may / 15

Si nos conocemos más, nos cuidamos mejor

Informe sobre políticas de biometría en la Argentina.

ADC / Asociación por los Derechos Civiles

policy paper

ADC / Asociación por los Derechos Civiles

policy paper

Si nos conocemos más, nos cuidamos mejor. Informe sobre políticas de biometría en la Argentina.

Mayo de 2015

En los últimos años hemos visto, desde la Argentina, la expansión de distinto tipo de políticas de recolección, almacenamiento y procesamiento de datos biométricos de los ciudadanos. Estas políticas han avanzado de manera sigilosa, sin un alto impacto en la agenda pública y sin que surgieran voces que alertaran sobre los riesgos que ellas acarrean para nuestra privacidad. En parte, ello tiene razones históricas: las nuevas políticas de identificación importan una actualización tecnológicas sobre viejas prácticas aceptadas y no cuestionadas por los ciudadanos. Los avances tecnológicos hacen que esas políticas sean más efectivas, pero a la vez crean nuevos riesgos para los derechos humanos.

Esta pequeña investigación busca conocer el estado actual del desarrollo de las políticas de identificación biometrica en la Argentina. Desde nuestro punto de vista, ellas implican riesgos que no han sido debidamente ponderados. El informe procede de la siguiente manera.

En la primera parte se presentan conceptos básicos sobre mecanismos de identificación biométrica. El objeto es introducir al debate público información sobre una tecnología en pleno proceso de desarrollo, expansión y perfeccionamiento. Del análisis tecnológico, y como segundo paso, pasamos al análisis de las políticas de identificación biométrica en la Argentina, uno de los países pioneros en la adopción de este tipo de mecanismos de registro y clasificación de la población. El análisis de esa historia sugiere dos conclusiones: por un lado, que el marco normativo que regula la recolección de

datos de los ciudadanos con fines de "clasificación" tiene un bajísimo *pedigree* democrático que lo vuelve sospechoso; por el otro, que se trata de un régimen legal que establece políticas de *normalización* a las cuales los Argentinos, a diferencia de lo que ocurre en otros países, se han acostumbrado.

En la tercera parte analizamos los problemas involucrados en este tipo de políticas, que son de un triple orden: (a) las políticas de normalización, disciplinamiento y control que este tipo de prácticas favorece; (b) los riesgos que esta clase de registros significan para los derechos de los ciudadanos y (c) los débiles marcos legales que limitan el alcance del poder del Estado en el desarrollo de las mismas.

Finalmente, en la cuarta parte analizamos la más reciente encarnación de las políticas de registro de los ciudadanos: el Sistema Federal de Identificación Biométrica para la Seguridad (SIBIOS) creado en 2011 que tiene por objeto unificar información hoy dispersa en una sola base de datos. Cuando el sistema fue anunciado generó alarma a nivel internacional pero poca cobertura a nivel local: el video oficial que lo presentaba anunciaba a los ciudadanos argentinos que pronto todos sus datos personales capaces de identificarlos iban a estar en una sola base de datos, a la que podrían acceder de manera remota cientos de miembros de fuerzas de seguridad y que pronto podría contener registros sobre nuestra forma de caminar o nuestro ADN. Ese video que la Dirección Nacional de Migraciones transmitía en las salas de ingreso y egreso del país generó que, por ejemplo, el activista Richard Stallman anuncie que no regresaría a la Argentina hasta tanto el sistema sea desmantelado. Esta investigación sugiere que el sistema no se encuentra, todavía, suficientemente implementado. Ello es una buena noticia para los derechos de los ciudadanos ya que significa que aún es posible impedir el desarrollo de esas capacidades en el Estado o establecer controles estríctos que hoy están ausentes.

I. La biometría: conceptos básicos

La biometría es el reconocimiento autómatico de los individuos con base en sus características biológicas y de comportamiento (Pato y Millet, 2010). Es una herramienta para identificar a las personas y se basa en la premisa de que cada individuo es único y posee rasgos que lo distinguen de todos los demás. La biometría utiliza lo que las personas *son* para identificarlas. A diferencia de los sistemas que se basan en algo que ellas *saben* –como una contraseña– o que ellas *tienen* –como una llave– los sistemas biométricos actúan sobre el cuerpo de las personas y pueden utilizarse sin el consentimiento de ellas.

Existen distintas técnicas de análisis biométricos.

- **Estáticas**. Se basan en características físicas de las personas. La imagen del rostro, las huellas dactilares y el iris de los ojos suelen ser las "fuentes" de extracción de "datos" más utilizadas para producir identificaciones. A través de programas de reconocimiento facial, por ejemplo, es posible "identificar" a una persona de acuerdo a la distancia que hay entre su nariz, su boca, sus ojos. Todo lo que se necesita es una fotografía de esa persona para ser analizada y confrontada con una base de datos que vincule a determinado rostro con una persona en particular.
- **Dinámicas**. Se concentran en el análisis del comportamiento, la forma de caminar, el modo en que una persona firma, la forma en que utiliza el teclado de una computadora, etcétera. Estas técnicas analizan las acciones comunes de los individuos con el objeto de detectar patrones de conducta que puedan vincularse a una persona en particular.
- **Mixtas**. Como, por ejemplo, el patrón de voz, que combina técnicas estáticas —características fisiológicas de los apéndices que se utilizan en la creación del sonido– y dinámicas, como el comportamiento del discurso.

Todas estas herramientas arrojan resultados en términos de probabilidad: la identificación nunca es perfecta y los sistema biométricos deben analizarse teniendo en cuenta este dato fundamental. Pato y Lynette señalan numerosas fuentes de incertidumbre y variación en los sistemas biométricos. Una de ellas se vicula a los cambios en las personas como consecuancia de, por ejemplo, enfermedades, envejecimiento, cirugías, ectétera. Según los autores, "cada interacción del individuo con el sistema en el momento del registro e identificación estará asociada a *diferente* información biométrica" (Pato y Millet, 2010: 3). Ello produce incertidumbre en el sistema. La calidad, edad y calibración de los sensores que se utilizan para capturar los datos biométricos también impactan en el proceso de identificación. La calidad de la información que se utiliza para producir las identificaciones puede degradarse con el tiempo o corromperse como consecuencia de fallas de seguridad, etcétera (Pato y Millet, 2010: 4).

Además de esos elementos que generan incertidumbre respecto de la calidad de los resultados y la eficacia de los sistemas de biometría, los expertos también señalan que éstos requieren necesariamente de procesos de toma de decisiones, tanto por parte del sistema automatizado como por parte de los humanos encargados de interpretar sus resultados (Pato y Millet, 2010: 4). Una *identificación biométrica positiva* no significa *realmente* una identificación positiva, sino "una probabilidad de identificación correcta" (Pato y Millet, 2010: 4). La diferencia es sutil pero fundamental, especialmente cuando los sistemas de identificación biométrica son una pieza clave en procesos de distribución de derechos, recursos y penalidades.

Estas características de los sitemas de biometría no los hace necesariamente inútiles: para determinadas cuestiones, un juicio probabilístico puede ser suficiente si arroja resultados satisfactorios en un número elevado de casos. Pero las tecnologías de identificación biométricas son esencialmente imperfectas y ello nos obliga a analizar con cuidado su uso cuando el mismo puede poner en riesgo los derechos de las personas. Como sugerimos en este trabajo, ello ocurre cuando estas tecnologías se convierten pasos previos al acceso a derechos, beneficios u obligaciones. En estos casos, es imprescindible que el Estado demuestre que las tecnologías que implementa son *necesarias* y que no hay ninguna alternativa que afecte menos los derechos de los ciudadanos y pueda alcanzar los objetivos que se presiguen.

