía la comunicación de datos entre organismos públicos sin consentimiento cuando hubieran sido "obtenidos o elaborados por una con destino a otra (art. 21 inc. 2)"[83] que mencionamos más atrás. Para arribar a esta conclusión entendió que "el interesado debe ser informado tanto de la posibilidad de cesión de sus datos personales y sus circunstancias como del destino de estos, pues sólo así será eficaz su derecho a consentir, en cuanto facultad esencial de su derecho a controlar y disponer de sus datos personales. Para lo que no basta que conozca que tal cesión es posible según la disposición que ha creado o modificado el fichero, sino también las circunstancias de cada cesión concreta. Pues en otro caso sería fácil al responsable del fichero soslayar el consentimiento del interesado mediante la genérica información de que sus datos pueden ser cedidos (...)". En el mismo sentido sostuvo que "el derecho a consentir la recogida y el tratamiento de los datos personales (art. 6 L.O.P.D.) no implica en modo alguno consentir la cesión de tales datos a terceros, pues constituye una facultad específica que también forma parte del contenido del derecho fundamental a la protección de tales datos. Y, por tanto, la cesión de los mismos a un tercero para proceder a un tratamiento con fines distintos de los que originaron su recogida, aun cuando puedan ser compatibles con éstos (art. 4.2 L.O.P.D.), supone una nueva posesión y uso que requiere el consentimiento del interesado. Una facultad que sólo cabe limitar en atención a derechos y bienes de relevancia constitucional y, por tanto, esté justificada, sea proporcionada y, además, se establezca por Ley, pues el derecho fundamental a la protección de datos personales no admite otros límites"[84].

[82] Para más información sobre el caso y acceder a la presentación hecha por Vía Libre, ver https://www.vialibre.org.ar/covid-datos-personales-y-estado-nos-presentamos-como-amigos-del-tribunal/
[83] Peyrano, G., F., Régimen legal de los datos personales y hábeas data, Lexis Nexis, Bs. As., Argentina, 2002, pág. 136.
[84] Tribunal Constitucional de España. Pleno. Sentencia 292/2000, Op. Cit.

Un ejemplo concreto

En febrero de 2022, salió a la luz que los laboratorios forenses de California estaban usando ADN de sobrevivientes de agresiones sexuales para investigarlos por delitos no relacionados[85]. Fue gracias al relato de un fiscal del distrito de San Francisco que encontró esta prueba dentro de un largo informe sobre una mujer acusada de un delito contra la propiedad, como una forma de identificarla. Para peor, mencionó que aparentemente se trata de una "búsqueda rutinaria" que se realiza en los laboratorios forenses del Departamento de Policía de esa localidad, es decir dentro de los datos que el propio Estado almacena a partir de sus investigaciones criminales.

Además de la vulneración de la máxima intimidad de las personas, una práctica de este tipo tiene como efecto directo la disuasión de otras posibles víctimas de denunciar delitos de este tipo. En ejemplos como este vemos el impacto directo en un gran abanico de derechos, no sólo -aunque indiscutiblemente- en la privacidad.

ii. La seguridad de la información en poder del Estado. Filtraciones, vulnerabilidades y la falta de respuesta adecuada.

Es evidente hasta acá que el Estado puede -e incluso en muchos supuestos *debe*- tener en su poder datos personales de los ciudadanos. Sin embargo, existen fuertes límites en la legalidad de la recolección y tratamiento de esa información, partiendo del consentimiento de aquellos e incluyendo las reglas para ser compartidos entre dependencias del mismo Estado.

Pero llegados a este punto necesitamos mencionar un universo más de deberes estatales en torno a la garantía del derecho a la privacidad: **nos referimos a la seguridad referida a aquella información que legítimamente puede poseer y tratar.**

[85] Ver, entre otros portales de noticias, https://apnews.com/article/crime-california-san-francisco-sexual-assault-3dcd00bf0522ce7c39bb2a7ec53cf7d317/02/2022.

Partimos de la base de la exigencia que la propia ley plantea: por un lado, su art. 9 obliga al responsable o usuario del archivo de datos a "adoptar las medidas técnicas y organizativas que resulten necesarias para garantizar la seguridad y confidencialidad de los datos personales, de modo de evitar su adulteración, pérdida, consulta o tratamiento no autorizado, y que permitan detectar desviaciones, intencionales o no, de información, ya sea que los riesgos provengan de la acción humana o del medio técnico utilizado", a la vez que prohíbe registrar datos personales en registros que no reúnan las condiciones técnicas mínimas de integridad y seguridad.

Seguidamente establece el secreto profesional de quienes intervengan en cualquier fase del tratamiento de datos personales sobre éstos -incluso una vez terminada su relación laboral-, que sólo podrá ser relevado por resolución judicial o cuando existan razones fundadas vinculadas con "la seguridad pública, la defensa nacional o la salud pública" (art. 10).

La cuestión de las medidas adoptadas para la seguridad es tan importante que incluso es parte de la información que se debe aportar al inscribir un registro, archivo, base o banco de datos, sea público o privado (art. 21). En este sentido, son potestades del órgano de aplicación de la ley (que abordaremos más adelante) "controlar la observancia de las normas sobre integridad y seguridad de datos por parte de los archivos" así como solicitar "antecedentes, documentos, programas u otros elementos relativos al tratamiento de los datos personales" a las entidades públicas o privadas, que deberán (cfr. art. 29 incs. e y f).

Sin embargo, la ley en su formulación actual no contempla los incidentes de seguridad de los datos ni cómo proceder ante ellos, cuestión sumamente relevante en contexto de avance tecnológico permanente en el que vivimos[86]. Nos referimos, por ejemplo, a vulnerabilidades de los sistemas y en consecuencia *hackeos*, filtraciones, secuestro o robo de datos, suplantación de identidad, fraude, entre otras.

