sep / 14

El Estado recolector

Un estudio sobre la Argentina y los datos personales de los ciudadanos.

ADC / Asociación por los Derechos Civiles

policy paper

ADC / Asociación por los Derechos Civiles

policy paper

El estado recolector. Un estudio sobre la Argentina y los datos personales de los ciudadanos

Septiembre de 2014[*]

Cualquier persona argentina conoce de cerca los múltiples trámites, complejos y no tanto, que exigen, de nosotros, la presentación de nuestro Documento Nacional de Identidad (DNI). Ello es una experiencia diaria: los trámites bancarios, la compra de pasajes de larga distancia y la entrada a edificios públicos y privados requieren presentar una tarjeta que nos acompaña desde el año 1968, cuando el decreto-ley No. 17.671 de Juan Carlos Onganía estableció el DNI como documento de identificación de todos los ciudadanos[1]. Muchas sociedades se sorprenderían de ver la presencia de estas pequeñas tarjetas en nuestra vida diaria: hay muchos países que no cuentan con sistemas únicos de identificación de los ciudadanos y, cuando intentaron imponerlos, fracasaron por la fuerte oposición de la ciudadanía[2].

Con los avances tecnológicos, las políticas públicas de *identificación*, *registro* y *clasificación* del "potencial humano nacional" se hicieron más eficientes y efectivas[3]. 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. El DNI único que entrará en

[*]Este trabajo fue realizado por el área de Privacidad de la Asociación por los Derechos Civiles (ADC), como parte de la *Cyber Stewards Network* y con el apoyo financiero del International Development Research Center, Ottawa, Canadá.

[1]Ley 17.671, de Identificacion, Registro y Clasificacion del Potencial Humano Nacional

[2]Ejemplo de Inglaterra.

[3]La ley 17.671, que estableció el DNI, lleva por nombre *Ley de identificacion, registro y clasificacion del potencial humano nacional*.

vigencia en 2015 permitirá que todos los datos de los ciudadanos argentinos integren una única base de datos de información biométrica digitalizada[4].

Los avances tecnológicos que se produjeron en relación al sistema de clasificación de los datos filiatorios de los argentinos se extendieron, en general, a todas las áreas del Estado. La información que antes era recolectada de manera analógica hoy es capturada en formatos digitales que la vuelven más útil: ellos permiten el análisis automatizado, el acceso remoto y la reproducción a bajo costo. Pero esa mayor efectividad ha creado nuevos riesgos que los sistemas analógicos no presentaban. Este trabajo busca indagar sobre esos riesgos procurando ofrecer respuestas a las siguientes preguntas.

1. El ordenamiento jurídico argentino, ¿protege adecuadamente nuestros datos personales o tiene deficiencias –ya sea de diseño o de implementación– que los ponen en riesgo?

2. ¿Qué tipos de bases de datos tiene el Estado argentino? ¿Cuentan con medidas de seguridad, con sistemas protegidos de acceso remoto, con niveles de autorización para el acceso a las mismas? ¿Existen registros de los accesos? ¿Hay protocolos de seguridad estandarizados?

3. ¿Ha habido vulneraciones a la seguridad de esas bases de datos que hayan sido conocidas? ¿Que ha hecho el Estado cuando eso ha ocurrido?

I. La ley de Protección de Datos Personales y dos pecados originales

El marco legal argentino en materia de protección de datos personales es uno de los mejores de la región. En efecto, la Argentina cuenta con una garantía constitucional para la protección de los datos personales reconocida en el artículo 43 de la Constitución, que dispone:

> "Toda persona podrá interponer esta acción 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."

[4]Cfr. Telam. *A partir de 2015 el DNI tarjeta será el único documento válido*. Consultado el 19 de junio de 2014 y La Nación. *A partir de 2015, sólo tendrá validez el nuevo "DNI tarjeta"*. Consultado el 19 de junio de 2014. Cabe señalar, sobre el punto, que por datos biométricos nos referimos a información sobre rasgos físicos de las personas que son utilizados con fines de identificación, como huellas dactilares, fotografía, patrones faciales, etcétera.

La ley 25.326 de *Proteccion de los Datos Personales* recoge los principios de la Directiva 95/46/CE de la Unión Europea. Esta norma establece estándares elevados de protección y desde 2003 la Argentina es considerada por la UE como un país con nivel adecuado de protección de datos personales (Travieso, 2006).

Este marco legal protectorio presenta, sin embargo, dos debilidades estructurales: (a) un órgano de control débil y dependiente del poder ejecutivo y (b) una excesiva permisibilidad hacia el Estado en relación al almacenamiento, tratamiento y cesión de datos personales.

Sobre la primera cuestión cabe decir lo siguiente: la versión original de la ley 25.326 preveía un órgano de control que tendría "autonomía funcional" y actuaría "como órgano descentralizado en el ámbito del Ministerio de Justicia y Derechos Humanos de la Nación." Tendría un director designado por el poder ejecutivo por un mandato de cuatro años y, para su nombramiento, debería contar con el acuerdo del Senado de la Nación. Esas garantías de independencia funcional y autarquía financiera fueron dejadas de lado por el poder ejecutivo al promulgar parcialmente la norma mediante el decreto 995/00, que invocó razones de índole financiera para mantener al órgano de control dentro de la esfera del poder ejecutivo. Esa decisión fue fundamental para construir un órgano de control débil y dependiente del poder ejecutivo[5].

Para abordar la segunda cuestión es útil analizar la estructura de la ley 25.326, que protege los datos personales a través de dos prohibiciones generales que parecen cumplir un rol fundamental en la arquitectura jurídica de la norma: la prohibición de tratar y de ceder datos personales sin el consentimiento de los titulares[6]. 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.

En efecto, el artículo 5 que exige consentimiento permite evadir ese permiso cuando los datos se "recaben para el ejercicio de funciones propias de los poderes del Estado o en virtud de una obligación legal". Ello significa que la garantía del consentimiento es inútil cuando quien recaba información es el Estado. Asimismo, el artículo 11 impide la *cesión* de los datos si el titular de los mismos no ha prestado su consentimiento. Pero –nuevamente– ese requisito puede ser dejado de lado cuando lo disponga una ley, cuando los datos haya sido recabados para el ejercicio de funciones propias de los

[5] A pesar de que el decreto reglamentario 1558/01 establece en su artículo 29.1 que el "Director tendrá dedicación exclusiva en su función, ejercerá sus funciones con plena independencia y no estará sujeto a instrucciones."

[6] Ley 25.326, artículos 5.1 y 11.1.

poderes del Estado o cuando la cesión se realice entre dependencias de los órganos del Estado en forma directa en la medida del cumplimiento de sus respectivas competencias[7]. Como vemos, las barreras que establece la ley en términos generales se levantan sin mayores consideraciones cuando quien recaba datos es el Estado.

Mediante estas excepciones, redactadas en términos amplios, la ley 25.326 permite al Estado evadir las prohibiciones que constituyen el núcleo duro de su estructura: las de tratar o ceder datos sin el consentimiento de su titular. Al hacerlo, priva a los ciudadanos de la principal herramienta de defensa de la privacidad de sus datos.

Estamos entonces en condiciones de responder la primer pregunta que habíamos planteado: ¿nuestro ordenamiento jurídico protege adecuadamente nuestros datos o tiene deficiencias que los ponen en riesgo? Hemos identificado dos problemas vinculados al diseño mismo de la norma que parecen ser especialmente relevantes para el objeto de este estudio:

1. En primer lugar, el organismo creado de la ley fue dejado de lado por el poder ejecutivo que la vetó parcialmente. Y el organismo que se creó en su reemplazo carece de las garantías de independencia que establecía la versión original de la norma.

2. En segundo lugar, dos prohibiciones estructurales que *empoderan* a los ciudadanos al permitirles negarse al tratamiento de sus datos no se aplican cuando quien hace ese tratamiento es una dependencia estatal que –además– puede ceder esa información a otros organismos estatales sin mayores restricciones.

En la siguiente sección procuraremos analizar si, además de esas falencias de diseño, hay problemas en la implementación del sistema vigente.

II. El Estado y los datos personales

En la Argentina, el órgano encargado de defender los datos personales de los ciudadanos es la Dirección Nacional de Protección de Datos Personales (DNPDP) que nació –como vimos– seriamente limitada en sus facultades de acción. Esos problemas estructurales, ¿se reflejan en las prácticas del organismo? Para responder a esa pregunta es necesario analizar si la ausencia de la *autarquía financiera* que establecía la ley se reflejó en la estructura de la DNPDP y si los amplios permisos hacia el Estado conferidos por la ley han impactado en la actuación del organismo.

[7] Cfr. Ley 25.326, artículo 11.3.