Resulta, en este sentido, interesante ver cómo Pato y Lynette reflexionan sobre el desarrollo de estos sistemas.

> "El desarrollo exitoso [de sistemas biométricos] tiene un buen manejo y definiciones de metas, alineación de capacidades biométricas con las necesidades y el ambiente operativo, y cuentan con análisis de amenazas y riesgos. Los fracasos muchas veces tienen que ver con falta de claridad acerca del problema que se busca resolver (…) y el uso inadecuado de tecnologías biométricas cuando otras tecnologías serían mejores, la elección incorrecta del tipo de tecnología biométrica, falta de sensibilidad respecto de las percepciones de los usuarios y los requisitos de usabilidad, falta de soporte técnico adecuado y falta de entendimiento de la población que va a ser sometida al sistema. Los comportamientos de los usuarios, las actitudes y la usabilidad del sistema contribuye a las identificaciones falsas y la manera en que se lidia con los resultados incorrectos o indeterminados es clave para que los sistemas alcancen objetivos" (Pato y Millet, 2010: 9).

Este punto se vinculan con la eficacia de los sistemas biométricos. Pero también es necesario realizar consideraciones previas a la implementación vinculadas al impacto que ellos pueden tener en el acceso a derechos y beneficios o en la aplicación de determinadas penalidades. Un sistema mal diseñado puede violar la *igualdad* si promueve o facilita una distribución inequitativa de recursos que debería ser equitativa. Un sistema mal diseñado se puede prestar más fácilmente a abusos por parte de las autoridades encargadas de aplicarlo. Como señalan Pato y Lynette, un sistema biométrico debe tomar en serio los temores de la población para ser efectivo.

Estas consideraciones están ausentes de los debates de políticas biométricas en la Argentina. Cuando en 2011 el poder ejecutivo creó SIBIOS por medio del decreto 1766/11, las complejidades propias de los sistemas biométricos no estuvieron presentes ni se discutió en el Congreso la conveniencia de

adoptar este tipo de políticas para la identificación de los ciudadanos. No se deliberó sobre los límites, mecanismos de control y garantías de seguridad de la base de datos ni se presentaron los detalles técnicos del sistema. Ello es consecuencia de que las tecnologías de identificación biométrica, en la Argentina, representan avances tecnológicos sobre políticas de larga data.

II. Una breve historia de la biometría en la Argentina

La Argentina, pionera

En la Argentina, las políticas de identificación de los ciudadanos con base en criterios biométricos tienen una larga historia.

El policía francés Alphonse Bertillón fue quien desarrolló la técnica de la *antropometría*, el primer sistema de identificación de criminales con base en las características físicas de éstos. Así, las políticas de registro de este tipo de datos tuvieron por objeto –en primer lugar– identificar a los ciudadanos que eran considerados "anormales" o "peligrosos" (Anitúa, 2005: 12). Con el advenimiento de la fotografía, muchos países comenzaron a identificar a personas catalogadas como delincuentes comunes, vagos o prostitutas(Anitúa, 2005: 14). Pero pronto se avanzó la idea de que lo más conveniente era contar con cédulas de identidad que identificasen a todos los ciudadanos (Anitúa, 2005: 15) y hacia fines del siglo XIX se avanzó con el método de identificación fotográfica universal.

En 1887, el entonces jefe de la policía Alberto Capdevila encargó a Agustín Drago un estudio sobre las técnicas de Bertillón, para lo cual fue enviado a París. A su regreso un año más tarde, Drago fue designado como director de la oficina de identificación antropométrica de Buenos Aires (Quesada, 1901: 97), que funcionaría como un brazo auxiliar del servicio de justicia.

En efecto, en el Congreso Internacional de Antropología Criminal celebrado en París en 1889, el encargado de leer la propuesta para la aceptación internacional del sistema antropométrico desarrollado por Alphonse Bertillon fue el delegado argentino, quien señaló que la policía de la Ciudad de Buenos Aires había adoptado este nuevo sistema dando "los mejores resultados" y pedía sumar esfuerzos "para extenderlo universalmente" (Magitot, 2010: 379). El propio Bertillon destacó que la Argentina fue el primer gobierno –después de Francia– en adoptar, por decreto, el uso oficial de las fichas antropométricas, por oposición a otras ciudades de los Estados unidos en las que su aplicación había sido producto de iniciativas privadas (Magitot, 2010: 380).

Además de ser pionera en la adopción de este tipo de técnicas, la Argentina

hizo un aporte fundamental cuando en 1897 el policía Juan Vucetich, desde su puesto de Jefe de la Oficina de Identificación de la policía de la Provincia de Buenos Aires, creó e implementó el primer sistema de clasificación y archivo de huellas dactilares Vucetich desarrolló herramientas para la toma de estas impresiones, aplicó el nuevo método a detenidos en distintas cárceles, creó las primeras Cédulas de Identidad y concibió tempranamente la posibilidad de la identificación general de la población (García Ferrari, 2009: 1).

El desarrollo de Vucetich representó un avance que –en cierto sentido– dejaba atrás ciertas dificultades asociadadas con la antropometría, que tendía a funcionar relativamente bien sólo en casos cuerpos masculinos cuyo desarrollo físico se encontraba concluido. Era prácticamente inútil para identificar a niños y adolescentes en edad de crecimiento y era demasiado invasivo –en esos tiempos– para ser considerada aceptable su aplicación a mujeres. Las huellas dactilares se presentaban, en este sentido, como inmutables, atemporales, únicas, asexuadas, sin distinción racial o social. Según Vucetich, era la forma en que había elegido la naturaleza para individualizar a las personas (García Ferrari, 2009: 2).

Anitúa explica cómo esta política de identificación fue evolucionando de una forma expansiva.

> "Vucetich logró en cinco años hacerse con más de un millón de fichas distintas de habitantes de la provincia de Buenos Aires gracias al fuerte apoyo de las autoridades argentinas, las primeras en adoptar este sistema primero para los delincuentes, luego para los inmigrantes, tras ellos los funcionarios públicos y los que realizaban el servicio militar y, finalmente, toda la población masculina" (Anitúa, 2005: 16).

Anitúa reseña el avance de los registros en la Argentina: en 1881 la Policía de la Capital Federal se creó el *Registro de Ladrones Conocidos*; en 1884 el *Registro de Vecindad*; en 1889 se adoptó el sistema Bertillon y en 1903 se asumió el *Sistema de Identificación Dactiloscópico* ideado por Vucetich. Eso dio lugar al *prontuario* en 1905 y a la *cédula de identidad* en 1906 (Anitúa, 2005: 16).

Los sistemas de registro avanzaron, no sin algunas objeciones que no fueron escuchadas (Anitúa, 2005: 17). Hacia 1933 se creó –por medio de una ley– el *Registro Nacional de Reincidencia y Estadística Criminal* que permitió –desde ese momento– a la policía requerir la presentación de documentos identificatorios a todos los ciudadanos, sin ningún motivo en particular (Anitúa, 2005: 18).