Es fundamental entender el escenario: los incidentes de seguridad, tales como *hackeos* o "*data breaches*" (fugas de información) crecieron en los últimos años, en parte como respuesta a "múltiples factores propios de la industria de

[86] Si bien no ahondaremos en este informe en las vulnerabilidades en sí mismas, remitimos en este punto al informe específico elaborado en 2022 por la Fundación Vía Libre junto con Democracia en Red y O.D.I.A., "Panorama general sobre la seguridad de la información, las vulnerabilidades y los incidentes en Argentina" donde nos referimos los distintos tipos de vulnerabilidades, cómo y qué derechos afectan, y la situación de los reportes. Está disponible para su descarga en https://drive.google.com/file/d/1y5ruA9d_HOeIN42rx03bmUkt6NIW3jt0/view

procesamiento de datos: la capacidad técnica para procesar datos de manera ilegítima evoluciona con la misma potencia de la capacidad de procesamiento legítimo"[87]. Recientemente publicó su informe de gestión 2023 la Unidad Fiscal Especializada en Ciberdelincuencia[88] donde señala un alza continua de los delitos informáticos, principalmente de fraude en línea, usurpación de identidad y secuestro o robo de datos (por ejemplo mediante técnicas de ingeniería social -*phishing*-). Es importante señalar que este informe se basa en las denuncias realizadas, pero es sabido que sólo un porcentaje se reportan: son frecuentes las políticas de persecución penal a quienes identifican, denuncian y reportan vulnerabilidades informáticas[89].

A este aumento objetivo se le suma la frecuente subestimación a nivel general. Es que socialmente suele ser difícil la comprensión de lo que pueden significar estos incidentes en términos de derechos y vulneración a la privacidad. Explica la doctrina que "el foco de dicha actividad son por lo general datos calificados como críticos o sensibles e información calificada para la organización víctima del incidente. La pérdida de esos datos por lo general conduce a su utilización para llevar adelante actividades delictivas, tales como fraude financiero, robo de identidad, afectaciones a la propiedad intelectual, espionaje e inteligencia, extorsión, etcétera. Dada la cotidianidad de la ocurrencia de este fenómeno, los individuos se han vuelto progresivamente indiferentes a su existencia (...) Esta progresiva indiferencia a la severidad y trascendencia que poseen los incidentes de seguridad se debe en parte a la pérdida progresiva y relajamiento en la noción y percepción de la privacidad e intimidad personal"[90].

Esto se ve habilitado por no tener estos incidentes en general una manifestación de daño material concreto: "La falta de tangibilidad del daño latente que implica la pérdida de datos sensibles y críticos por fugas de información, cuyas consecuencias dañosas para sus titulares pueden presentarse espaciadas temporalmente al incidente hace que la sensación de peligro sea percibida a la ligera; el robo de algo material causa un mayor impacto o impresión que la pérdida

[87] Faliero, J. C., *La protección de datos personales*, Ed. Ad-Hoc, Buenos Aires, 2019, p. 171
[88] Para más información y acceso al Informe ver https://www.fiscales.gob.ar/ciberdelincuencia/la-unidad-fiscal-especializada-en-ciberdelincuencia-senalo-un-alza-continua-de-los-delitos-informaticos-en-su-informe-de-gestion-2023/
[89] Para más información ver Fundación Vía Libre, Democracia en Red y O.D.I.A, "Reportantes de vulnerabilidades en sistemas digitales ante la ley penal argentina", 2022. Disponible en https://drive.google.com/file/d/1D-W5_UvRbZnlbdSA49k_ohScvPFMPXNP/view
[90] Faliero, J. C., Op. Cit. p. 168.

de algo inmaterial e intangible y sus consecuencias no se sienten de manera instantánea (...)"[91].

Si contemplamos que además la ley no prevé cursos de acción frente a los incidentes, el escenario es aún más complejo. La legislación comparada (el RGPD, por ejemplo) obliga, en caso de vulneración, a un informe que dé cuenta del hecho a la autoridad de control y, en algunos supuestos, a los titulares de los datos. En este sentido, en parte subsanando las lagunas legales, la Dirección Nacional de Protección de Datos Personales y la Agencia de Acceso a la Información Pública emitieron diversas disposiciones sobre el tratamiento y conservación de datos personales y las respectivas medidas de seguridad. En particular, la AAIP estableció mediante su resolución 47 del 2018 las "Medidas de seguridad recomendadas para el tratamiento y conservación de los datos personales en medios informatizados". Si bien se trata únicamente de disposiciones enunciativas ("recomendaciones"), establece pautas para a) la recolección de datos, b) el control de acceso, c) el control de cambios, d) el respaldo y la recuperación, e) la gestión de vulnerabilidades, f) la destrucción de la información, g) los incidentes de seguridad -donde corresponde elaborar un informe y enviar la notificación correspondiente a la autoridad de aplicación-, y h) para la definición de los entornos de desarrollo de los sistemas de información. Aún así, no existen hoy recursos apropiados para la mitigación de esos incidentes.

Disposiciones de este tipo son armónicas con los principios internacionales y la legislación más avanzada de otras regiones que rigen la materia, entre aquellos contenidos en el Convenio para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal, conocido como *Convenio 108* (vinculante para la Argentina), las directrices de la OCDE sobre privacidad[92] o los principios de la OEA antes citados, relevantes como criterios interpretativos en tanto se trata de altos estándares del derecho internacional de los derechos humanos en la materia.