Estructura y funcionamiento de la DNPDP

Si se analiza el presupuesto operativo de la DNPDP desde su creación es posible ver que el mismo fue relativamente bajo, tanto en términos de recursos como de personal[8]. Si se consideran los datos del presupuesto y se da cuenta de la inflación interanual, es posible –también– verificar que ciertos casos de aumento nominal representaron una disminución *real* del presupuesto asignado a esos años, como ocurrió en 2005, 2006, 2008, 2009 y 2013. Sólo entre 2010 y 2012 el presupuesto real de la DNPDP creció, hecho que acompañó también un proceso de aumento de su personal (Cuadro 1).

Año	Presupuesto	Personal	Inflación	Variación Real
2014	$ 5.662.014	26		
2013	$ 4.291.557	25	28,3	-
2012	$ 3.809.908	25	25,9	+
2011	$ 1.727.045	23	24,3	+
2010	$ 1.021.095	21	26,1	+
2009	$ 862.729	21	16,7	-
2008	$ 728.605	11	23,5	-
2007	$ 702.158	10	8,8	+
2006	$ 396.667	10	1,9	-
2005	$ 380.091	10	9,8	-
2004	$ 595.124	9	4,4	

Cuadro 1: Presupuesto y estructura de la DNPDP (2004-2014).

Analizar la estructura y el presupuesto de la DNPDP es especialmente útil si comparamos esos datos con las funciones que le asigna la ley 25.326.

- Asistir y asesorar a los ciudadanos para la defensa de sus derechos (Artículo 29.1.a).
- Dictar normas y reglamentaciones necesarias para la implementación de la ley (Artículo 29.1.b)
- Realizar un censo de archivos alcanzados por la ley y mantener el registro (Artículo 29.1.c)

[8]El artículo 29.3 del decreto reglamentario 1558/01 establece que la DNPDP se financiará a través de lo que recaude en concepto de tasas por los servicios que preste; el producido de las multas previstas en el artículo 31 de la Ley Nº 25.326 y las asignaciones presupuestarias que se incluyan en la Ley de Presupuesto de la Administración Nacional a partir del año 2002.

- Controlar la observancia de las normas sobre integridad y seguridad en bases de datos (Artículo 29.1.d)
- Solicitar información a las entidades públicas y privadas (Artículo 29.1.e).
- Iniciar procedimientos e imponer las sanciones administrativas (Artículo 29.1.f y 30.3 del dec. 558/01).
- Constituirse en querellante en las acciones penales por violaciones a la ley (Artículo 29.1.g).
- Controlar el cumplimiento de los requisitos y garantías necesarias para inscribirse en el registro (Artículo 29.1.h).
- Controles de oficio y sanciones por violación del principio de finalidad (Artículo 4, decreto 1558/01).
- Verificar el respecto de la ley en la etapa de recolección, intercambio, transmisión y cesión de bases (Artículo 4, decreto 1558/01).
- Establecer requisitos para el consentimiento informado (Artículo 5, decreto 1558/01).
- Promoverá la cooperación entre sectores públicos y privados (Artículo 9, decreto 1558/01).
- Recibir denuncias por denegaciones de derecho de acceso a datos personales (Artículo 14, decreto 1558/01).
- Elaborar el formulario modelo para el ejercicio del derecho de acceso (Artículo 15, decreto 1558/01).
- Dictar normas complementarias para los contratos de cámaras, asociaciones y colegios profesionales. (Artículo 2 558/01 y 29.5, dec. 1558/01).
- Dictar normas sobre registro, tratamiento y seguridad de bases de datos públicas y privadas (Artículo 29.5, decreto 1558/01).
- Atender las denuncias y reclamos interpuestos en relación al tratamiento de datos personales (Artículo 29.5, decreto 1558/01).
- Percibir las tasas que se fijen por los servicios de inscripción y otros que preste (Artículo 29.5, decreto 1558/01).
- Organizar el registro de archivos, registros, bases o bancos de datos públicos y privados (Artículo 29.5, decreto 1558/01).
- Diseñar instrumentos para la mejor protección de los datos personales de los ciudadanos (Artículo 29.5, decreto 1558/01).

- Alentar la elaboración de códigos de conducta (Artículo 30, decreto 1558/01).

Como puede observarse, las funciones de la DNPDP asignadas por la ley y el decreto reglamentario son sumamente ambiciosas y ellas parecen estar pensadas para un órgano con independencia y autarquía financiera, así como con la estructura necesaria para poder cumplir con ellas de manera adecuada. En efecto, y como surge de la lista precedente, tanto la ley como su decreto reglamentario asignan a la DNPDP funciones de asesoramiento a ciudadanos, reglamentación de facultades, control y registro de bases de datos públicas y privadas y sanción ante casos de incumplimiento con una competencia amplia que se extiende a todo el territorio del país y para lo cual contó –durante los primeros seis años de existencia– con sólo una decena de empleados (cfr. cuadro 1). Debe tenerse en cuenta, además, que esta estructura mínima de personal se mantuvo mientras la tecnología avanzaba y facilitaba el almacenamiento y tratamiento de datos de todo tipo. Para decirlo de otra manera: la estructura del controlador se mantuvo relativamente inmóvil mientras la actividad a controlar se expandía radicalmente.

El punto señalado en el párrafo anterior queda más claro si analizamos en profundidad una de las facultades de la DNPDP, como es la de control. Según información de la DNPDP, entre 2008 y 2012 esa dependencia ha realizado 137 inspecciones (cuadro 3)cuando en el *Registro Nacional de Bases de Datos* había a fines de 2006 más de 60 mil bases de datos inscriptas[9].

Año	Cantidad de inspecciones
2008	4
2009	16
2010	50
2011	28
2012	39

Cuadro 2: Cantidad de inspecciones de la DNPDP (2008-2012).

El análisis precedente 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

[9]Cfr. Diario Judicial. *Registro de bases de datos: esperan 60 mil inscriptos a fin de año*. (25 de mayo de 2006). Disponible en: www.diariojudicial.com/contenidos/2006/05/26/noticia_0009.html

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 que identificamos antes y exploraremos a continuación.

Ejercicio de las facultades

Así como el presupuesto y la estructura de la DNPDP parecen reflejar una situación de debilidad, también es posible verificar la permisibilidad de la ley respecto del Estado en el accionar de la dirección. En efecto, las 137 inspecciones realizadas por la DNPDP entre 2008 y 2012 fueron realizadas a empresas privadas: nunca una dependencia estatal responsable de alguna base de datos fue objeto de una inspección por parte de la DNPDP entre esos años[10].

Es posible verificar lo mismo en el análisis de las sanciones por violación de la ley impuestas por la DNPDP: las 36 sanciones aplicadas por la DNPDP entre 2005 y 2013 fueron impuestas a entidades privadas. 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.

De todas formas, prestar atención a las sanciones impuestas por la DNPDP tiene sentido: ellas revelan que el ejercicio de sus facultades sancionatorias requiere –por distintas razones– una estructura de la que la DNPD parece carecer. En efecto, el 42 por ciento de las sanciones impuestas son el resultado de falencias en la inscripción, reinscripción o actualización del Registro de Base de Datos por parte de las empresas registradas (ver cuadro 3). Otro 25 por ciento es el resultado de falencias detectadas por la DNPDP en el marco de inspecciones que no fueron debidamente resueltas por las empresas titulares de las bases de datos. Es decir, el 67 por ciento de las sanciones impuestas son por cuestiones menores o el resultado de inspecciones realizadas que –como se dijo– fueron 137 sobre una base de más de 60 mil titulares de bases de datos inscriptos.

Causa de la sanción	Porcentaje
Negativa de derecho de acceso	8.33 %
Errónea información sobre deudores	8.33 %
Producción de informes sin respaldo legal	8.33 %
Inspecciones	25.00 %

[10]Los listados de inspecciones se pueden encontrar en el sitio de la DNPDP, www.jus.gob.ar/datos-personales.

Reinscripción, actualización de datos	41.68 %
Errónea asignación de líneas de teléfono	8.33 %

Cuadro 3: Sanciones impuestas por la DNPDP (2005-2013)

El contenido de las sanciones restantes se vincula a algunos de los problemas más graves que sufren los ciudadanos argentinos en relación a sus datos personales: la errónea inscripción en registros públicos y privados de deudores, la negativa al acceso a los propios datos personales y la producción de informes sobre las personas en violación de la ley 25.326.

El primero de esos problemas ha sido una de las principales causas de litigiosidad en materia de datos personales: la errónea inscripción en un registro de deudores genera innumerables inconvenientes para las personas, vinculados –especialmente– al acceso a crédito bancario. La DNPDP ha sancionado en tres oportunidades a empresas privadas que habían informado el estado de *deudor* de sus clientes de manera errónea.

El segundo problema tiene que ver con la negativa del *derecho de acceso* que implica, simplemente, permitir a las personas conocer qué información el titular de una base de datos tiene sobre ella.