El documento identificatorio general llegó de la mano de la llamada *libreta de enrolamiento*, que se otorgaba a todos los hombres mayores de 18 años y

que permitía –además– el ejercicio del derecho al voto (Anitúa, 2005: 18). Argentina, de este modo, se transformó "en la pionera en exigir un documento obligatorio de identificación con finalidades disciplinarias" (Anitúa, 2005: 19). La expansión del voto femenino en 1949 generó la *libreta cívica* para la población femenina mayor de 18 años y en 1968 el "documento nacional de identidad" para la población en general[^11].

En efecto, la Decreto-Ley 17.671 estableció al Documento Nacional de Identidad (DNI) como política de Estado y fijó pautas claras respecto de la información que ese documento iba a recabar. El DNI era el vínculo entre el ciudadano y el Registro Nacional de las Personas (RNP) creado por la por la ley 13.482, que buscaba identificar "a todas las personas de existencia visible que se domicilien en territorio argentino o en jurisdicción argentina y a todos los argentinos sea cual fuere el lugar donde se domiciliaren"[^12]. Las funciones del RNP son las siguientes:

> a) La inscripción e identificación de las personas comprendidas en el artículo 1, mediante el registro de sus antecedentes de mayor importancia desde el nacimiento y a través de las distintas etapas de la vida, los que se mantendrán permanentemente actualizados; // b) La clasificación y procesamiento de la información relacionada con ese potencial humano, con vistas a satisfacer las siguientes exigencias: // 1) Proporcionar al Gobierno nacional las bases de información necesarias que le permita fijar, con intervención de los organismos técnicos especializados, la política demográfica que más convenga a los intereses de la Nación. // 2) Poner a disposición de los organismos del Estado y entes particulares que los soliciten, los elementos de juicio necesarios para realizar una adecuada administración del potencial humano; posibilitando su participación activa en los planes de defensa y de desarrollo de la Nación; // c) La expedición de documentos nacionales de identidad, con carácter exclusivo, así como todos aquellos otros informes, certificados o testimonios previstos por la presente ley, otorgados en base a la identificación dactiloscópica; // d) La realización, en coordinación con las autoridades pertinentes, de las actividades estadísticas tendientes a asegurar el censo permanente de las personas. // e) La aplicación de las multas previstas en los artículos 35, 37, 38 y 39 de esta ley. // f) La recepción y ulterior restitución a sus legítimos titulares, de documentos nacional de identidad extraviados, que hubieren sido encontrados por terceros.

El RNP crea un legajo personal con un número fijo, exclusivo e inmutable

y en él "se irá formando desde el nacimiento de aquéllas y en el mismo se acumularán todos los antecedentes personales de mayor importancia que configuran su actividad en las distintas etapas de su vida.[^13]" Para incorporar de manera paulatina a los ciudadanos al RNP, la ley estableció un sistema de actualización de información que se activaba cuando el ciudadano o ciudadana llegaba a edad escolar, oportunidad en la que se tomaba la fotografía y huella dactilar de la persona en cuestión[^14], a los 14 años y a los 30 años. El Poder Ejecutivo quedaba, de todas formas, habilitado a cambiar esos *momentos de actualización* cuando lo creyese conveniente. Actualmente, esas etapas están fijadas por el decreto 1501/2009 que –además– autorizó el uso de tecnologías digitales[^15].

Resulta significativo el avances de las tecnologías de identificación en la Argentina: se comenzó desde los supuestos "márgenes" de la sociedad mediante el registro de personas percibidas y designadas como malhechores o delincuentes pero el Estado avanzó, de modo invariable, hacia el registro total de la población. El hecho de que el sistema se haya unificado legalmente durante la dictadura de Juan Carlos Onganía no es de poca importancia: durante una de las dictaduras más autoritarias sufridas por la Argentina se establecieron las bases legales del sistema de identificación, registro y clasificación de la población que hoy está vigente y que se continúa perfeccionando de la mano de avances tecnológicos que hacen a estas políticas más eficientes pero a la vez más riesgosas para los derechos de los ciudadanos.

Los documentos de identidad en la Argentina, hoy

Documento Nacional de Identidad

En la Argentina el documento nacional de identidad (DNI) es el único instrumento de identificación personal y es obligatorio para todos los ciudadanos y residentes. El DNI no puede ser suplido por ningún otro documento a efectos legales; es obligatorio para ejercer el derecho al voto y para la identificación ante la autoridad judicial. El DNI argentino es requerido también para efectuar trámites ante las autoridades estatales y también habilita al portador para trabajar legalmente dentro del país.

El nuevo Documento Nacional de Identidad se comenzó a expedir en el año 2009 para todos los ciudadanos argentinos y para aquellos residentes extranjeros cuya situación migratoria los habilite en formato tarjeta plástica con distintos elementos de seguridad que permiten garantizar su legitimidad. Las innovaciones fueron introducidas por el Decreto1501/2009 y las Resoluciones del Registro Nacional de las Personas No. 585/2012 y No. 797/2012. El Nuevo DNI pasó a ser íntegramente confeccionado por el Estado Argentino he incorporó tecnologías informáticas en el proceso de su

producción: datos biográficos y huellas en bases de datos digitalizados y procesos de verificación dactiloscópica mediante herramientas informáticas.

En junio de 2014 un comunicado del Ministerio del Interior señaló que gracias a un acuerdo con la Casa Real de la Moneda de España, el DNI incorporaría tecnología que lo haría "inteligente" (ADC, 2014b). De acuerdo a información publicada por el diario La Nación, el documento tendría en el futuro dos chips, "uno con los datos identificatorios de la persona y en el otro cada persona podrá tener incorporados los datos de su historia clínica, de ANSES, de PAMI y de la tarjeta SUBE, lo que simplificará y mejorará los trámites, evitando papeles y múltiples identificaciones". La noticia –que mereció el reproche inmediato de la Fundación Vía Libre y la ADC– es significativa, ya que revela la lógica bajo la cual los avances tecnológicos son receptados por la administración sin que haya un análisis previo respecto del impacto que este tipo de medidas podrían tener sobre el derecho a la privacidad de los ciudadanos.

Pasaporte

El Ministerio del Interior y Transporte, a través del Registro Nacional de las Personas, trabajó durante el último tiempo en desarrollos que permitieron al Estado Argentino emitir un Nuevo Pasaporte Electrónico, el cual contiene un chip que almacena los datos biométricos de su titular para permitir su utilización en sistemas de reconocimiento automatizados. Estos chips son de la tecnología RFID, *Radio-Frequency Identification*. Estos chips pueden ser leídos a una distancia considerable, lo que permitiría la extracción de los datos allí contenidos –que, por ahora, son los que incluye el pasaporte– por parte de terceros no autorizados por el titular de los datos. Por ejemplo, en Holanda un programa televisivo demostró que era posible *hackear* los pasaportes desde más de diez metros de distancia, revelando la fecha de nacimiento, el rostro y la huella dactilar del titular de los datos (Lettice, 2006).

Cédula de Identidad

En Argentina la cédula de identidad fue un documento de identidad que estuvo a cargo de la Policía Federal hasta el 1 de marzo de 2011. A partir esa fecha la cédula dejó de emitirse. Esta disposición del Poder Ejecutivo Nacional y del Ministerio de Seguridad fue motivada por la superposición en la que se encontraba la cédula desde la creación del DNI *tarjeta*, que complementó en un primer momento –y luego reemplazó– al DNI *libreta* que to-

davía continúa vigente pero ha sido discontinuado. Junto con esta medida, en dicha disposición se previó que los Pasaportes pasarían a ser confeccionados por el Registro Nacional de las Personas, documento que hasta esa fecha también era emitido por la institución policial.