Por ejemplo, el RGPD establece en su art. 5.1.f) que los datos siempre deben ser tratados garantizando "una seguridad adecuada (...), incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidentales, mediante la aplicación de medidas técnicas u organizativas

[91] Ibidem, pp. 168-169

[92] Organización para la Cooperación y el Desarrollo Económicos, "Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data", 1980, actualizado en 2013. Se trata de estándares internacionales no vinculantes para la Argentina pero sí relevantes para del derecho internacional de los derechos humanos sobre la temática.

adecuadas.". Las Directrices de la OCDE antes citadas, por su parte, establecen que "Los datos personales deben ser protegidos con salvaguardas razonables de seguridad contra riesgos tales como pérdida o acceso no autorizado, destrucción, uso, modificación o divulgación" ("Principio de salvaguardia de la seguridad", traducción propia). Por ejemplo, las limitaciones de uso y divulgación deberían ser reforzadas mediante medidas físicas (por ejemplo, bloqueo de puertas, uso de tarjetas de identificación), organizacionales (niveles de autoridad para acceder a los datos) y propias de los sistemas informáticos (como el cifrado o el seguimiento a amenazas de actividades inusuales y respuestas a ellas)[93].

Así, es evidente que los estándares internacionales y nuestra ley de Protección de Datos Personales exigen por parte del Estado y los responsables de las bases la garantía de máxima seguridad y confidencialidad. Pero, ¿por qué es tan importante esto? Para dimensionarlo es interesante traer a colación un caso reciente, que se suma a una larga lista de incidentes[94] que convierten la vulnerabilidad en un asunto estructural.

En octubre de 2021 se conoció que la base de datos del Registro Nacional de las Personas (RENAPER) había sufrido una vulneración de seguridad donde se extrajo información de los documentos nacionales de identidad como foto y número de trámite[95]. Los detalles sobre cómo se produjo son variados y contradictorios; de acuerdo a comunicaciones oficiales, se detectó el uso indebido de una clave otorgada al Ministerio de Salud de la Nación que permitió el acceso al sistema y la obtención de los datos.

Pese a numerosos intentos por parte de organizaciones de la sociedad civil y expertos y expertas en la materia, no ha sido posible obtener respuestas para esclarecer los hechos, conocer los sistemas de seguridad implementados, las políticas para el otorgamiento y administración de llaves de acceso. La negativa del RENAPER de dar respuesta a los pedidos de acceso a la información pública va en

[93] Ver CEPAL, Biblioguías, Gestión de datos de investigación. Disponible en https://biblioguias.cepal.org/c.php?g=495473&p=4398118#:~:text=Las%20limitaciones%20de%20uso%20y,informáticos%2C%20(como%20la%20cifración%20y (fecha de consulta: diciembre 2023).

[94] Nos referimos, por ejemplo, al conocido como "la gorra leaks" (2019), la filtración de la base de datos del Instituto de la Obra Social de las Fuerzas Armadas (2021), la vulneración de la base de datos de la Dirección Nacional de Migraciones (2020) y la filtración de datos del Ministerio de Salud (2021), solo para mencionar los más recientes.

[95] Ver, por ejemplo, https://www.clarin.com/tecnologia/filtracion-renaper-difunden-datos-sensibles-60-000-argentinos-piden-cerca-17-mil-dolares-dni_0_2eE_kXXBo.html.
Organizaciones de la sociedad civil nos pronunciamos con un comunicado conjunto disponible en https://www.accessnow.org/solicitud-suspension-tecnologias-procesamiento-masivo-datos-personales-argentina/ (28/01/22).

contra de la normativa nacional y opaca la transparencia con la que el Estado debería actuar.

En consecuencia se presentó una acción judicial individual[96], bajo la forma de *habeas data,* para conocer qué datos personales del actor estaban en poder del Renaper y si fueron objeto de los incidentes de seguridad que tomaron estado público, así como para saber qué medidas de seguridad de la información se tomaron en función de esas filtraciones, independientemente de que sus datos personales hayan o no estado involucrados. A pesar de que el Ministerio Público Fiscal entendió la respuesta que dio el RENAPER como "insuficiente y parcial" (se había limitado a entregar alguna información que constaba en sus bases sobre el actor y a negar sin mayor fundamento que haya sido parte de los datos vulnerados), la acción fue rechazada por el juez de primera instancia. Hoy el caso se encuentra pendiente de decisión ante la Cámara de Apelaciones en lo Contencioso Administrativo Federal. En este contexto Vía Libre se presentó como *amicus curiae*, entendiendo la relevancia del caso por la violación del derecho a la privacidad y protección de datos personales, así como el incumplimiento a las obligaciones que tiene el Estado en materia de seguridad de la información[97].

Este ejemplo reciente resulta particularmente ilustrativo para este informe en tanto pone de relieve la falta de medidas idóneas de seguridad de la información justamente dentro del organismo encargado, por definición, de la identificación registral de los ciudadanos. No sólo es importante limitar sus facultades para recolectar, almacenar, tratar y ceder datos personales -tal como venimos desarrollando hasta acá-, sino que resulta imprescindible demandar que adopte las medidas de seguridad exigidas por la normativa local e internacional, cumpliendo su deber legal, y cuente con recursos apropiados para la mitigación de los posibles daños.

Las filtraciones que sufrieron diversas reparticiones del Estado en el último tiempo nos hacen temer que sus sistemas son vulnerables. Dado el uso abusivo de las excepciones que permite la ley en estos asuntos hasta el punto de desnaturalizarla, y viendo que el accionar estatal suele aprovecharlo, entendemos necesaria una reforma normativa en este sentido. En concreto, consideramos indispensable precisar y profundizar los requisitos necesarios para que una cesión

[96] Se trata de un Habeas Data presentado por Pablo Palazzi en el fuero Contencioso Administrativo Federal. "Palazzi, Pablo c/ EN-Registro Nacional de las Personas S/Habeas Data", expte. 18307/2021.