El tercer problema es uno de los más serios y se vincula con la expansión de sitios de Internet que venden informes sobre ciudadanos que incluyen datos personales como los vinculados a su domicilio, estado civil, situación financiera y patrimonial, etcétera[11]. Por ello, tiene sentido ver qué ha dicho la DNPD al respecto.

Hay tres sanciones que son relevantes sobre esta cuestión: una de ellas contra la empresa *Advanced Development Solutions S.R.L.* (en adelante, ADS) que mantiene el sitio www.reportesonline.com y dos de ellas contra *Globinfo Argentina*, un emprendimiento de la firma *Open Discovery S.A.*.

El procedimiento contra ADS fue el resultado de quejas de personas que obtuvieron informes personales a través de la página de la compañía. Ellos denunciaron que pudieron obtener –a través de sus servicios– referencias a empleos anteriores, bienes personales, vínculos familiares que no se limitan al cónyuge, datos personales de vecinos, nivel de salario del consultado, etcétera. La DNPD consideró que este servicio violaba el principio de *interés*, que se había violado la garantía de *cesión* y también el principio de *finalidad*. Cabe señalar además que la DNPDP destacó que el acceso a la información *salarial* no es posible a través de "bases de datos de acceso público irrestricto", lo que hace suponer que hubo un tratamiento ilícito de datos ya que el titular de los mismos no prestó su consentimiento libre, expreso e informa-

[11]Cfr. Emiliano Villa. 2014. *La privacidad al alcance de todos*. Digital Rights LAC, No. 12, 2 de abril de 2014.

do.

Los procedimientos contra *Globalinfo Argentina*, por su parte, se iniciaron a petición de la Defensoría del Pueblo de la Ciudad de Buenos Aires y de un ciudadano particular. El análisis de la DNPDP da cuenta de una de las prácticas que más afectan los derechos personales de los ciudadanos, que se vincula con empresas que almacenan y procesan informes que son comercializados[12]. Estos sitios ofrecen distintos tipos de reportes. De manera gratuita, suelen ofrecer el nombre, número de DNI de los ciudadanos y el domicilio registrado en distintos registros públicos. De manera paga, ofrecen información más valiosa y difícil de acceder como la reseñada en el párrafo anterior.

La DNPDP consideró que el tratamiento de los datos por parte de Globalinfo no era necesariamente violatorio de la ley aunque la *cesión* de esos datos a terceros sí lo era. Consideró que los informes de *Globalinfo* eran *excesivos*, ya que para la localización de las personas se brindaba información sobre su situación patrimonial, y los informes con fines patrimoniales incluían información necesaria para su localización[13]. Sobre las fuentes de esa información, la DNPDP consideró que –en principio– *Globalinfo* había accedido a esa información de *fuentes de acceso público irrestricto* pero en ningún caso se refiere a qué tipo de fuentes se trata.

Mucha de la información contenida en estos informes provienen de bases de datos estatales que fueron compiladas con fines específicos, como el Registro Nacional de las Personas, el Registro Nacional de la Propiedad, la Administración Nacional de la Seguridad Social, entre otras. En ningún caso el dictamen se pregunta sobre la forma en que se accedió a esa información: sólo se limita a recordar que de acuerdo al artículo 11 del decreto reglamentario No. 1558/2001, "en el caso de archivos o bases de datos públicas dependientes de un organismo oficial que por razón de sus funciones específicas estén destinadas a la difusión al público en general, el requisito relativo al interés legítimo del cesionario se considera implícito en las razones de interés general que motivaron el acceso público irrestricto." La pregunta que se impone en este análisis es la siguiente: ¿todos los datos de las bases públicas estatales están destinadas a la difusión del público en general? ¿En qué condiciones y bajo qué garantías está la cesión de datos autorizada? El dictamen no profundiza en la cuestión y al no hacerlo evita cuestionar prácticas estatales que parecen ser la causa principal de la expansión de estas prácticas empresariales que violan los derechos de los ciudadanos.

[12] Id.

[13] DNPDP. Disposición No. 005 del 22 de abril de 2008, fs. 184.

III. La DNPDP y las bases de datos estatales

Hasta el momento hemos visto que la ley creó una autoridad de aplicación débil y tuvo una mirada excesivamente condescendiente hacia las actividades de archivo, tratamiento y cesión de datos hacia adentro del Estado. También verificamos que la debilidad impuesta por una promulgación parcial sobre la autoridad de aplicación fue ratificada por presupuestos magros y recursos humanos escasos. Señalamos, también, un desfasaje considerable entre las facultades de la DNPDP y los recursos de los que ella dispone, así como un sesgo considerable en su acción hacia actores privados, algo que tal vez pueda explicarse por la permisividad de la ley hacia las dependencias estatales.

Con base en esas conclusiones parciales hemos procurado conocer las prácticas estatales en relación a sus bases de datos a través de 16 pedidos de acceso a la información pública[14] en los que buscamos respuestas a ciertas preguntas básicas[15]. En general, el nivel de respuestas fue alto: diez depen-

[14]Las autoridades y/ registros requeridos fueron: Dirección Nacional de Inteligencia Criminal; Dirección los Registros Nacionales de la propiedad automotor y créditos prendarios; Dirección Nacional de Derechos de Autor; Registro Nacional de información de Personas Menores Extraviadas; Dirección nacional de Derechos Humanos y Derecho Internacional Humanitario; Registro nacional de tierras rurales; Oficina nacional de contrataciones; Dirección general de personal y bienestar del Ejército Argentino; Secretaría de gestión y articulación institucional; Registro nacional de la agricultura familiar; Servicio Penitenciario Federal; Dirección Nacional Migraciones.

[15]Las preguntas que se plantearon en los pedidos de acceso a la información fueron las siguientes: "Integración de los archivos, registros, bases o bancos de datos del [Registro X]. En particular, nos interesa conocer (a) si el [Registro X] tiene archivos, registros, bases o bancos de datos. En caso de tratarse de varios, por favor identificarlos; (b) locación física de los servidores que alojan los archivos, registros, bases o bancos de datos; (c) datos de las personas físicas que contienen esos archivos, registros, bases o bancos de datos (por ejemplo, Número de DNI, número de trámite, nombre, apellido, fotografía, etcétera) precisando e identificando (de existir varios) cada sistema de registro por separado. // ¿Quienes pueden acceder a esos archivos, registros, bases o bancos de datos? Indicar por favor el nombre, apellido y cargo que desempeñan los funcionarios autorizados. En caso de tratarse de empleados de [Registro X], ¿hay distintas categorías que permiten distintos niveles de acceso? ¿Pueden acceder terceras personas ajenas al [Registro X] a la base de datos? En su caso, por favor identificar los terceros autorizados al acceso. En caso de existir de distintos archivos, registros, bases o bancos de datos, por favor precisar cada caso concreto. // ¿Cómo se accede a esos archivos, registros, bases o bancos de datos? Por ejemplo, nos interesa conocer los detalles técnicos del acceso, es decir, si ocurre por medio de ordenadores conectados a una red; si las personas autorizadas deben introducir una clave para acceder; si esa clave es personal; etcétera. Si esa clave se pierde, ¿cuál es el procedimiento para reestablecerla? ¿Queda asentado el inconveniente? ¿Dónde? En caso de existir distintos archivos, registros, bases o bancos de datos, por favor precisar cada caso concreto. // ¿Con qué tipo de garantías de seguridad cuentan esos archivos, registros, bases o bancos de datos del [Registro X]? Por ejemplo, nos interesa saber si están conectados a Internet y —en su caso— con qué tipo de medidas de seguridad cuentan esos archivos, registros, bases o bancos de datos para impedir intrusiones de personas no autorizadas. En caso de existir distintos ar-

dencias contestaron los pedidos pero en varias oportunidades lo hicieron invocando excepciones legales y entregando información de manera parcial. Sin embargo, del universo de respuestas obtenido y de información de fuentes secundarias es posible obtener una imágen aproximada de la forma en que el Estado maneja los datos de los ciudadanos. Del análisis de las respuestas surgen las siguientes conclusiones:

- En general, todas las bases de datos cuentan con distintos niveles de acceso según las categorías de empleados.
- Los servidores suelen estar localizados en las oficinas donde funcionan las dependencias respectivas.
- Las medidas de seguridad parecen estar vinculadas con la existencia de claves personales de los empleados, aunque en muchas ocasiones las dependencias se negaron a informar sobre medidas técnicas de seguridad.
- La seguridad depende del área de informática de cada dependencia.

Estas características surgen de varias de las respuestas ofrecidas por las dependencias públicas consultadas que contestaron los pedidos de acceso a la información. Cabe destacar que en ningún caso fue posible recibir información respecto de qué funcionarios están autorizados a acceder a los datos contenidos en las bases de datos, ya que las dependencias consideraron que esa información es parte de una de las excepciones al acceso a la información prevista en el Anexo VII al decreto 1172/03[16].