III. Los problemas de las políticas de registro e identificación de la población

Las políticas de identificación masiva de los ciudadanos son aceptadas por todos los argentinos, quienes –de acuerdo a la historia reseñada en la sección anterior– no recuerdan haber vivido *sin* alguna variante del documento nacional de identidad. Pero ello no es así en todos los países, cuyas poblaciones muestran diversos grados de aceptación o rechazo de este tipo de políticas.

Un buen ejemplo de ello es lo que ocurrió en el Reino Unido en los últimos diez años, a partir de que en 2005 el gobierno del Partido Laborista avanzara con la idea de establecer un sistema de identificación universal capaz de recolectar los datos biométricos de los ciudadanos. Esa propuesta fue recibida con críticas por parte de grupos de activistas quienes, sin embargo, no lograron impedir que en 2006 el Parlamento sancione la *Identity Cards Act*. Esta norma creaba un documento de identidad que permitía viajar dentro de la Unión Europea y recogía información que sería volcada al *National Identity Registry* (BBC, 2005). De acuerdo a la ley, se registrarían cincuenta categorías de información sobre los ciudadanos de manera centralizada y la base de datos se actualizaría cada vez que se utilizase la tarjeta de identificación[1]

Alarmados por los alcances de la política de registro, organizaciones del reino unido como Privacy International, Liberty80 y NO2ID emprendieron un esfuerzo doble: por un lado, reunir a quienes se oponían fervientemente al registro de los ciudadanos; por el otro, educar a los millones que se mantenían más o menos indiferentes respecto de la cuestión.[2]

El argumento en contra del sistema único de identificación fue múltiple y sostenía –por ejemplo– lo siguiente:

- **No es efectivo**. No hay ningún tipo de evidencia que establezca que el establecimiento de estos sistemas reduce el delito. Tampoco permite evitar fraudes en el acceso a beneficios: las estadísticas del Reino Unido muestran que el 95 por ciento de los fraudes es por falsificación de las circunstancias que habilitan a acceder al beneficio, no por

[1] *Ver* EFF (s. f.).
[2] *Ver* EFF (s. f.).

falsificación de identidad.

- **Es injusto**. Las cédulas de identidad se vuelven un foco más de control que podría agravar prácticas de vigilancia y hostigamiento sobre minorías, grupos étnicos, inmigrantes, etcétera.
- **Es costoso**. Según una estimación del gobierno británico, la implementación del sistema de registro de los ciudadanos tendría un costo de 5 mil millones de libras.
- **Es excesivo**. El registro contendría mucha información sobre las personas, incluyendo –por ejemplo– información sobre su estatus inmigratorio o las direcciones físicas en las que esa persona tiene y tuvo su domicilio. Esta información sería compartida entre agencias gubernamentales y contratistas. Las falencias del Estado en cuidar la información sobre los ciudadanos vuelve a estos registros aún más problemáticos, ya que el riesgo de filtraciones no sólo es posible sino que es probable. En efecto, en 2007 se comprometieron más 25 millones de registros de ciudadanos británicos.[3]

Esa campaña de movilización ciudadana fue efectiva: el mensaje de los activistas por el derecho a la privacidad llegó a los medios de comunicación y –eventualmente– logró impactar en el sistema político. En efecto, en mayo de 2010 la coalición entre el Partido Conservador y el Partido Liberal acordaron derogar la *Identity Cards Act* de 2006. Cuando finalmente accedieron al gobierno, promovieron la sanción del *Identity Documents Act* de 2010, que dispuso:

- Derogar la ley que exigía el registro de los ciudadanos.
- Cancelar las tarjetas de identidad que ya habían sido emitidas.
- Eliminar el *National Identity Register*.
- Destruir la información contenida en el *National Identity Register*.
- Cerrar la oficina del Comisionado de Identidad.

Para enmarcar el debate, fue esencial la campaña que se construyó en torno al concepto de "estado de base de datos" (Herbert, 2010). En efecto, el activista se encargó de denunciar cómo la recopilación de datos por parte del estado era una herramienta de vigilancia masiva que podía utilizarse como mecanismo de control de la sociedad. Este tipo de mensajes hicieron que el apoyo de las tarjetas de identificación decreciera considerablemente[4].

El repaso del proceso de las tarjetas de identificación en el Reino Unido tiene sentido para contrastarlo con lo que ocurre en la Argentina, que –en cierto

[3] *Ver* NO2ID (s. f.).
[4] *Ver* Report (s. f.).

sentido– implica una dinámica opuesta. En efecto, mientras que en el Reino Unido se avanzó en un sentido que la ciudadanía rechazó, en la Argentina se avanza en políticas de identificación de los ciudadanos sin que éstos conozcan los detalles de los sistemas o puedan participar del debate público imprescindible detrás de políticas públicas de este estilo. Y ello ocurre gracias a una diferencia significativa con el Reino Unido: en la Argentina no se trata de cambios legislativos sino de actualizaciones tecnológicas. Todas las modificaciones en nuestros documentos de identidad que experimentamos en los últimos son cambios construidos sobre un decreto-ley de la dictadura de Juan Carlos Onganía, autorizados por decretos presidenciales u oscuras resoluciones de direcciones administrativas. Estos cambios no pasan por el proceso de discusión política porque son implementados como modificaciones técnicas que no requieren nuevas autorizaciones legales por parte del Congreso. Esto es un problema serio que impide que estos cambios sean tamizados por una discusión política y echa un manto de sospecha sobre la constitucionalidad de las medidas adoptadas por el Estado.

Asimismo, no existe ciudadano argentino vivo que recuerde un tiempo sin algún tipo de sistema de identificación. Desde que nacemos, la única realidad que conocemos es la del DNI: no nos imaginamos cómo podríamos viajar, comprar pasajes en colectivo o incluso ingresar a oficinas públicas sin presentar el documento oficial que nos identifica pero –como corolario necesario– también nos registra y clasifica. Esto no es así en todos los países: Lyon destaca al caso argentino como una anomalía junto a países como Francia, Sudáfrica o Taiwan, entre muchos otros (Lyon, 2009: 3). Mientras en algunos países los sistemas de identificación están naturalizados, en otros no. Y suele ser en estos últimos donde las propuestas de identificación universal encuentran resistencia[5]

Para empezar a comprender lo problemático de los cambios tecnológicos es necesario reflexionar sobre los problemas específicos que estas clases de políticas presentan para los ciudadanos prestando especial atención al contexto social, político y legal de la Argentina que es uno en el que la práctica de registro está naturalizado.

Las políticas de registro y clasificación y el vínculo con la vigilancia

Uno de los argumentos usuales en contra de este tipo de políticas es que el registro masivo de la población implica, ante todo, un intento por clasificar y controlar a la población como si cada uno de los ciudadanos fueran *medios*

[5]Además de Inglaterra, hay muchos otros países donde este tipo de políticas generaron campañas ciudadanas que las cuestionaron. Sobre el caso de Australia, y a modo de ejemplo, ver el trabajo de Davies (2004: 224).

a manipular para la consecución de determinados *fines*. Este argumento parece ser persuasivo en sociedades que han padecido regímenes dictatoriales que recurrieron a mecanismos de clasificación para controlar a la población y emprender distintas medidas represivas. Por ejemplo, en Alemania Oriental el Ministerio de Seguridad (STASI) llevaba un cuidadoso registro de los ciudadanos objeto de vigilancia, donde se consignaban numerosos datos sobre su vida privada (Knabe, 2014). O piensese, por ejemplo, en el caso del *Diario Militar* en Guatemala, como se conoce a un documento militar de Guatemala donde se registraba y clasificaba a detenidos políticos y que servía para crear conexiones entre personas detenidas y a detener [ˆ131](*Ver* Mack (s. f.)). Estos ejemplos extremos muestran de qué manera las políticas de clasificación pueden utilizarse con fines represivos en regímenes dictatoriales.