[97] Para más información ver https://www.vialibre.org.ar/via-libre-se-presenta-como-amigos-del-tribunal-en-la-causa-contra-el-renaper/, 07/02/2024.

de datos entre dependencias estatales sea legítima. Además de las disposiciones actuales debería exigirse, como mínimo, 1) que la cesión sea indispensable para el cumplimiento de un fin público asignado por ley a la entidad receptora de los datos y que no pueda resolverse sin esos datos, 2) que la entidad receptora de los datos cuente con medidas de seguridad y protocolos adecuados para garantizar la integridad, disponibilidad y confidencialidad necesarios. Esto debe ir acompañado de una autoridad de control fuerte y autónoma con capacidad de defender los derechos de los ciudadanos -como veremos en el capítulo siguiente- así como de concientización sobre la gravedad de los posibles incidentes de seguridad. Es urgente la construcción de una cultura de protección de datos personales en la sociedad, que involucre tanto al Estado como a los ciudadanos, y que se sustente desde una perspectiva ética y de derechos humanos.

04.

La autoridad de aplicación

La autoridad de aplicación

i. El rol de una autoridad de aplicación

Los estándares internacionales colocan en cabeza de las autoridades de aplicación una gran cantidad de recomendaciones y potestades: ningún marco de protección de datos puede considerarse suficiente si no cuenta con un organismo que asegure su correcta observancia, desde monitorear la implementación de la norma hasta sancionar a quienes la incumplan.

Para esto, los más altos principios regionales e internacionales en la materia coinciden en que deben ser autoridades plenamente autónomas e independientes tanto del sector privado como del público y para ello contar con los recursos humanos, técnicos y financieros suficientes.

De hecho, la cuestión relativa las autoridades de protección de datos es uno de los principios generales en la materia que establecen los Principios sobre Privacidad de la OEA, que destacan las características mencionadas a la vez que promueven la cooperación con las autoridades e instituciones públicas y privadas relevantes (del ámbito penal, financiero, del consumidor, entre otras) cuyas labores tengan relación con la protección de datos personales, así como con sus pares de otros países[98].

Por su parte, los Estándares Iberoamericanos[99] agregan que normativamente se "deberá otorgar a las autoridades de control suficientes poderes de investigación, supervisión, resolución, promoción, sanción y otros que resulten necesarios para garantizar el efectivo cumplimiento de ésta, así como el ejercicio y respeto efectivo del derecho a la protección de datos personales." (cap. VII, art. 42). A la vez, recomiendan que sus decisiones únicamente puedan ser revisadas judicialmente, teniendo en cuenta la obligación de contar con un régimen que garantice a los

[98] OEA, Op. Cit, Principio 13, pp. 16 y 87-88.
[99] Estándares Interamericanos elaborados por la Red Iberoamericana de Protección de Datos (2017). Al igual que los Principios de la OEA no son vinculantes para la Argentina pero sí de gran peso interpretativo.

titulares mecanismos y procedimientos para hacer valer sus derechos (cfr. considerandos 24 y 25 del texto).

El Reglamento General de Protección de Datos Personales (RGPD) determina en el mismo sentido que "El establecimiento en los Estados miembros de autoridades de control capacitadas para desempeñar sus funciones y ejercer sus competencias con plena independencia constituye un elemento esencial de la protección de las personas físicas con respecto al tratamiento de datos de carácter personal" y agrega que "La independencia de las autoridades de control no debe significar que dichas autoridades puedan quedar exentas de mecanismos de control o supervisión en relación con sus gastos financieros, o de control judicial" (cons. 17 y 188), armonizándolas así con el ordenamiento republicano de gobierno.

También aporta directivas para su conformación, que vale la pena destacar: a fin de garantizar la independencia, sostiene que "sus miembros deben actuar con integridad, abstenerse de cualquier acción que sea incompatible con sus funciones (...). La autoridad de control debe tener su propio personal, seleccionado por esta o por un organismo independiente (...) que esté subordinado exclusivamente al miembro o los miembros de la autoridad de control." (cons. 121).

Teniendo en cuenta la protección de datos personales en poder del Estado, que aquí nos interesa, es fundamental destacar su rol en la promoción y garantía de derechos humanos. En este sentido, las autoridades de supervisión o aplicación "(...) tienen el poder de impulsar investigaciones independientes en las organizaciones y tener audiencias presentadas por individuos u ONG. (...) actúan como guardianas de los derechos de los usuarios y pueden ayudar a proteger sus derechos fundamentales. (...) Los gobiernos deben también promover el trabajo de las DPA [por sus siglas en inglés - *Data Protection Authorities*], explicar sus roles, y brindarles un presupuesto adecuado para garantizar que cumplan con sus responsabilidades."[100].

Sobre este último punto, es interesante reflexionar sobre la necesidad no sólo de dotarlas de potestades suficientes (como veremos a continuación) sino también de darlas a conocer como primer paso para alentar al cumplimiento de la ley, para quienes efectúan tratamiento de datos personales en el sector pero también para ciudadanos y organizaciones de la sociedad civil que busquen defender derechos previstos en la ley y por lo tanto necesiten conocer las funciones y competencias de estos organismos.

[100] Access Now, Op. Cit., pág. 13.

ii. El caso argentino. Los límites de la autoridad de aplicación frente al uso de datos personales por parte del Estado.

En Argentina, a nivel federal, desde 2017 la autoridad de aplicación de la Ley de Protección de Datos Personales es la Agencia de Acceso a la Información Pública (en adelante AAIP). Veamos cómo llegamos hasta aquí.