También se negó el acceso a datos sobre "detalles técnicos de acceso y/o medidas de seguridad adoptadas por el organismo" ya que consideró que

chivos, registros, bases o bancos de datos, por favor precisar cada caso concreto. // ¿Ha habido casos de extracción de información no autorizada? En caso de que haya habido, ¿cómo ha procedido el [Registro X] ante el conocimiento de ese hecho? En caso de que no haya habido intrusiones no autorizadas, ¿cuál sería el procedimiento a seguir en caso de que las hubiera? // ¿Quienes se ocupan de brindar soporte técnico frente a los distintos problemas que pudieran ocasionarse en los archivos, registros, bases o bancos de datos? // ¿Tienen estas personas acceso irrestricto a los archivos, registros, bases o bancos de datos? ¿A quién reportan? Indicar por favor el nombre, apellido y cargo que desempeña. // Cómo se procesan los pedidos de acceso a información del [Registro X] cuando son objeto de requerimiento por parte de otras autoridades? Por favor, diferenciar casos en los que se trate de autoridades pertenecientes al poder ejecutivo, legislativo o judicial (en caso de que haya diferencias)."

[16]Ver, por ejemplo, respuesta de Esteban F. de Gracia, Director del Registro Nominativo y Dactiloscópico del Registro Nacional de Reincidencia, 15 de enero de 2014 (copia en Archivo de la ADC).

esa negativa permitía "garantizar la seguridad y confidencialidad de los datos personales, conforme lo establecido por el artículo 9 de la ley 25.326"[17]. Sólo se informó, en varios casos y de manera genérica, sobre la existencia de distintas categorías de empleados con diferentes niveles de acceso[18]. Por ejemplo, el *Registro Nacional de Información de Personas Menores Extraviadas* (RNIPME) informó que el acceso es "por perfiles" (como *coordinadora*, *equipo social*, *abogados*, *técnicos*, *operadores*) y que "cada usuario [puede] realizar las operaciones correspondientes a su perfil y sólo sobre la información de su competencia"[19]. En el mismo sentido, el *Registro Nacional de Tierras Rurales* informó diversas categorías de operadores que pueden acceder al sistema (*operador*, *operador avanzado*, *operador avanzado con firma digital*) e indicó que todos ellos "han firmado compromisos de confidencialidad" con el Registro[20].

Algunas dependencias informaron sobre medidas de seguridad pero en términos muy generales. Por ejemplo, el Registro Nacional de Agricultura Familiar señaló que su base de datos se encuentra vinculada a Internet a través de "un sistema de seguimiento y carga" de las declaraciones juradas que integran el archivo y destacó que las medidas de seguridad están a cargo de la Dirección de Informática del Ministerio de Agricultura[21].

[17]Cfr. Respuesta de Esteban F. de Gracia, Director del Registro Nominativo y Dactiloscópico del Registro Nacional de Reincidencia, 15 de enero de 2014 (copia en Archivo de la ADC); respuesta de Inés García Holgado, Asesora legal de la Dirección Nacional de Derechos de Autor, del 10 de enero de 2014 (en archivo en la ADC) y respuesta de Manuel Enrique Pedreida, Director del Registro Nacional de Agricultura Familiar, del 7 de noviembre de 2013 (en archivo en la ADC); Respuesta del Registro Nacional de Tierras Rurales del Ministerio de Justicia de la Nación, del 22 de enero de 2014. Cabe destacar que el artículo 9 de la ley 25.326 en nada impide que se informe sobre las medidas de seguridad adoptadas, ya que él establece –en su parte pertinente– lo siguiente: "Artículo 9.1. El responsable o usuario del archivo de datos debe 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."

[18]Ver, por ejemplo, respuesta de la Dirección Naiconal de Derechos de Autor, donde se señaló que "sólo una parte del personal de la DNDA tiene autorizado el ingreso a ellos. Existen distintas categorías de agentes con distintos niveles de acceso y restricciones diferentes en cuanto a la manipulación de los datos y a la posibildiad de su carga o modificación. El acceso es controlado mediante un ingreso restringido con nombre de usuario y claves de carácter personal". Ver respuesta de Inés García Holgado, Asesora legal de la Dirección Nacional de Derechos de Autor, del 10 de enero de 2014 (en archivo en la ADC).

[19]Cfr. Registro Nacional de Información de Personas Menores Extraviadas. Informe de Gestión 2012 del 8 de abril de 2013. Disponible en: http://www.jus.gob.ar/media/774132/informe_de_gestion_2012.pdf.

[20]Cfr. Respuesta del Registro Nacional de Tierras Rurales del Ministerio de Justicia de la Nación, del 22 de enero de 2014 (en archivo en la ADC).

[21]Respuesta de Manuel Enrique Pedreida, Director del Registro Nacional de Agricultura Familiar, del 7 de noviembre de 2013 (en archivo en la ADC). Ver, también, Registro Nacional de Información de Personas Menores Ex-

Las dependencias que informaron sobre la ubicación de las bases de datos señalaron que las mismas se encuentran en los edificios donde funcionan las distintas reparticiones[22] aunque en algunos casos las bases se encuentran en las oficinas de otras dependencias[23]. En general, la seguridad es esas bases de datos está a cargo de oficinas técnicas en cada uno de los Ministerios donde funcionan[24], lo que parece sugerir que no hay un sistema centralizado de control o estándares unificados en materia de seguridad.

Una de las respuestas que se apartó de esta tendencia –tanto por las características de la información brindada como por su detalle– ha sido la de la Oficina Nacional de Contrataciones[25]. La ONC maneja dos importantes bases de datos relevantes para el proceso de contrataciones del Estado: el Sistema de Identificación de Bienes y Servicios y el Sistema de Información de Proveedores y de Transparencia, que contiene la información publicada en el sitio web de la oficina. La locación física de estas bases de datos se encuentra dispersa en tres localizaciones diferentes: en la *Sala Cofre* de la AFIP, en el *DMZ* de la Secretaría de Hacienda y en el *Data Center* de la Subsecretaría de Tecnologías de Gestión.

En todos estos casos, las bases de datos de la ONC son de acceso público irrestricto a través de la página www.argentinacompra.gob.ar. Sin embargo, cabe destacar que no es posible acceder a los datos brutos que integran la base de datos sino que es necesario proceder a través de distintos señaladores y filtros que permiten acceder a información específica.

Respecto de las personas que pueden acceder a la información, ello depende de las medidas de seguridad con que cuenta cada servidor. Por ejemplo, en la *Sala Cofre* de la AFIP sólo pueden acceder "personal autorizado de la AFIP que pertenece al área de soporte de base de datos", y lo hacen bajo solicitud de la ONC. También puede acceder personal de la ONC que trabaja en la Dirección de Sistemas de Información y Transparencia. En cuanto a la forma de acceso, el mismo es remoto "mediante un punto a punto entre la ONC y la sala cofre de la AFIP" y mediante el uso de "usuarios y contraseñas". Lo mismo ocurre con el DMZ de la Secretaría de Hacienda. La ONC no tiene acceso directo al Data Center de la Subsecretaría de Tecnologías de Gestión.

La *sala cofre* de la AFIP muestra medidas de seguridad relevantes para la protección de los datos: se trata de una sala protegida, ignífuga, con ga-

traviadas. Informe de Gestión 2012 del 8 de abril de 2013. Disponible en: http://www.jus.gob.ar/media/774132/informe_de_gestion_2012.pdf.

[22]Ver, por ejemplo, respuesta de Inés García Holgado, Asesora legal de la Dirección Nacional de Derechos de Autor, del 10 de enero de 2014 (en archivo en la ADC).

[23]Es el caso de la Oficina Nacional de Contrataciones.

[24]Ver, por ejemplo, la respuesta de Juan Carlos Nadalich, Secretario de Gestión y Articulación Institucional del Ministerio de Desarrollo Social, del 11 de noviembre de 2013.

[25]Respuesta de María Verónica Montes, Directora Nacional de la Ofincina Nacional de Contrataciones, del 6 de noviembre de 2013 (en archivo en la ADC).

rantías de seguridad y acceso restringido a personas especialmente autorizadas[26]. La sala incluye un sistema de monitoreo sobre el tráfico de la red y sobre los ataques informáticos que pueden poner en riesgo la seguridad de los datos allí contenidos. Según la AFIP, sufren entre "200.000 y 300.000 intentos de ataques diarios"[27].

Cabe destacar que la *sala cofre* de la AFIP incluye no sólo la información de la ONC sino datos de otras entidades –por ejemplo, Presidencia de la Nación– pero también información impositiva sobre las transacciones que los 8 millones de contribuyentes realizan con con la AFIP en tiempo real[28]. También incluye información sobre declaraciones juradas impositivas e "información exógena que [...] suministran otras entidades, como por ejemplo, tarjetas de crédito, bancos, registros de las propiedades inmuebles, automotor, todo eso está en la sala cofre"[29]. El dato es significativo, ya que las bases de datos con que cuenta el Estado suelen ser alimentadas por información que actores privados entregan a las autoridades públicas.