Pero los problemas no se limitan a las dictaduras. En efecto, uno de los principales argumentos en contra de este tipo de políticas se vincula con que éstas son parte de *dispositivos* de control y vigilancia, es decir, son prácticas administrativas sobre las cuales se asientan mecanismos que sirven para controlar a la población. Es un punto que Lyon explica de la siguiente manera:

> "La vigilancia ocurre cuando las organizaciones prestan atención, de manera rutinaria y sistemática, a los datos personales [de los ciudadanos]. En el caso de los documentos nacionales de identificación, las organizaciones en cuestión son departamentos gubernamentales, que tiene variados propósitos: aumentar la eficiencia administrativa, asegurarse que los beneficios y servicios alcancen a las personas que tienen que alcanzar, facilitar el cumplimiento de la ley y la seguridad nacional, etcétera. Mientras que los sistemas de registro de los ciudadanos siempre han tenido una dimensión de vigilancia, las capacidades de vigilancia de los neuvos sistemas digitales representan un salto cualitativo comparado con los viejos sistemas de archivos físicos" (Lyon, 2009: 5-6).

Muchas veces, esta lógica de *disciplinamiento* y *vigilancia* se descubre sólo a través de un análisis genealógico de las prácticas que constituyen los dispositivos disciplinarios. En cierto sentido, el análisis histórico de las políticas de registro y clasificación reseñado previamente tiene ese objetivo: poner de presente que estas políticas que empezaron en los supuestos márgenes de la sociedad fueron extendiéndose hasta someter a todo el cuerpo social a los mecanismos de control. Pero en la Argentina este análisis es más transparente gracias al hecho de que la "ley" sobre la cual se sostiene el sistema de registro de la población tuvo su orígen en la dictadura de Juan Carlos Onganía y los fines problemáticos de la norma son explícitos.

En efecto, el decreto-ley 17.671 de 1968 tiene por objeto la "identificacion, registro y clasificacion del potencial humano nacional". El objetivo de *control* y *manipulación* en este caso es claro: su artículo 2 señala que el objetivo de la recolección y actualización permanente del registro de la ciudadanía es fijar la política demográfica de acuerdo a "los intereses de la Nación" y "administrar el potencial humano nacional", definición vaga y ambigua que sin embargo considera a cada ciudadano como una *herramienta* a ser manipulada en función de intereses superiores.

El decreto-ley es poco democrático por su contenido pero también, lógicamente, por su origen. Dictado bajo las atribuciones usurpadas por el llamado *Estatuto de la Revolución Argentina*, la legislación sobre la cual se basa nuestro sistema de documento nacional de identidad arrastra las marcas de una dictadura autoritaria, loq eu arroja sobre el sistema un manto de sospecha que nunca ha sido cuestionado ni política ni judicialmente. Sobre la base de esta estructura legal se construyeron avances tecnológicos que resaltamos antes y que recién ahora empiezan a mirarse con sospecha por parte de actores políticos (UCR, 2014) y sectores de la sociedad civil preocupados por el derecho a la privacidad (ADC, 2014c).

Los riesgos para los derechos: igualdad y discriminación

Las políticas de registro y clasificación de los ciudadanos son mecanismos efectivos para la implementación de políticas de control y manipultación, pero también para políticas de represión. Los ejemplos mencionados de Alemania y Guatemala son sólo eso, ejemplos de casos históricos en donde este tipo de tecnologías de control fueron implementadas para perseguir, detener y asesinar a disidentes políticos. Por supuesto, los riesgos que esta clase de tecnologías presentan bajo una dictadura no están presentes en una democracia que cuenta con garantías de distinto tipo para impedir esa clase de abusos y directamente excluye a las políticas de represión masiva de su catálogo de acciones posibles.

No es necesario, sin embargo, pensar que es el derecho a la vida y a la libertad los únicos que este tipo de políticas de registro masivo ponen en riesgo. Ni es razonable tampoco reducir esos riesgos a los gobiernos autoritarios. En efecto, uno de los principales derechos que se ponen en riesgo con el registro centralizado de información personal de los ciudadanos es el derecho a la *igualdad*, especialmente a recibir un trato equitativo y justo.

La información sobre los ciudadanos puede utilizarse para trazar comparaciones, realizar distinciones de acuerdo a diversos criterios y para clasificar a los ciudadanos en distintos grupos. Si bien el Estado puede comprometerse en no llevar adelante ese tipo de políticas, no existe ningún tipo de prohibición legal específica que impida el desarrollo de políticas pro-

blemáticas como –por ejemplo– la clasificación de personas de acuerdo a niveles económicos, o de acuerdo al lugar en donde viven, nivel educativo, etcétera. La única prohibición explícita se encuentra en el artículo 7.3 de la ley 25.326 de Protección de Datos Personales, que establece que "[q]ueda prohibida la formación de archivos, bancos o registros que almacenen información que directa o indirectamente revele datos sensibles", es decir, datos "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" (artículo 2). Esta limitación es valiosa pero abre un amplio abanico para realizar clasificaciones de diferente tipo, como las mencionadas a modo de ejemplo anteriormente.

Una interpretación razonable de la Constitución prohibiría muchas de esas clasificaciones en la medida en que éstas puedan utilizarse con fines *discriminatorios*, ya sea por el Estado o por terceros con acceso a los registros correspondientes. Pero no existe una ley específica que lo prohíba ni una autoridad estatal en el ámbito del ejecutivo capaz de impedir que estas clasificaciones ocurran. Si el riesgo en un estado democrático es bajo por la existencia de garantías constitucionales que resguardan la igualdad ante la ley, la mera existencia de la información que permite el registro y la clasificación representa un riesgo, ya que podría ser utilizada por actores no estatales con fines que irían en contra del principio de igualdad de trato. Algunos ejemplos puede clarificar este punto.

- Una empresa de seguros de automotor con acceso a información sobre (a) ingresos medios diferenciados por zonas geográficas y (b) domicilios de las personas podría cruzar esa información para cobrar primas más elevadas en seguros sobre la propiedad a las personas que habitan zonas de ingresos bajos por considerar con base en (c) información estadística de delitos que el riesgo contra la propiedad es mayor en esos barrios.

- Ante (a) fallas en el servicio de telefonía fija en un barrio de una Ciudad, una empresa de telefonía celular con (b) información procesada sobre la identidad de las personas que allí habitan podría adoptar medidas de marketing directo para vender líneas o adoptar prácticas abusivas por el hecho de conocer las necesidades de esos ciudadanos.

- Lo mismo podría ocurrir con la aceptación o rechazo de personas en obras sociales como consecuencia del lugar donde viven si ese lugar presenta condiciones ambientales que generan de manera usual determinados problemas de salud.