La ley 25.326 determinaba en su redacción original que el órgano de control de su aplicación gozaría "de autonomía funcional" y actuaría "como organismo descentralizado", pero al momento de su promulgación el Poder Ejecutivo efectuó un veto parcial que privó al órgano de control de la independencia que debía tener por cuestiones presupuestarias y para convertirlo, en cambio, en una dependencia dentro de la Administración[101].

Así, al reglamentarse la ley, se creó como órgano de control la Dirección Nacional de Protección de Datos Personales dentro de la entonces Secretaría de Justicia y Asuntos Legislativos del Ministerio de Justicia y Derechos Humanos[102]. Funcionó allí hasta el 2017, cuando se sancionó la Ley Nacional de Acceso a la Información Pública nº 27.275, que creó la Agencia de Acceso a la Información Pública (AAIP), ente autárquico con autonomía funcional en el ámbito de la Jefatura de Gabinete de Ministros, y entre sus objetivos incluyó el "actuar como Autoridad de Aplicación de la Ley de Protección de Datos Personales N° 25.326" (art. 19), por lo que se estableció como nuevo órgano de control de la ley de datos personales[103]. Este tipo de diseño institucional implica que el titular sea nombrado o removido únicamente por el Poder Ejecutivo (sin intervención, por ejemplo, del Senado): el procedimiento establecido legalmente[104] incorpora una audiencia pública para su designación pero no le da carácter vinculante, a la vez que tampoco le exige determinada experiencia o conocimientos sobre protección de datos personales.

En este marco, en noviembre del mismo año se dictó una Decisión Administrativa[105] que conformó tres direcciones dentro de la AAIP: Dirección de

[101] Decreto 95/2000
[102] Decreto 1558/01, anexo I, artículo 29.
[103] Decretos746/17 y 899/17, art. 1.
[104] Ley 27.275, art. 21.
[105] Decisión Administrativa N° 1002, 15/11/2017.

Acceso a la Información Pública, Dirección de Protección de Datos Personales (DNPDP) y Dirección de Informática e Innovación.

Poco tiempo después la propia AAIP dictó una resolución[106] en la que justifica el diseño concentrado del derecho de acceso a la información pública y a protección de datos personales en un solo organismo a través de experiencias comparadas y de la interrelación entre ambos derechos. Destaca, por ejemplo, el principio general de presunción de publicidad de la información en poder de los organismos públicos y por lo tanto el régimen limitado de excepciones basadas en la protección de otros derechos o intereses, entre las que se encuentra información que contenga datos personales (con sus salvedades), por lo que ambos derechos "deben ser ejercidos y protegidos de manera armónica". Teniendo este esquema en mente y buscando establecer "los mecanismos a implementar ante una posible colisión de derechos, a efectos de llevar adelante una correcta ponderación y protección de ellos", consagra a través de esta resolución la intervención obligatoria de la DPDP en casos que versen sobre la Ley de Protección de Datos Personales o sobre la Ley de Acceso a la Información Pública pero que "afecten o potencialmente puedan afectar" la protección de datos personales (cfr. arts. 1 y 2). Agrega también que en caso de controversia entre informes de esta Dirección y de la de Acceso a la Información Pública, será el/la Director/a de la AAIP quien resuelva.

Veremos que un sistema concentrado de este tipo no parecería ser el mejor diseño institucional al pensar en fortalecer el derecho a la privacidad de la ciudadanía:

Por un lado, es posible advertir varias falencias en el diseño normativo. En primer lugar, resulta problemático que una misma agencia estatal concentre las facultades de órgano de control de acceso a la información pública y de autoridad de protección de datos personales. Es que se trata objetivos dispares cuyo cumplimiento puede en ocasiones colisionar y, desde que el contralor de la ley de protección de datos personales pasó a la órbita de la Agencia quedó, en la práctica, subordinada a la cuestión del acceso a información pública.

En segundo lugar, aunque no quedara subsumido en la práctica a las competencias de acceso a la información, lo cierto es que la Agencia se trata en sí misma de un ente autárquico dentro de la Jefatura de Gabinete de Ministros. Esto implica menor independencia y autonomía que si fuera un organismo

[106] Resolución 5-E/2018 de la AAIP, disponible en https://www.argentina.gob.ar/normativa/nacional/resolución-5-2018-306577/texto (fecha de consulta: noviembre de 2023)

descentralizado con autonomía funcional en los términos en que lo preveía la ley en su redacción original. Como mencionamos, nombrar o remover a su titular es potestad exclusiva del Poder Ejecutivo, por lo que no se garantiza la independencia de la autoridad, a la vez que se desnaturaliza el espíritu original de la ley.

De hecho, es importante recordar que al momento de debatir el tipo de autoridad que debería estar a cargo de la Agencia de Acceso a la Información Pública[107], la Fundación Vía Libre manifestó que estas funciones de defensa de derechos ciudadanos bien podrían ser integradas al mandato del Defensor del Pueblo de la Nación, órgano constitucional que lamentablemente ha sido vaciado de contenido y acción a lo largo de los años.

Por otro lado, nos encontramos también con obstáculos relativos a las voluntades políticas para su correcta implementación dentro del marco que establece la norma: la escasa importancia que los distintos gobiernos hasta la fecha han dado a la protección de los datos personales se tradujo en la constante falta de capacidades técnicas y recursos económicos en el órgano de control. Así, "la debilidad impuesta por una promulgación parcial sobre la autoridad de aplicación fue ratificada por presupuestos magros y recursos humanos escasos."[108].