> "La entidad que comanda Ricardo Echegaray tiene una radiografía de los movimientos económicos de cada contribuyente, que alcanza hasta los consumos más frecuentes. Viajes, compras en comercios y por Internet, expensas, movimientos bancarios, resúmenes de tarjetas de crédito, transacciones en sitios como Mercado Libre, gastos en telefonía celular o en prepagas, entre otros conceptos son seguidos con detenimiento por los inspectores que cruzan datos en función de determinar si los gastos se corresponden con las declaraciones juradas, para detectar contradicciones y posibles sanciones"[30].

Este dato ratifica una política de *vigilancia* permanente permitida por los avances tecnológicos y por los deberes de información que pesan sobre distintos actores de la economía. Esas transferencias de información de actores privados a actores públicos es permitida, también, por la ley 25.326 que establece que no se necesita el consentimiento del titular de los datos cuando "así lo disponga una ley" o cuando ellos se "recaben para el ejercicio de funciones propias de los poderes del Estado o en virtud de una obligación legal"; o se trate de operaciones que "realicen las entidades financieras y de las informaciones que reciban de sus clientes conforme las disposiciones del artículo 39 de la Ley 21.526" (artículos 5 y 11 de la ley 25.326). Las entidades financieras deben ceder la información por disposición del artículo 39

[26]Cfr. Acción Impositiva. *El centro de computos de la AFIP*. (2010).
[27]Id.
[28]Id.
[29]Id.
[30]Cfr. Pagano, M. (2014). *La AFIP ya controla todos los gastos de los consumidores*. Diario Clarin. Consultado el 19 de julio de 2014.

mencionado, que permite esa sesión "a los organismos recaudadores de impuestos nacionales, provinciales o municipales sobre la base de las siguientes condiciones: (a) debe referirse a un responsable determinado; (b) debe encontrarse en curso una verificación impositiva con respecto a ese responsable, y (c) debe haber sido requerido formal y previamente". Sin embargo, respecto de los requerimientos de información que formule la AFIP, "no serán de aplicación las dos primeras condiciones de este inciso".

El ejemplo de la Ley de Entidades Financieras es significativo por la forma en que se concede la autorización: se establecen prohibiciones pero con excepciones generosas en materia de transferencia o acceso a información por parte de agentes estatales. Sigue una técnica legislativa similar a la ley 25.326 reseñada al comienzo de este trabajo que revela un patrón común: prohibiciones y garantías a los ciudadanos que no se aplican cuando interviene el Estado.

Esta situación de almacenamiento masivo e incorporación de información de actores privadas es problemática desde el punto de vista de la privacidad. Como señaló Beatríz Busaniche, de la Fundación Vía Libre:

> "Es inédita en la historia, la capacidad de registro y procesamiento de datos y también de cruce de esos datos. Capacidad de cálculo, desarrollos de software, avances que no tienen históricamente parangón. Y una cuestión que está en el eje es que el Estado no debe recopilar más datos que los estrictamente necesarios para el objetivo que debe cumplir. El punto central de una política pública en la cual la retención de datos es un instrumento para una medida, es tomar el mínimo de datos indispensable para cumplir el objetivo y que ese procesamiento de datos sea transparente al ciudadano que debe saber qué se hace con ese dato y, si no es indispensable, debe poder negarse a otorgarlo. El otro punto es que el organismo no es el dueño de los datos y debe ser garante de su privacidad y seguridad. A mí algo que me preocupa es que vos conociendo el CUIT de una persona en AFIP obtenés un montón de información personal, domicilio, categoría fiscal, eso es carne para los ladrones. La cantidad de gente que vende datos personales que chupa de la AFIP es atroz. El Estado no es dueño de nuestros datos y debe velar por la protección y cumplir con las garantías de la Constitución"[31].

La facilidad con que la información puede cederse entre distintas autoridades públicas y las múltiples obligaciones de información que operan sobre distintos actores de la economía generan, de todas formas, riesgos para la

[31] Cfr. Filozof, L. (2012). *El gran hermano fiscal*. Revista Veintitrés. Consultado el 19 de julio de 2014.

privacidad de los datos. De nada sirven las *salas cofres* o los sistemas de *DMZ* si la información allí contenida se comparte con actores estatales con prácticas o sistemas de seguridad menos seguros: la fortaleza de una cadena es determinada por su eslabón más débil, como veremos en la siguiente sección.

Antes de concluir con este análisis, sin embargo, resulta significativo analizar la acción de las DNPDP sobre las bases de datos estatales. La respuesta de la Dirección Nacional de Migraciones (DNM) fue significativa, ya que respondió a las preguntas adjuntando los registros de empadronamiento de sus bases de datos en la DNPDP. Analizarlos es relevante por lo siguiente: permite conocer el tipo de información que la DNPDP tiene sobre las bases de datos estatles.

Del análisis de esas actas de empadronamiento surge, por ejemplo, que la DNM tiene información en su registro de recursos humanos sobre las huellas dactilares de los empleados, la imagen, estado civil, títulos, oficio, sanciones, evaluaciones, historia clínica, informes preocupacionales, afiliaciones jubilatoria y afilación sindical. Todos esos datos "deben ser facilitados por su titular de manera obligatoria"[32]. Asimismo, se informa que esos datos se mantienen sin un plazo determinado –es decir, para siempre– y que se encuentran en un servidor central.

También es significativa la información sobre el *Registro de Admisión de Extranjeros* y el *Registro de Ingresos y Egresos de Personas al Territorio Nacional*: además de los datos personales señalados similares al registro de recursos humanos, ambos registros expresamente reconocen que realiza el tratamiento de datos sensibles y que planea efectuar cesiones de datos a terceros, cesiones *masivas*, interconexiones con otros bancos y transferencias internacionales[33]. Respecto de las medidas de seguridad, se informa que esos datos pueden ser tratados por 14 dependencias estatales, entre ellas Cancillería, Ministerio de Educación, INDEC, RENAPER, Secretaría de Turismo, la AFIP y todas las fuerzas de seguridad[34].

[32]Cfr. Memorandum No. 378/13 de la Dirección de Sistemas de la Dirección Nacional de Migraciones (en archivo en la ADC).

[33]Cfr. Memorandum No. 378/13 de la Dirección de Sistemas de la Dirección Nacional de Migraciones (en archivo en la ADC).

[34]Cfr. Memorandum No. 378/13 de la Dirección de Sistemas de la Dirección Nacional de Migraciones (en archivo en la ADC).

IV. El caso de las fotos del padrón

La acción judicial

El caso que relataremos a continuación muestra uno de los problemas que genera una ley permisiva hacia el tratamiento y cesión de información entre entidades estatales. Llegó a la ADC por el trabajo que –desde esta organización– hacemos en defensa de los derechos humanos en general, y del derecho a la privacidad en particular. Él funciona, en el marco de este informe, como un caso de estudio paradigmático que revela los riesgos para la privacidad que se pueden generar por el manejo inadecuado de la información de los ciudadanos.

El caso llegó a la ADC a través de Enrique Chaparro, presidente de la Fundación Vía Libre, quien encontró en el sistema de consulta en línea del Padrón Electoral que la información sobre el lugar en el que debería votar en las elecciones de octubre de 2013 incluía la fotografía de su DNI. Esa fotografía revelaba que la Cámara Nacional Electoral había recibido esa información del Registro Nacional de las Personas, la autoridad pública que almacena esa información por disposición del decreto-ley 17.671.

La primera aproximación de la ADC al problema fue considerar que se trataba de una cesión ilegítima que correspondía cuestionar, además, porque afectaba el principio de *finalidad* de la ley 25.326, que en su artículo 4.3 dispone que "[l]os datos objeto de tratamiento no pueden ser utilizados para finalidades distintas o incompatibles con aquellas que motivaron su obtención". Asimismo, también intuíamos que se había violado la prohibición de *cesión* dispuesta en el artículo 11 de la ley, que exige –para que ello sea posible– el "cumplimiento de los fines directamente relacionados con el interés legítimo del cedente y del cesionario" y 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".

Cuando comenzamos a analizar en profundidad la situación, vimos –sin embargo– que la situación era más compleja.

En efecto, pronto nos dimos cuenta que era posible argumentar que las autorizaciones amplias de almacenamiento, tratamiento y cesión de los datos personales entre organismos estatales podría ser invocada para justificar la cesión entre el Renaper y la Cámara Nacional Electoral. Como se explicó antes, el artículo 11.3.c de la ley 25.326 permite que las cesiones de datos se hagan sin el consentimiento de los titulares de datos cuando esa cesión "[s]e realice entre dependencias de los órganos del Estado en forma directa, en la medida del cumplimiento de sus respectivas competencias". Ese argumento era problemático ya que impedía cuestionar de manera directa la cesión en sí, aunque la misma era de todas formas atacable por la violación del prin-

cipio de *finalidad* antes expuesto. De todas formas, fuimos a buscar al acto que había incorporado al padrón las fotografías de los ciudadanos.