Estos ejemplos no son extremos: podríamos pensar en políticas más problemáticas y claramente ilegales. En estos casos, vinculados a la actividad

aseguradora y a políticas de determinación de precios no son necesariamente contrarios a la ley y hasta podría pensarse que son prácticas comerciales razonables, especialmente la vinculada a cálculos actuariales que precisan de información para ser más precisos. El punto que queremos destacar con estos ejemplos que este tipo de prácticas implican un trato *desigual* hacia los ciudadanos: se registran datos sobre nosotros, somos *clasificados* de acuerdo al cruce de esos datos con otros que muchas veces están públicamente disponibles o son fáciles de recolectar y –como corolario necesario de las primeras dos prácticas– somos *tratados* como miembros de una determinada *clase*. Ello viola nuestro derecho a ser tratados como iguales y como individuos que gozan de autonomía y libertad.

Los ejemplos mencionados previamente, además, son inocentes: podríamos pensar que una consecuencia posible del registro y clasificación de la población sean políticas discriminatorias explícitas como el *apartheid* sudafricano. Pero no es necesario llegar a esos extremos para señalar los riesgos que el registro de información personal de los ciudadanos representa para sus derechos. Si bien la ley 25.526 establece algunos resguardos, ellos –como veremos en el siguiente apartado– no son suficientes.

Estos riesgos se ven incrementados por los cambios tecnológicos, que tienden a reemplazar la identificación tradicional a la que estamos acostumbrados, es decir, la que se produce *cara* a *cara*, se limita a la verificación de la veracidad del documento y funciona en instancias individualizadas. Como señala Lyon, los nuevos sistemas de identificación tienden a funcionar de manera remota, es decir, permiten el control de la información contenida en los documentos a distancia –por ejemplo, cuando un pasaporte es leído en un punto fronterizo que se comunica con una base de datos centralizada (Lyon, 2009: 143). Además, los sistemas de identificación son interoperables lo que significa que empiezan a ser objeto de estándares tecnológicos que los vuelven utilizables en otros países (Lyon, 2009: 144). Estas características se suman a otras que las tecnologías vuelven más efectivas: la posibilidad de establecer categorías de ciudadanos, de limitar la ciudadanía de las personas al ejercicio de funciones *útiles* como –por ejemplo– permisos de trabajo limitados que impiden el acceso a ciertos beneficios, etcétera. Además, este tipo de sistemas siempre tiene la posibilidad de excluir a determinadas personas del goce de derechos vinculados a la ciudadanía o –en los casos en los que la Constitución es generosa con los extranjeros, como en el caso argentino– a la situación de habitante de determinado país.

En la Argentina existen razones para pensar que nuestros años de gobiernos dictatoriales y autoritarios han quedado definitivamente en el pasado. Sin embargo, cabe plantearse la siguiente pregunta hipotética: ¿qué hubiera pasado durante la última dictadura militar si ella hubiera contado con las tecnologías disponibles actualmente y el grado de información que el Estado tiene sobre los ciudadanos? Es difícil imaginar hechos más mons-

truosos que los acontecidos en la Argentina entre 1976 y 1983. Sin embargo, sí es posible señalar que las políticas represivas instauradas durante esos años hubieran sido implementadas de un modo más efectivo. Ello obliga, creemos desde la ADC, a plantearnos una segunda pregunta: ¿qué hace la democracia argentina para resguardar los derechos de los ciudadanos ante una improbable regresión autoritaria? El análisis de nuestro marco normativo y las prácticas de los organismos estatales a cargo de defender nuestra privacidad deja a esa pregunta con una respuesta muy poco satisfactoria.

Falta de garantías y potenciales abusos

Como reveló un estudio realizado por la ADC en septiembre de 2014, la información que recolecta el Estado no se encuentra adecuadamente protegida (ADC, 2014a). En efecto, en el estudio *El Estado Recolector* la ADC mostró cómo el Estado está legalmente autorizado a recolectar una enorme cantidad de información de sus ciudadanos, que la agencia estatal encargada de la protección de esos datos no cuenta con recursos humanos o materiales suficientes para realizar tareas de control y que el poco control que adelante se enfoca exclusivamente en actores privados (ADC, 2014a). Además, tampoco cuenta con medidas uniformes de seguridad de los datos y ha experimentado en el pasado *filtraciones* que fueron graves y que pusieron en riesgo los datos de los ciudadanos (ADC, 2014a: 18).

Si –como argumenta el Estado– el registro de datos personales es una medida *necesaria* que busca satisfacer fines *imperativos* del Estado, lo mínimo que el Estado podría hacer es garantizar la seguridad de los datos y asegurarnos de que los mismos no llegarán a manos de actores privados que podrían utilizarlos de los modos que hemos señalado. Pero el Estado argentino, hoy en día, no puede ofrecer esa garantía (ADC, 2014a).

Este argumento es claramente subsidiario: las políticas de registro masivo de los ciudadanos presentan riesgos *en sí mismas* y por más garantías que se establezcan es posible cuestionar determinados alcances de las mismas. Sin embargo, la situación de falta de garantías de los datos en la Argentina hace que la expansión de estas políticas sean aún más problemáticas como veremos a continuación mediante un análisis del sistema SIBIOS creado por decreto presidencial en 2011.

IV. SIBIOS y la sociedad de control

El Sistema Federal de Identificación Biométrica (SIBIOS) es un nuevo servicio de identificación biométrica centralizado, con cobertura nacional, que permitirá a las agencias de seguridad hacer "referencias cruzadas" de in-

formación con datos biométricos y otros datos inicialmente recogidos por el Registro Nacional de de las Personas (RENAPER). Fue creado en 2011 por medio del decreto 1766, el cual se basa en una lógica de seguridad y prevención del delito. En efecto, como explica el artículo 1 del decreto, SIBIOS fue concebido para "prestar un servicio centralizado de información respecto de los registros patronímicos y biológicos individuales, a los fines de contribuir a la comprobación idónea y oportuna en materia de identificación de personas y rastros, en procura de optimizar la investigación científica de delitos y el apoyo a la función preventiva de seguridad".

La principal fuente de información de SIBIOS es la base de datos del RENAPER, tal como establece el artículo 2 del decreto 1176/2011. Esto significa que SIBIOS opera un cambio significativo en el Registro Nacional de las Personas y en los fines del Documento Nacional de Identidad, que ahora pasan a ser un elemento fundamental de la política criminal del Estado argentino. Antes, la relación entre las fuerzas de seguridad y el Registro Nacional de las Personas era *indirecta*: si la Policía Federal quería acceder a información del RENAPER debía solicitar ese acceso. Ahora la base de datos de RENAPER va a alimentar a la base de datos de SIBIOS a la cual tendrán acceso como usuarios todas las fuerzas de seguridad federales (policía, gendarmería, prefectura y policía aeroportuaria) así como la Dirección Nacional de Migraciones (DNM) y el RENAPER. Además, el artículo 3 del decreto 1176/2011 "invita" a que las Provincias se adhieran, lo que implica que cada una de las fuerzas de seguridad provinciales también podrán acceder a una única base de datos para poder realizar "consultas biométricas en tiempo real" (artículo 4, decreto 1176/2011).