De hecho, el traspaso de funciones de autoridad de aplicación a la AAIP -producida por el decreto 746/2017 antes citado- tuvo como resultado la disminución de sus ya menguadas capacidades operativas y, en la práctica, la subordinación de los objetivos de protección de la privacidad a aquellos de acceso a información pública, como relatamos anteriormente. Un ejemplo reciente es la falta de intervención de la autoridad de protección de datos personales frente a resoluciones administrativas potencialmente abusivas en el contexto de la pandemia por COVID-19[109].

Sobre estas cuestiones es interesante el relevamiento hecho por la Asociación por los Derechos Civiles sobre el funcionamiento en la DNPDP en la práctica y su correlación con los problemas estructurales del diseño normativo[110]. Refiere al bajo

[107] Este aporte se dio en abril de 2016 en el marco del debate por la entonces nueva Ley Nacional de Acceso a la Información Pública, finalmente entrada en vigencia en septiembre de 2017. Para más información sobre el posicionamiento de Vía Libre ver https://www.vialibre.org.ar/contribuciones-al-debate-sobre-la-ley-de-acceso-a-la-informacion-publica/.
[108] ADC, Op. Cit., pág. 11
[109] Nos referimos en particular a la Decisión Administrativa 431/2020 que permitió, sin límite temporal ni criterios de reversión, el intercambio de datos en poder del Estado para "acciones útiles para la protección de la salud pública", sin mayores definiciones. La autoridad de protección no tuvo intervención alguna.
[110] ADC, Op. Cit.

presupuesto, tanto con respecto al personal como recursos materiales, con respecto a las funciones ambiciosas que le asigna la ley y la estructura que necesitaría tener. De hecho, se mantuvo durante muchos años una estructura mínima de personal, mientras la tecnología avanzaba y facilitaba el tratamiento de todo tipo de datos. Por ejemplo, en cuanto a la facultad de control que tiene la Dirección, el informe concluye que "(...) hay una correlación entre el diseño de las instituciones y su desempeño en la práctica: un organismo de control al que se le negaron las garantías de independencia y autarquía financiera que preveía la ley tuvo un presupuesto magro y escaso personal para desarrollar tareas que excedían las capacidades institucionales realmente disponibles. La divergencia entre lo que la ley esperaba que haga y la estructura creada por el Poder Ejecutivo limitó sus capacidades de acción que -además- fueron permisivas hacia el Estado, no sólo por la falta de independencia del organismo sino por los propios sesgos de la ley (...)"[111]. Explica así la relación entre los dos aspectos problemáticos a los que nos referimos más arriba: el diseño normativo y su traducción en la práctica.

Resalta sobre esto último otro aspecto que nos interesa especialmente destacar, concerniente a la deferencia con el Poder Ejecutivo que la ley habilita ("permisividad") y la voluntad política aprovecha, a través de recursos insuficientes y mecanismos de control y sanción laxos o discrecionales. A través de un repaso del tipo de inspecciones y sanciones realizadas por la DNPDP afirma que, en el período bajo estudio, "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 dependiente del poder ejecutivo y -en consecuencia- débilmente empoderado para dictar sanciones contra dependencias jerárquicamente iguales o, en general, superiores."[112].

iii. La necesidad de autonomía y capacidad de defender los derechos de la ciudadanía. Propuestas para una reforma normativa.

En línea con los comentarios presentados desde la Fundación Vía Libre en noviembre de 2022 al último anteproyecto de reforma que se presentó

[111] Ibidem, p. 7.
[112] Ibidem, p. 8.

oficialmente[113], consideramos que, además de llevar adelante políticas públicas que refuercen la protección de datos -tal como nos referimos en los capítulos 2 y 3 de este documento a la regulación normativa de la cesión entre organismos del Estado-, es fundamental introducir cambios en las normas que regulan a la autoridad de aplicación de la ley de datos personales.

Así, entendemos que la autoridad de aplicación debe estar facultada para dictar normas de cumplimiento obligatorio y para hacerlas cumplir, cuestiones que según el diseño normativo actual no están previstas. A modo de ejemplo, estas normas que debería dictar podrían incluir:

- Condiciones de seguridad exigidas para el tratamiento de datos sensibles (por ejemplo, que los datos sensibles se almacenen siempre en forma cifrada) con un estricto protocolo de acceso a ellos;
- Normas para el tratamiento de datos personales en circunstancias en que está exceptuado el consentimiento (archivos, estadísticas e investigación científica actividad periodística, investigación judicial);
- Protocolos de inspección de las instalaciones y documentación de los responsables y encargados de tratamiento.

A su vez, la autoridad de aplicación debe tener capacidad suficiente para hacerlas cumplir: nos referimos a las potestades necesarias para requerir cualquier información necesaria -con las respectivas normas de confidencialidad que deben alcanzar al personal a cargo- y para ingresar a cualquier local en que se efectúe tratamiento de datos sin necesidad de previa orden de allanamiento, pero también para imponer sanciones. Hoy en día, "el ejercicio de sus facultades sancionatorias requiere -por distintas razones- una estructura de la que la DNPDP parece carecer"[114]. Como mencionamos anteriormente, la autoridad de aplicación debe contar con los recursos humanos, técnicos y financieros necesarios, así como con la mayor transparencia posible.

Es que no es posible un cumplimiento efectivo sin que la autoridad de aplicación tenga condiciones de independencia y profesionalidad. Los estándares internacionales que desarrollamos más arriba colocan en cabeza de las autoridades de aplicación una gran cantidad de recomendaciones y potestades. Es indispensable entonces dotarla de idoneidad y recursos acorde, especialmente teniendo en cuenta

[113] Disponible en https://www.vialibre.org.ar/aporte-ley-datos/
[114] ADC, Op. Cit., p. 8

que debe ser absolutamente independiente tanto del sector público como del privado para no desnaturalizar su función.