La primera norma que encontramos al respecto fue la acordada 18/13 de la Cámara Nacional Electoral, de marzo de 2013. Esa acordada dispuso sumar la fotografía de los electores y electoras al sistema de padrón on line provisorio que podía consultarse en el sitio www.padron.gob.ar. La Acordada también aprobó nuevos modelos de padrones para utilizar en las elecciones que incorporían la fotografía de los electores para el llamado "padrón especial" que es el que está a disposición del presidente de cada mesa electoral.

La ampliación de los datos que debe contener el Registro Nacional de Electores por medio de una acordada judicial nos parecía problemática: esa ampliación, al afectar derechos constitucionales como el de la privacidad y el ejercicio del derecho al voto, debe ser dispuesta por una ley. Pero esa ley existía: el artículo 3 de la ley 26.774 de noviembre de 2012, por medio de la cual se extendió el derecho al voto a los menores de 16 años, modificó el artículo 15 del Código Electoral Nacional (CEN), el cual quedó redactado de la siguiente manera en su parte pertinente:

> "El Registro Nacional de Electores consta de registros informatizados y de soporte documental impreso. El registro informatizado debe contener, por cada elector los siguientes datos: apellidos y nombres, sexo, lugar y fecha de nacimiento, domicilio, profesión, tipo y número de documento cívico, especificando de qué ejemplar se trata, fecha de identificación y datos filiatorios. Se consignará la condición de ausente por desaparición forzada en los casos que correspondiere. *La autoridad de aplicación determina en qué forma se incorporan las huellas dactilares, fotografía y firma de los electores*. El soporte documental impreso deberá contener además de los datos establecidos para el registro informatizado, las huellas dactilares y la firma original del elector, y la fotografía" (el destacado nos pertenece).

Ello significa que el Congreso de la Nación delegó en la Cámara Nacional Electoral, como autoridad de aplicación del régimen electoral argentino, la posibilidad de incorporar huellas dactilares, fotografías y firmas, todos datos contenidos en el DNI y en manos del Renaper, organismo que –en virtud del artículo 17 del Código Nacional Electoral– debe

> "remitir al Registro Nacional de Electores, en forma electrónica los datos que correspondan a los electores y futuros electores. Sin perjuicio de ello, debe remitir periódicamente las constancias documentales que acrediten cada asiento informático, las que quedarán en custodia en forma única y centralizada, en la Cámara

> Nacional Electoral. (…) La Cámara Nacional Electoral podrá reglamentar las modalidades bajo las cuales el Registro Nacional de las Personas deberá remitir la información, así como también los mecanismos adecuados para su actualización y fiscalización permanente, conforme lo previsto en la presente ley, y de acuerdo a la posibilidad de contar con nuevas tecnologías que puedan mejorar el sistema de registro de electores."

Como vemos, no era necesario para el Estado argumentar que la transferencia de información había sido realizada por las autorizaciones amplias que concede la ley 25.326: había leyes específicas que la autorizaban.

En la acordada 18/13, la Cámara Nacional Electoral explicaba que la incorporación de las fotografías se haría a modo de prueba piloto:

> "del mismo modo, y teniendo en consideración que la incorporación de fotografías se efectuaría –como se resaltó– a modo de prueba piloto, es conveniente prever que en ese supuesto se incorpore también la fotografía al padrón provisional –tanto en su versión impresa como para su exhibición en Internet– a fin de que los electores dispongan con suficiente antelación de una ocasión para realizar oportunamente las observaciones que correspondan"[35].

Según informó el Centro de Información Judicial, el banco de datos del padrón en línea contenía las fotografías de 9.338.672 electores, es decir, un 30,59 por ciento de todos los electores inscriptos en el padrón nacional definitivo[36].

La situación era seria. Como explicó la ADC en su acción de amparo, "las imágenes fotográficas del rostro de más de nueve millones de ciudadanos están disponibles en Internet y, en consecuencia, a ellas puede acceder cualquier persona que conozca un mínimo conjunto de datos personales que, por otra parte, pueden ser obtenidos con relativa sencillez e incluso pueden ser objeto de un procedimiento de recuperación automatizada de datos".

Los argumentos de la ADC

El derecho a la privacidad

El argumento de la ADC se construyó sobre el derecho a la privacidad reconocido por la Constitución y por tratados internacionales de derechos hu-

[35]Cámara Nacional Electoral. Acordada 18/13. Considerando 7.

[36]Cfr. CIJ. (2013). *Más de 9 millones de electores tienen su fotografía en los padrones*.

manos incorporados a ella con jerarquía constitucional.

> "En el ordenamiento jurídico argentino, el derecho a la privacidad es un derecho amplio que incluye –a la vez– una dimensión vinculada a la autonomía personal y otra vinculada a la intimidad. En el primer sentido –más amplio y generoso y receptado por el artículo 19 de la Constitución– de lo que se trata es de 'asegurar que cada individuo pueda estar en condiciones de desarrollar su propia vida, conforme a sus propias decisiones'. El segundo sentido es más limitado y se ve reflejado por el artículo 18 de la Constitución cuando éste establece que '[e]l domicilio es inviolable, como también la correspondencia epistolar y los papeles privados; y una ley determinará en qué casos y con qué justificativos podrá procederse a su allanamiento y ocupación.' Como explica Nino, se trata de 'una esfera de la persona que está exenta del conocimiento generalizado por parte de los demás'. Esa esfera se expande más allá del domicilio o los papeles en sentido estricto, e incluye a todas las comunicaciones entre los ciudadanos y a diversos aspectos de la personalidad y espacios respecto de los cuales es posible sostener una 'razonable expectativa de privacidad'.
>
> El derecho a la privacidad es –además– un derecho fundamental para poder desarrollar la ciudadanía democrática. Sin el derecho a decidir sobre la propia vida y sin un espacio ajeno a la mirada de los otros, ciertas libertades básicas que hacen al núcleo de la ciudadanía democrática no podrían ejercerse de manera plena. Por ejemplo, derechos como la libertad de expresión, la libertad de reunión o de asociación no pueden ejercerse explotando toda su potencialidad si –por ejemplo– los ciudadanos son objeto de medidas de control o vigilancia por parte del Estado. En el mismo sentido, la autodeterminación informativa que garantizan las leyes de protección de datos personales también tiene por objeto resguardar un espacio 'privado' necesario para la plena autodeterminación y para no ser objeto de actores de terceros que pueden coartar esa libertad fundamental"[37].

La ADC consideró que el tratamiento descuidado del Estado sobre las fotografías de los ciudadanos y ciudadanas registradas con motivo del Documento Nacional de Identidad (DNI) ponía en riesgo la autonomía de esas

[37] Acción de Hábeas Data Colectivo presentada por la ADC. Las citas internas pertenecen a Gargarella, R. (2008). *Constitucionalismo y Privacidad*. En Teoría y Crítica del Derecho Constitucional (1a. ed., Vols. 1-2, Vol. II, pp. 779–793). Buenos Aires: Abeledo-Perrot y Nino, C. S. (1992). Fundamentos de derecho constitucional: análisis filosófico, jurídico y politológico de la práctica constitucional. Astrea.

personas en tanto les impide tener un control adecuado sobre un dato personalísimo y sensible como es la fotografía de sus respectivos rostros. Además, al publicarse en un sistema de acceso abierto, cualquier persona con un mínimo de datos sobre la persona podía acceder a ella lo que hace que un dato personal y sensible pase al conocimiento generalizado de los demás, como definía Nino a la intimidad[38].

El derecho a la propia imagen y los riesgos creados

Asimismo, la ADC argumentó que además de esa afectación directa a los derechos a la privacidad y la intimidad, el mal manejo de los datos personales y sensibles que se encuentra en manos del Estado genera una afectación indirecta más amplia, toda vez que aumenta los riesgos de que terceros utilicen esa información de un modo violatorio de derechos.

> "La posibilidad de que el Estado o que empresas privadas accedan a los datos sensibles de los ciudadanos nunca ha sido tan grande. En efecto, la descuidada publicación en Internet de la fotografía de –según se informa– más del 30 por ciento del padrón electoral importa una cesión de facto de esa información a terceros que podrían compilar esos datos e integrarlos a bases de datos que podrían utilizarse con fines ilícitos"[39].

Estos argumentos fueron sostenidos sobre la protección de la *imagen* como una forma especial de protección del derecho a la privacidad[40]. Pero además, se señaló la dimensión negativa del *derecho a la propia imagen*, que consiste en el derecho a excluir la obtención, reproducción y publicación de la misma por un tercero que carece del consentimiento del titular.