SIBIOS representa, entonces, la consolidación de bases de datos que estaban dispersas y la ampliación del acceso a las fuerzas de seguridad del Estado. A septiembre de 2014, SIBIOS contaba con 13.200.000 registros de huellas dactilares.[6] A medida que los pasaportes y los DNI vayan caducando, el RENAPER recogerá información que alimentará de manera directa a la base de datos de SIBIOS. Eso significa que en pocos años todos los ciudadanos argentinos y residentes estarán en una base de datos que podrá establecer controles del tipo *one-to-many* cuando así sea requerido el sistema, ya sea para el control de las huellas dactilares o el rostro de los ciudadanos. En efecto, así explica el Ministerio de Seguridad la forma en que el control de huellas dactilares es realizado:

> "La clasificación de los registros [de huellas dactilares] se realiza según las características de las minucias dactilares, a las cuales se le aplica un algoritmo y el resultado arrojado se utiliza como medida de comparación, arrojando de esta forma los porcentajes

[6]Respuesta del Ministerio de Seguridad del 16 de septiembre de 2014, en archivo en la ADC.

de los candidatos cotejados"[7].

Según el experto en políticas de biometría Eduardo Thill, el decreto de 2011 no fue la presentación en público de SIBIOS sino la orden de crearlo[8]. A su criterio, SIBIOS no se encuentra plenamente implementado y ello es consecuencia de que aún falta incorporar al sistema las bases de datos de muchas fuerzas de seguridad provinciales que no se han adherido al sistema. De acuerdo a información provista por el Ministerio de Seguridad a un pedido de acceso a la información realizado por la ADC[9], a septiembre de 2014 sólo once provincias se habían adherido al sistema: Chaco, Mendoza, San Juan, Tucumán, Catamarca, Santiago del Estero, Santa Fe, Santa Cruz, Entre Ríos, Salta y La Rioja.

En parte, la falta de implementación total de SIBIOS se vincula con la estructura federal del Estado: para que las policías provinciales puedan sumarse al sistema se necesita la decisión política del gobernador o gobernadora de turno, lo que ha generado que muchas provincias estén fuera del sistema por razones políticas[10].

En términos de acceso, el Ministerio de Seguridad informó que el acceso remoto de los usuarios (fuerzas de seguridad federales y de provincias adheridas) se limita al sistema AFIS de identificación de huellas dactilares y al sistema patronímico, que las vincula con los nombres de las personas[11]. Según el Ministerio, "todos los usuarios con acceso al sistema son personas de existencia física permitiendo ser identificables perfectamente"[12]. Thill señaló que el acceso remoto implica sólo una consulta, no existen posibilidades de modificar el registro dando de alta nuevos registros, dando de baja otros o modificándolos[13].

En cuanto a medidas de seguridad, el Ministerio se limitó a señalar que ellas son las que derivan del estándar de seguridad de información ISO/IEC 27.001 y del *Modelo de Políticas de Seguridad de la Información* desarrollado por la Oficina Nacional de Tecnologías de la Información (ONTI)[14]. La efectividad de las medidas de seguridad no dependen sin embargo de la adopción

[7]Respuesta del Ministerio de Seguridad del 16 de septiembre de 2014, en archivo en la ADC.

[8]Entrevista con Eduardo Thill realizada en Buenos Aires el 20 de mayo de 2014.

[9]Respuesta del Ministerio de Seguridad del 16 de septiembre de 2014, en archivo en la ADC.

[10]Entrevista con Eduardo Thill realizada en Buenos Aires el 20 de mayo de 2014.

[11]Respuesta del Ministerio de Seguridad del 16 de septiembre de 2014, en archivo en la ADC.

[12]Respuesta del Ministerio de Seguridad del 16 de septiembre de 2014, en archivo en la ADC.

[13]Entrevista con Eduardo Thill realizada en Buenos Aires el 20 de mayo de 2014.

[14]El *Modelo de Política de Seguridad de la Información* puede consultarse en http://www.sgp.gov.ar/sitio/PSI_Modelo-v1_200507.pdf.

de estándares adecuados: se requiere que ellos sean debidamente implementados y que exista una autoridad de control encargada de verificar que los estándares vigentes se cumplan. No resulta claro si estas autoridades existen: el *Modelo de Políticas de Seguridad de la Información* crea un Comité de Seguridad de la Información en el ámbito de "cada organismo", lo que sugiere que no hay una autoridad centralizada de control (ADC, 2014a). Para Thill el punto sobre el *control* es clave: para que el sistema se aceptado por la ciudadanía se requiere establecer "un círculo de controles recíprocos"[15].

Uno de los principales motivos de alarma del sistema estuvo vinculado con el vídeo que Presidencia de la Nación creó para presentar SIBIOS ante la sociedad[16], cuyo *slogan* de presentación fue utilizado como título de este trabajo. La lógica del vídeo era preocupante: asegurara a los ciudadanos que *si nos conocemos más, nos cuidamos mejor*, postulando una política de control y vigilancia masiva que se sostenía sobre tecnología desarrollada junto a Cuba y que incluiría la información sobre el iris de las personas, su ADN y hasta su forma de caminar. El sistema se vincularía a las cámaras de vigilancia –en expansión en las grandes ciudades– y permitiría la comparación de los rostros de las personas con la base de datos de SIBIOS. Para Thill, el vídeo fue realizado con una lógica publicitaria que no se condice con la realidad[17].

Por ejemplo, si bien existe la posibilidad de incluir más datos sobre el iris de las personas, la forma de caminar o el ADN en la base de datos, no hay planes de que ello ocurra. Pero a medida que avanzan los desarrollos tecnológicos, estas posibilidades se vuelven mucho más factibles y de acuerdo al avance de las políticas de identificación biométrica en la Argentina no hay razones para pensar que no podrían ser implementadas como otro caso de actualizaciones tecnológicas sobre políticas públicas asentadas y no cuestionadas. Según el decreto 1766/2011, la información de SIBIOS se va a limitar a las huellas dactilares y al rostro de las personas pero el Ministerio de Seguridad reconoce que además procesa la voz de los ciudadanos y su firma. Si bien la firma se obtiene de los registros del RENAPER, es una incógnita de donde el Estado obtiene los registros de voces de los ciudadanos. Un pedido de acceso a la información adicional sobre este punto no había sido respondido a la fecha de cierre de este informe.

V. Conclusión

Los avances de las políticas de identificación biométrica representan una problemática que debe enmarcarse en la tensión entre *seguridad* y *libertad* que afecta a las sociedades occidentales desde comienzos de siglo, especial-

[15] Entrevista con Eduardo Thill realizada en Buenos Aires el 20 de mayo de 2014.
[16] El video puede encontrarse en http://vimeo.com/77142306
[17] Entrevista con Eduardo Thill realizada en Buenos Aires el 20 de mayo de 2014.

mente luego de los atentados en Estados Unidos de septiembre de 2001. Los avances tecnológicos permiten una mayor expansión y efectividad de las tecnologías de control, tal como surge de las revelaciones del ex contratista de la NSA Edward Snowden. Las políticas de identificación biométrica deben insertarse necesariamente en ese contexto ya que cumplen una función estrechamente vinculada con la seguridad, tal como el decreto de creación de SIBIOS reconoce expresamente.