Entonces, volviendo al diseño institucional vigente, colocar la responsabilidad de la protección de datos personales en cabeza de la actual Agencia de Acceso a la Información Pública es contrario a los principios desarrollados. Como mencionamos, esta temática tiene una especificidad propia, que de hecho suele requerir una lógica inversa a la del acceso a información pública (en tanto es otro el derecho que busca proteger) y, en los hechos, suele quedar subsumida a esta última. En el mismo sentido, que la designación de su titular no cuente con una instancia de audiencia pública vinculante ni concurso de oposición y antecedentes referidos a la Protección de datos ya demuestra, desde el diseño institucional, que no hay garantía efectiva de cumplimiento de la misión específica más allá de la buena voluntad de quien ocupe la dirección de la Agencia. La independencia de la autoridad encargada de proteger la información personal resulta indispensable para garantizar el efectivo respeto a derechos fundamentales.

En este sentido, por lo menos dos reformas se vuelven urgentes: por un lado, colocar la autoridad de aplicación por fuera de la Agencia de Acceso a la Información Pública, como un organismo con autonomía descentralizado con autonomía funcional propia (en los términos en que lo preveía la ley en su redacción original) y no en la órbita de la Jefatura de Gabinete del Poder Ejecutivo. De otro modo, es muy difícil controlar y sortear la deferencia con el propio Estado a la hora de ejercer sus facultades de control y sanción. Por otro, diseñar un proceso de nombramiento de su titular distinto al que hoy rige para la AAIP; uno donde tenga intervención el Senado de la Nación, haya audiencias públicas de carácter vinculante y se ponderen, también de manera obligatoria, los antecedentes en la materia para evaluar la idoneidad de el/la candidata/a. Sólo así se podrá garantizar su autonomía y capacidad suficiente para defender los derechos de la ciudadanía.

05.

Conclusión general

Conclusión general

A lo largo de este informe buscamos reponer la función estatal en relación con la identificación de la ciudadanía y pudimos observar cómo mutó de una cuestión meramente registral a una actividad más abarcativa y con objetivos diversos. En función de eso, evolucionaron también las formas y los documentos con que se identifica.

Si bien la normativa que rige al Registro Nacional de las Personas data de otra época y mantiene una lógica castrense como forma de regir su actividad, hoy el Estado recopila, almacena y trata datos de formas muy distintas y para servir a finalidades amplias, idealmente vinculada con el diseño de políticas públicas más específicas. Esta ampliación se da en simultáneo con -y gracias a- avances tecnológicos que permiten la obtención y procesamiento de datos de manera masiva.

El avance estatal en la posibilidad material y la decisión política de vigilancia a la ciudadanía a través de la obtención y tratamiento de sus datos (incluyendo, por supuesto, la cesión) implica una grave intrusión y potencial vulneración de la privacidad y un conjunto de otros derechos, más aún considerando que los datos que se pueden obtener son cada vez más íntimos y sensibles. En este contexto es indispensable una legislación que imponga límites rigurosos al Estado, proteja a los ciudadanos y siente las bases para una autoridad de aplicación fuerte, autónoma y con perspectiva de derechos humanos. cuestiones que hoy no tenemos en Argentina, en algunos casos por falta de voluntad política y en otros por el propio diseño normativo de una ley pensada para otro momento.

Es que el marco normativo rector en el país sigue siendo el mismo: la Ley de Protección de Datos Personales 25.326 del año 2000, anacrónica, imprecisa y vaga en cuanto a las limitaciones y obligaciones estatales. La jurisprudencia y la doctrina suelen coincidir en la interpretación restrictiva, pero esto no parece ser suficiente. Argentina adhirió a tratados y convenios internacionales que exigen profundas reformas normativas para adecuarse; existen legislaciones en el mundo que pueden ser tomadas como faro.

En simultáneo surge otra voz: aquella que apela a la cesión indiscriminada -o con menos limitantes- de datos entre agencias del Estado en pos de hacerlo más eficiente. Es común escuchar que la Administración no debería "duplicar esfuerzos" pidiendo a sus ciudadanos los mismos datos más de una vez. A esto respondemos que el costo de hacerlo es infinitamente menor a aquel en términos de derechos en caso contrario, tal como vimos a lo largo de este informe.

Como dijimos, es necesaria una reforma legislativa en general, teniendo en cuenta la evolución tecnológica y las nuevas prácticas que exceden las previsiones de la ley actual. En este informe destacamos la urgencia de un marco claro, robusto y con mayores salvaguardas en relación con la cesión de datos como con el diseño y potestades de la autoridad de aplicación[115], que indefectiblemente debe ir acompañada de voluntad política para mayores controles que aseguren el cumplimiento de derechos.

Mientras tanto, en el escenario actual, hay consenso sobre algunas cuestiones indispensables por las que la actuación del Estado debe regirse: el respeto a los límites del consentimiento y la cesión de acuerdo con los arts. 4, 5 y 11 de la ley 25.326, lo cual implica la interpretación restrictiva de las excepciones a esas restricciones, especialmente cuando el pretexto es el "interés legítimo" o "cumplimiento de funciones", que se invocan tantas veces de manera dogmática sin mayor justificación. En este sentido es fundamental el apego al principio de finalidad, al amparo de los principios de proporcionalidad y de minimización de los datos. También la importancia de implementar medidas de seguridad suficientes y efectivas en la gestión de datos en su poder. En cuanto a la autoridad de control, la Agencia de Acceso debe procurar un rol activo en todo aquello que la ley ya prevé, lo cual implica también voluntad política (tanto del Poder Ejecutivo como del Legislativo, en tanto ente autárquico cuyo presupuesto depende de la Ley nacional) para dotarla de los recursos suficientes y promover su autonomía para la defensa de derechos de los ciudadanos.