En este sentido, el Supremo Tribunal español ha sostenido que la protección de la imagen "se salvaguarda reconociendo la facultad de evitar la difusión incondicionada de su aspecto físico, ya que constituye el primer elemento configurador de la esfera personal de todo individuo, en cuanto instrumento básico de identificación y proyección exterior y factor imprescindible para su propio reconocimiento como sujeto individual"[41].

[38]Cfr. Nino, op. cit., pág. 304 y ss.

[39]Cfr. Acción de Hábeas Data Colectivo presentada por la ADC.

[40]Cfr. Human Rights Council. *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue*. A/HRC/17/27. 16 de mayo de 2011, párr. 58.

[41]Cfr. SSTC 231/1988; 99/1994; 81/2001; 139/2001; 156/2001; 83/2002.

La imagen como dato *sensible*

La ADC argumentó que las imagenes son, en muchos casos, datos que cabe definir como sensibles en los términos de la ley 25.326, que los define como "datos personales que revelan origen racial y étnico, opiniones políticas, convicciones religiosas, filosóficas o morales, afiliación sindical e información referente a la salud o a la vida sexual".

El rostro de las personas puede revelar –al menos en muchos casos– su origen racial o incluso religioso. En efecto, prácticas deleznables de discriminación racial como las leyes de Jim Crow en los estados del sur de los Estados Unidos o el *apartheid* sudafricano se basaban, casi exclusivamente, en el color de la piel de las personas. Este tipo de datos –por el riesgo que conllevan para la autonomía personal– merecen estándares de protección más elevados que los datos personales comunes. La posibilidad de que se puedan conformar bases de datos con la raza o etnia de los ciudadanos y ciudadanas y que esa información pueda ser analizada o clasificada de manera automática por medio de algoritmos que detectan ciertos rasgos faciales da cuenta del tipo de riesgos que importa tratar de manera descuidada datos personales como los involucrados en este caso.

Esta posibilidad se ve acrecentada por los sistemas automatizados de reconocimiento facial. Esto es posible mediante un análisis de las características faciales del sujeto extraídas de la imagen que son contrastadas en línea con otras imágenes alojadas en una base de datos. En la práctica, se toma una imagen facial "desconocida" y se la compara con una imagen de la misma cara en un conjunto de imágenes "conocidas". En el caso bajo análisis, las imágenes que son subidas al padrón en línea pertenecerían al grupo de imágenes conocidas, acompañadas por una serie datos que permiten individualizar a la persona que se trate (nombre, apellido, DNI, sección y circuito electoral).

La violación de los principios de *finalidad* y *proporcionalidad*

La incorporación de fotografías al Registro Nacional Electoral producto de una cesión del Renaper violó el principio de finalidad que es un eje fundamental en toda regulación sobre protección de datos personales. Ese principio establece en el artículo 4.3 de la Ley 25.326 que "[l]os datos objeto de tratamiento no pueden ser utilizados para finalidades distintas o incompatibles con aquellas que motivaron su obtención". En efecto, las fotografías del nuevo DNI fueron brindadas para incorporarse a las bases de datos del Renaper y ser utilizadas en los nuevos documentos. La utilización de esta información para conformar el Registro Nacional Electoral importa una clara finalidad distinta en los términos de la Ley 25.326 y se encuentra, en

consecuencia, prohibida por el texto legal.

Se trata de dos registros diferentes con finalidades jurídicas distintas. En el primer caso, se trata del Registro que creó el decreto-ley 17.671 con el objeto de reunir información sobre toda la población argentina y para el ejercicio de las facultades y atribuciones que reconoce el artículo 2 de dicha norma legal. En el segundo, se trata del Registro Nacional de Electores, establecido por el Código Electoral Nacional y el que tiene por objeto registrar a los ciudadanos argentinos con derecho a voto, con la finalidad de confeccionar los padrones electorales. Desde nuestro punto de vista, las evidentes finalidades distintas entre ambos registros hacen que la información recabada por uno no pueda ser utilizada para los fines del otro.

Además, la incorporación de la fotografía viola el principio de *proporcionalidad* que también es un eje central de todo marco protectorio de los datos personales. En efecto, el almacenamiento y uso de datos personales importa una afectación al derecho a la privacidad y como tal debe ser sometido a un análisis de proporcionalidad estricto[42]. Es el Estado, en consecuencia, quien debe justificar por qué la incorporación de las fotografías de los ciudadanos al Registro Nacional Electoral para conformar los padrones electorales es en efecto necesaria y busca satisfacer un objetivo legítimo del Estado. Si el sistema electoral funcionó bien durante años con datos mínimos, una expansión de esos datos importa una injerencia mayor sobre el derecho a la privacidad. Y esa injerencia mayor era, para la ADC, constitucionalmente sospechosa toda vez que no hay motivos aparentes respecto del funcionamiento del sistema electoral que permitan suponer que el cambio es en efecto necesario desde el punto de vista constitucional.

La ADC cuestionó, entonces, la constitucionalidad de los artículos 15 y 17 del Código Electoral Nacional en tanto disponen la incorporación de la fotografía a los padrones informáticos y la remisión de información del Renaper al Registro Nacional de Electores. También se cuestionó la constitucionalidad de la acordada 18/13 de la Cámara Nacional Electoral que articula la incorporación y organización de las fotografías de los electores a los padrones; sin las debidas previsiones legales y constitucionales del caso.

Falta de consentimiento e información

Si bien, como se señaló, la cesión de datos estaba autorizada por ley, de todas formas cuestionamos que no se haya respetado el deber de *información* que debe acompañar a esa sesión: consideramos que ese deber –que surge

[42]Cfr. Human Rights Council. *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue*. A/HRC/17/27. 16 de mayo de 2011.

del artículo 11 de la ley 25.326– es independiente de la obtención previa del consentimiento. Ese deber de información permite que los ciudadanos conozcan quien almacena y da tratamiento a sus datos personales, lo que les permite mantener cierto grado de control sobre los mismos y vigilar que no se haga un mal uso de ellos.

La inseguridad de la base de datos

Finalmente, gran parte del argumento de la ADC se fundaba en una cuestión particular respecto de cómo los datos habían sido subidos a una base de datos en línea para la consulta de los ciudadanos. En efecto, la ADC señaló que las garantías de seguridad de la base de datos que alimentaba al sitio del consultas de padrón electoral eran insuficientes y que, entonces, toda la información allí contenida estaba en riesgo, lo que obligaba al Estado a tomar medidas urgentes de protección.

En efecto, la información contenida en el padrón electoral en línea había sido replicada en sitios privados alojados en el extranjero[43]. Según la ADC, "el descuido con que la Cámara Electoral ha manejado estos datos ya ha puesto en efectivo riesgo a los mismos, afectando así los derechos a la privacidad y a la intimidad de todos los electores y electoras".

Los hechos posteriores

Las advertencias sobre las falencias en la seguridad de la base de datos se comprobaron a las pocas semanas de presentada la acción de hábeas data colectivo por parte de la ADC, sin que la jueza intervinente hubiera tomado las medidas precautorias que se le habían solicitado. En efecto, de manera previa a que la ADC presentara su acción se habían detectado falencias: en agosto de 2013 el blog *Segu-Info* denunció al *Computer Emergency Response Team* de Argentina (ArCERT) la situación de vulnerabilidad de la base de datos sin que las autoridades pertinentes tomaran ninguna medida. Esa situación de vulnerabilidad había sido denunciada también por Enrique Chaparro en una carta enviada a la Cámara Nacional Electoral, que lo único que hizo con su denuncia fue dar de baja –de manera provisoria– su fotografía del sistema de consulta en línea.

Luego de la acción de amparo presentada por la ADC, esa vulnerabildad hipotética se hizo real: en octubre de 2013, un joven de 16 años descubrió la forma en que el sitio de consultas del padrón se comunicaba con la base de datos de la Cámara Nacional Electoral. En particular, el joven detectó cómo

[43]Por ejemplo, el sitio www.argentinaelecciones.com.

la aplicación de la Cámara Nacional Electoral para sistemas Android se comunicaba con una base de datos alojada en un servidor del Ministerio del Interior, bajo un sistema de encriptación de *base64* que –como denunciaba el joven– es "un algoritmo de encriptación reversible, es decir, no seguro"[44]. Como la aplicación para Android estaba programada en Java, el código original era fácilmente accesible y así se podía verificar que el sistema de encriptación lo único que hacía era reemplazar ciertas letras por otras.

> "Pasando este pseudo-código a cualquier lenguaje de programación, se pueden realizar *queries* arbitrariamente a la base de datos del Padrón, con los riesgos que esto conlleva: podemos pedir la información de cualquier persona, por ejemplo, del DNI número 1 (…) sin otorgar ninguna otra información, solo un número de DNI y el sexo, sin *captcha*, sin nada que nos limite" (los destacados nos pertenecen)[45].