En la Argentina, estas políticas se construyen sobre marcos legales poco democráticos, tanto por su orígen como por su contenido. La ley 17.611 que crea el Registro Nacional de las Persona considera a cada ciudadano como un dato a ser *clasificado* de un modo que permite aprovechar el *potencial humano* que representa la población. Cada ciudadano es un *medio* que puede ser utilizado como un *fin* y ello –por sí solo– debería levantar sospechas sobre la constitucionalidad del sistema. Pero además del problemático origen del sistema de registro, lo cierto es que la población argentina está sumamente acostumbrada al mismo: desde que nacemos tenemos nuestro DNI y éste nos sirve para ejercer derechos y acceder a beneficios de distinto tipo. El documento se vincula de manera estrecha al ejercicio de la ciudadanía y así cumple la doble función de facilitar el ejercicio de las prerrogativas que ese estatus significa y de construir un medio para registrar y clasificar a la población. La aceptación del DNI ésta seguramente vinculada al primer punto, mientras que las consecuencias problemáticas del registro no son percibidas como serias o graves.

Los cambios tecnológicos, sin embargo, deberían hacernos revisar esa segunda conclusión. Como se señaló anteriormente, las políticas de identificación biométrica tienen una larga data pero los cambios tecnológicos las han vuelto más efectivas lo que implica que los riesgos que ellas crean son mayores. Además de los riesgos improbables de un retorno a un sistema autoritario, la posibilidad de que la información se utilice con fines discriminatorios depende de riesgos mucho más factibles, como las filtraciones de datos, el robo por parte de personas con acceso, etcétera. Ello permitiría que la información recolectada por el Estado sea utilizado por terceros que crearían, *da facto*, distintas categorías de ciudadanos. Algunos podrían acceder a servicios en mejores condiciones que otros, otros no podrían acceder, etcétera. El registro de la información es condición necesaria para que ello ocurra y por eso representa un riesgo a evaluar desde una perspectiva de derechos humanos.

Desde esa mirada las políticas deben pensarse en función de su *razonabilidad* y *proporcionalidad*. Como lo ha señalado la Corte Suprema de Justicia de la Nación y los estándares internacionales de derechos humanos, las políticas públicas que afectan derechos humanos sólo se justifican si son establecidas por ley, buscan satisfacer un interés legítimo del Estado y son necesarias y proporcionales de acuerdo a los fines que buscan satisfacer, de acuerdo a los

medios que utilizan para su satisfacción y de acuerdo al grado de afectación de los derechos en juego. Los avances tecnológicos en las políticas de registro de la población modifican necesariamente ese análisis ya que los riesgos son mayores y, en consecuencia, también es mayor el grado de afectación de ese derecho.

La ADC ha impulsado un amparo colectivo a propósito de la filtración de las fotos del padrón electoral producida en octubre de 2013, cuando la Cámara Nacional Electoral subió a Internet las fotos de miles de ciudadanos sin su consentimiento.[18] En ese caso se discute los riesgos creados para los derechos de los ciudadanos, el manejo descuidado de nuestra información personal y la falta de garantías adecuadas para ese uso. Además, se discute la *razonabilidad* y *proporcionalidad* de la inclusión de las fotos del DNI en el padrón electoral. Ese caso, que aún no tiene sentencia definitiva, representa una excelente oportunidad para que el poder judicial en su función de garante de derechos pueda evaluar políticas que han pasado desapercibidas para el sistema político. Junto al interés que la cuestión ha deparado en el Congreso (UCR, 2014) es posible que políticas que nunca han sido cuestionadas empiecen a ser analizadas desde una mirada preocupada por la plena vigencia de los derechos humanos.

Para un país que ha normalizado una práctica problemática, ello sería un gran primer paso en la dirección correcta.

[18]Un análisis detallado de este caso puede encontrarse en ADC (ADC, 2014a: 18).

Referencias

Lettice, John. (2006, enero). Face and fingerprints swiped in dutch biometric passport crack the register. *The Register*. Archive. Recuperado de: http://web.archive.org/web/20060131005717/http://www.theregister.co.uk/2006/01/30/dutch_biometric_passport_crack/

ADC. (2014a). *El estado recolector. un estudio sobre la argentina y los datos personales de los ciudadanos* (Policy Paper). Buenos Aires: Asociación por los Derechos Civiles.

ADC. (2014b, junio). DNI: no se trata sólo de avances tecnológicos. Asociación por los Derechos Civiles. Recuperado de: http://www.adc.org.ar/nuevos-dni-no-se-trata-solo-de-avances-tecnologicos/

ADC. (2014c, septiembre). Discusión sobre privacidad y vigilancia en la argentina. Asociación por los Derechos Civiles. Recuperado de: http://www.adc.org.ar/discusion-sobre-privacidad-y-vigilancia-en-la-argentina/

Anitúa, Gabriel Ignacio. (2005). Identifíquese! apuntes para una historia del control de las poblaciones. En David Baigún (ed.), *Estudios sobre justicia penal: Homenaje al profesor julio B.J. maier*. Ediciones del Puerto.

BBC. (2005). Government unveils ID card scheme. *BBC*. Recuperado de: http://news.bbc.co.uk/2/hi/uk_news/politics/4554827.stm

Davies, Simon. (2004). The australia card: Campaign of opposition. En Wendy McElroy & Carl Watner (eds.), *National identification systems: Essays in opposition* (1ST edition.). Jefferson, N.C: McFarland & Company.

EFF. (s. f.). Success story: Dismantling UKs biometric ID database. *Electronic Frontier Foundation*. https://www.eff.org/pages/success-story-dismantling-uk%E2%80%99s-biometric-id-database. Recuperado de: https://www.eff.org/pages/success-story-dismantling-uk%E2%80%99s-biometric-id-database

García Ferrari, Mercedes. (2009). El bertillon americano. una aproximación a la trayectoria intelectual de juan vucetich. IDES.

Herbert, Guy. (2010, mayo). Cameron will scale back database state. *The Guardian*. http://www.theguardian.com/commentisfree/2010/may/13/id-cards-database-cameron-clegg. Recuperado de: http://www.theguardian.com/commentisfree/2010/may/13/id-cards-database-cameron-clegg

Knabe, Hubertus. (2014, agosto). Transcript of "The dark secrets of a surveillance state". *TED*. Recuperado de: http://www.ted.com/talks/hubertus_knabe_the_dark_secrets_of_a_surveillance_state/transcript

Lyon, David. (2009). *Identifying citizens: ID cards as surveillance* (1 edition.). Cambridge, UK ; Malden, MA: Polity.

Mack, Fundación Myrna. (s. f.). Caso diario militar. Fundación Myrna Mack. Recuperado de: http://www.myrnamack.org.gt/index.php/caso-diario-militar

Magitot, E. (2010). *Actes du deuxieme congres international: D'Anthropologie criminelle biologie et sociologie*. Kessinger Publishing, LLC.

NO2ID. (s. f.). The problems with ÏD cards". NO2ID. Recuperado de: http://www.no2id.net/IDSchemes/whyNot

Pato, Joseph N., y Millet, Lynette I. (Eds.). (2010). *Biometric recognition: Challenges and opportunities*. National Academies Press.

Quesada, Ernesto. (1901). *Comprobación de la reincidencia: Proyecto de ley presentado al señor ministro de justicia é instrucción pública doctor don osvaldo magnasco*. Coni hermanos.

Report, UK Polling. (s. f.). ID cards update. Recuperado de: http://ukpollingreport.co.uk/blog/archives/category/id-cards

UCR. (2014, agosto). Jornada en el congreso sobre el nuevo DNI. Unión Cívica Radical.

Índice

ADC / Asociación por los Derechos Civiles

este trabajo fue realizado con el apoyo de

PRIVACY INTERNATIONAL