A través de este informe intentamos echar luz sobre una cuestión que muchas veces se subestima. En síntesis, nos interesa llamar la atención sobre los graves abusos que pueden darse bajo legislaciones como la actual, en un mundo donde la protección de los derechos humanos corre detrás del avance tecnológico y

[115] A estos efectos ponemos a disposición como anexo una propuesta de redacción para un nuevo artículo de ley sobre cesión de datos personales entre organismos del Estado, elaborada en conjunto entre Access Now y la Fundación Vía Libre en octubre de 2023. Sobre la Autoridad de Aplicación, nos remitimos aquí a los puntos mínimos que planteamos en el capítulo 4 de este informe.

las acciones de vigilancia que permite. Cuando son llevadas adelante por el Estado, que tiene además la potestad de ser garante de esos derechos y la obligación de identificarnos como parte de sus funciones, es aún más preocupante.

ANEXO

Propuesta de reforma normativa para cesiones de datos personales dentro del Estado, con especial atención al requisito del consentimiento.

Elaborada en conjunto con Access Now, octubre de 2023.

"Las transferencias de datos personales que se efectúen entre entes públicos en el marco de una obligación legal, interés público o ejercicio de poderes públicos, así como todo tratamiento realizado con los datos transferidos, serán lícitos en la medida en que se cumplan las siguientes condiciones:

- *Exista una **autorización expresa** por ley especial, o por la autoridad de aplicación siempre que se verifique lo siguiente:*
  - *que la transferencia sea **necesaria** para el cumplimiento de un fin público asignado por ley a la entidad receptora de los datos;*
  - *que los datos transferidos sean **necesarios** para el cumplimiento de dicha finalidad;*
  - *que la entidad receptora de los datos cuente con **medidas de seguridad y protocolos necesarios** para garantizar la integridad, disponibilidad y confidencialidad dispuestas en esta ley.*
- *La entidad cedente haya obtenido los datos de acuerdo a una base legal establecida en el Artículo 13 de esta ley y en el ejercicio de sus competencias asignadas por ley.*
- *La entidad receptora utilice los datos pretendidos para una finalidad que se encuentre dentro del marco de sus competencias legales vigentes y no sea distinta de aquella con la que los datos se recolectaron originalmente.*
- *Los datos involucrados en la transferencia sean únicamente los adecuados y estrictamente necesarios para acometer la finalidad pública, de conformidad con el principio de minimización. Se prohíbe la cesión masiva e indiscriminada de bases de datos.*

Las transferencias deberán ponerse en conocimiento de todos los titulares de los datos involucrados de manera segura y sin comprometer su confidencialidad, dentro de los siguientes quince (15) días a la ejecución de la

transferencia. La transferencia debe documentarse en un convenio interinstitucional que deberá ser publicado y puesto a disposición de la ciudadanía para su escrutinio, resguardando la confidencialidad de los datos personales involucrados en la transferencia. Este convenio deberá contener disposiciones específicas respecto de las condiciones que rigen la licitud del tratamiento por parte de las personas responsables; la descripción clara de la categoría de personas cuyos datos se procesarán, sin exponer datos que puedan identificar a las personas; los tipos de datos objeto de tratamiento, especialmente si contienen categorías de datos sensibles; la finalidad específica del tratamiento; los plazos de conservación de los datos; un detalle de las operaciones y los procedimientos del tratamiento; incluidas las medidas técnicas, físicas y organizativas de seguridad que se establecerán para proteger la información; y un medio de contacto para obtener más información sobre la transferencia.

La transferencia de datos sensibles entre entidades públicas deberá estar motivada en una ley, cumplir con los principios de necesidad y proporcionalidad, y autorizada por la autoridad de aplicación previa evaluación de impacto sobre el derecho a los datos personales. La entidad receptora de los datos podrá utilizar los datos sensibles exclusivamente para la finalidad que le dio origen a la transferencia, quedando prohibido todo uso ulterior indistintamente que sea compatible con sus funciones. Cumplido dicho objetivo, la entidad receptora deberá suprimir los datos o la autoridad cedente revocar el acceso a la base compartida. No serán aplicables estas reglas a las transferencias de datos sensibles realizadas entre entidades que cumplen las mismas funciones en distintas esferas del estado.

Esta ley es aplicable al tratamiento de datos personales efectuado por las Fuerzas
Armadas, fuerzas de seguridad y organismos de inteligencia.

Las empresas y sociedades del Estado como las sociedades de economía mixta recibirán el mismo tratamiento que las personas jurídicas privadas, en los términos de esta Ley. Cuando el objetivo de estas entidades consista en instrumentar o ejecutar políticas públicas, recibirán el mismo tratamiento que a las personas jurídicas y organismos públicos en los términos de este Artículo.

Las entidades y personas jurídicas públicas tienen prohibido transferir a las personas jurídicas privadas datos personales, excepto:

a. *En los casos de ejecución descentralizada de actividades públicas que requieran la transferencia, exclusivamente para este fin específico y particular, siguiendo lo dispuesto en la Ley de Acceso a la Información Pública.*
b. *Cuando así lo establezca una ley, y la transferencia esté respaldada por contratos, convenios o instrumentos análogos debidamente publicados.*

La autoridad de aplicación podrá, en cualquier momento, solicitar a las entidades públicas información específica sobre el alcance y naturaleza de los datos, detalles sobre el tratamiento realizado, la adopción de medidas dirigidas a garantizar la seguridad de los datos y emitir opiniones técnicas complementarias para garantizar el cumplimiento de la ley. También podrá establecer reglas complementarias para el cumplimiento de los deberes de información y para el uso compartido de datos personales."

Fundación Vía Libre