Luego de esta advertencia, a los pocos días alguien publicó de manera anónima en el sitio Jsfiddle.net un código completo que podía ser ejecutado desde el mismo sitio y que permitía obtener las fotografías del padrón electoral. El área de *Privacidad* de la ADC ejecutó ese código durante una noche y obtuvo la fotografía de más de 5,000 ciudadanos argentinos. Entregó esa información como parte de la evidencia en el marco de la acción de amparo presentada, que aún continúa sin sentencia definitiva. La Cámara Nacional Electoral dio de baja el sistema cuando la noticia de la vulnerabilidad llegó a los medios de comunicación.

En el marco del proceso, la jueza interviniente solicitó un informe a la *División Delitos Tecnológicos* (DDT) de la Policía Federal para que determine si la filtración denunciada por la ADC era en efecto factible. El informe del 10 de junio de 2014 es escueto: en dos fojas se limita a explicar que los técnicos de la DDT ingresaron a los sitios donde se había subido el código que permitía la descarga de las fotografías del pardón electoral. La DDT, al respecto, dijo lo siguiente:

> "Cabe señalar que a fin de resalizar la maniobra, debe utilizarse el código tal y cual fue publicado, en cualquier servidor de contenidos de internet, ya que el mismo, se trata de **código simple de programación**, no incurriendo en ninguna técnica de extracción de datos conocidas como 'INYECCIÓN SQL' o similar, sino, es un código que aprovecha la programación del sitio, poniendo

[44]Cfr. Another Bit in the Wall. Entrada del 20 de octubre de 2013.
[45]Id.

> en evidencia la seguridad del mismo" (el destacado nos pertenece)[46].

Como puede observarse, el peritaje ordenado por la Justicia verificó que la denuncia realizada era verídica: el código de programación era esencialmente vulnerable y la fotografía de millones de argentinos fue puesta a disposición de cualquier persona con mínimos conocimientos de programación. Al cierre de este informe aún no había sentencia de primera instancia.

V. Conclusión y recomendaciones

El presente informe ha procurado echar luz sobre la forma en que el Estado maneja nuestros datos personales. Si bien es posible verificar prácticas de seguridad adecuadas en algunos casos –como la *sala cofre* de la AFIP– también es posible ver cómo esas prácticas no son el resultado de políticas públicas implementadas por la autoridad a cargo de la protección de los datos de los argentinos: la Dirección Nacional de Protección de Datos Personales (DNPDP). Este organismo, que fue pensado para ser autárquico e independiente, ha sido limitado en su capacidad de acción por bajas asignaciones presupuestarias y de recursos humanos. Asimismo, su accionar ha mostrado un sesgo considerable hacia el control –limitado, por las razones antes mencionadas– sobre actores privados: el Estado parece estar ausente de la mirada de la DNPDP y ello es posiblemente el resultado de las amplias autorizaciones que concede la ley 25.326 al tratamiento y manejo de datos personales dentro del Estado. Así es como cuando la DNPDP se acerca a uno de los problemas graves en materia de datos –como los creados por los sitios que emiten informes sobre personas privadas– sólo araña la superficie: en el marco de procesos sancionatorios complejos, con limitades capacidad de acción, no puede ir al fondo del asunto, que se vincula con el mal manejo de los datos personales que hace el Estado.

El caso del padrón electoral en línea es sólo un ejemplo de ese mal manejo, que es –sin embargo– muy revelador.

En efecto, el caso revela que las medidas de seguridad se verían fortalecidas si se siguiesen criterios uniformes: si los datos –por ejemplo– del Renaper están en una *sala cofre*, todo ese esfuerzo de protección es inútil si la información se transifere a actores que tienen prácticas inseguras como las que implementó la Cámara Nacional Electoral. Esos criterios unificados de seguridad no parecen estar presentes: en los pedidos de acceso a la información

[46]Oficio judicial de la Policía Federal Argentina. Dirección de Lucha contra el Crímen Organizado. División de Delitos Informáticos. Recibido el 14 de junio de 2014 en el Juzgado Federal No. 1 a cargo de María Romilda Servini de Cubría, en el marco de la causa "ADC c. Cámara Electoral s/ amparo ley 16.968, Expediente 3246/13".

realizados por la ADC se señaló, de manera invariable, que la seguridad de los servidores dependen de las áreas técnicas de cada ministerio. Desconocemos si esas áreas técnicas están coordinadas pero, como revela el caso del padrón, no parecen estarlo.

Asimismo, es notable cómo el proceso de transferencia y cesión de datos de Renaper a la Cámara Nacional Electoral pasó completamente desapercibido para la DNPDP. Esto tiene que ver, probablemente, con las autorizaciones legales que existieron en ese caso y –con el hecho, también significativo– de que nadie haya considerado necesario solicitar a la DNPDP un dictamen sobre esa tranferencia. Hasta donde sabemos, la DNPDP tampoco intervino de oficio. La permisibilidad de la ley hacia el Estado y una autoridad de aplicación jerárquicamente subordinada son condiciones que obstaculizan, en lugar de favorecer, el rol de control y defensores de los derechos que debe cumplir la DNPDP.

Finalmente, cabe destacar que el rol de control de la DNPDP y las facultades y funciones que le asignan la ley exceden ampliamente su estructura y presupuesto. Más allá de las falencias de diseño de la ley –como consecuencia del veto presidencial cuando fue sancioanda– lo cierto es que esa situación de debilidad fue ratificada, año tras año, a través de las asignaciones presupuestarias. La DNPDP simplemente carece de los recursos para hacer lo que la ley espera de ella.

Este informe arroja, al menos de manera parcial, ciertas conclusiones que permiten pensar en una agenda de defensa y protección del derecho a la privacidad hacia el futuro. Esta agenda no puede ser el resultado, simplemente, del diagnóstico de una organización –como la ADC en este caso– que ha buscado observar el funcionamiento del sistema de protección de datos en la práctica. Esa agenda debe ser el resultado de un diálogo fluido entre distintos actores interesados en la defensa de un derecho fundamental en una demoracia moderna. Este informe busca ser un aporte en esa discusión que estimamos necesaria. Lo concluimos con algunas recomendaciones que –creemos– pueden informar a un proceso de discusión sobre una agenda en materia de privacidad para los próximos años.

VI. Recomendaciones

- **La propia ley 25.326 merece ser revisada**. En efecto, la autoridad de aplicación que ella crea debe ser auténticamente independiente y se debe garantizar un adecuado financiamiento de la misma, para que pueda cumplir con las importantes funciones de defensa de los derechos que la ley le asigna. Sería conveniente explorar los modelos de *Comisionados de Privacidad* de algunos países anglosajones, que parecen haber tenido éxito en la defensa de los datos personales de los

ciudadanos.

- **La revisión de la ley 25.326 no se puede hacer de manera aislada**. La ADC considera que es necesario, además, que ese análisis se haga de cara a una ley de Acceso a la Información Pública. Ambos derechos –el acceso y la protección de datos– pueden entrar en conflicto y creemos que es necesario que el marco legal argentino de cuenta de la tensión entre ambos y determine, con el mayor grado de certeza posible, los casos en los que debe primar el acceso y aquellos en donde el resguardo de la privacidad se impone.

- **Es necesario limitar las capacidades de almacenamiento y cesión de datos dentro del Estado**. La ley actual es, como se dijo, demasiado permisiva. Esto permitiría, no sólo mantener un control más estrícto sobre los actores estatales sino evitar los riesgos de que esos datos caigan en manos y sean explotados por actores privados con fines comerciales o de otro tipo.

- **Es necesario trabajar en la transparencia y unificación de criterios de seguridad**. Sería deseable que un organismo público, tal vez la Oficina Nacional de Tecnologías de Información, establezca criterios unificados de seguridad. Y ellos deberían ser públicos: a diferencia de la opinión de la DNPDP que impidió revelar ciertos detalles de las garantías de seguridad, el conocimiento sobre esas garantías no genera vulnerabilidades para los sistemas sino que permite que los ciudadanos evalúen si sus datos tienen el nivel de protección que merecen.

Referencias

[1] Juan Antonio Travieso María del Rosario Moreno. La protección de los datos personales y de los sensibles en la ley 25.326. *La Ley*, (14/07/2006), Julio 2006.

[2] Roberto Gargarella. Constitucionalismo y privacidad. En Roberto Gargarella, editor, *Teoría y Crítica del Derecho Constitucional*, volume II, páginas 779–793. Abeledo-Perrot, Buenos Aires, 1a. edición, 2008.

[3] Carlos Santiago Nino. *Fundamentos de derecho constitucional: análisis filosófico, jurídico y politológico de la práctica constitucional*. Astrea, 1992.

Índice

Índice de cuadros

ADC / Asociación por los Derechos Civiles

Este trabajo fue realizado por el área de Privacidad de la Asociación por los Derechos Civiles, como parte de la Cyber Stewards Network del Citizen Lab de la Universidad de Toronto y con el apoyo financiero del International Development Research Center, Ottawa, Canadá.