Siri, Laura (mayo, 2015). El Documento Nacional de Identidad Argentino: una "caja negra" y una política de veridicción. *III Simposio Internacional LAVITS Vigilancia, Tecnopolíticas y Territorios 13-15 Mayo 2015.* Río de Janeiro, Brasil. Red de Estudios Latinoamericanos sobre Vigilancia, Tecnología y Sociedad (LAVITS).

El Documento Nacional de Identidad Argentino: una "caja negra" y una política de veridicción

LAURA SIRI[1]

Resumen

En la Argentina todo ciudadano debe poseer un Documento Nacional de Identidad (DNI). Éste incluye datos biométricos y, si tiene el formato más reciente, también un chip. No es obligatorio por ley portarlo y exhibirlo permanentemente. Sin embargo, está naturalizado hacerlo, porque es requerido tanto en interacciones con el Estado como con empresas privadas. La información del DNI está incluida en un conjunto mayor llamado Sistema Federal de Identificación Biométrica (SIBIOS), utilizado por diversas agencias gubernamentales para entrecruzar información de diversas fuentes, entre ellas la agencia de impuestos (AFIP), la de Migraciones y la del registro individual de los trayectos en transporte público generado por el Sistema Único de Boleto Electrónico (SUBE). Hay muy escasa información oficial acerca de qué hace el Estado exactamente con esos datos recabados, por cuánto tiempo los almacena, cómo los analiza, quiénes tienen acceso a ellos ni con qué fines. En junio de 2014, el ministro de Interior y Transporte comunicó desde España que, desde algún momento de 2015, los DNI emitidos serían tarjetas inteligente multipropósito de dos chips que registrarían no solo datos biométricos y domiciliarios, sino también los de ANSES (la oficina que gestiona los aportes a la seguridad social) y los del SUBE. La supuesta comodidad para el ciudadano del nuevo sistema no fue el único argumento esgrimido por el funcionario. También se refirió a una eventual "prevención del delito". En este artículo se reflexiona sobre el carácter de "caja negra" –como diría Bruno Latour– del sistema sociotécnico del cual el DNI argentino es la cara visible y –como diría Michel Foucault– sobre cómo la evolución de dicho sistema lleva a los sujetos a exponer cada vez más cierta "verdad" sobre sí mismos, a la manera de una confesión involuntaria e invisible que refuerza un poder ejercido sobre quien "confiesa".

Palabras clave: Documento nacional de identidad, biometría, tarjetas inteligentes multipropósito, cajanegrización, veridicción

INTRODUCCIÓN

En la Argentina tenemos un organismo público al que la Ley 26.338 asigna temáticas a primera vista sin relación. Entre ellas:

- "el ejercicio de los derechos políticos de los ciudadanos",
- "todo lo relacionado con el transporte internacional, terrestre, marítimo y fluvial" y

[1] Fundación Vía Libre – Universidad de Buenos Aires, Facultad de Ciencias Sociales, Lic. En Comunicación y doctoranda en Ciencias Sociales – Santiago del Estero 1029, CABA, Argentina – laura.siri@gmail.com

- “la organización, conducción y control del Registro Nacional de las Personas” (RENAPER).

Se trata del Ministerio del Interior y Transporte, dependiente de la Presidencia de la Nación.

Con el fin de garantizar los derechos políticos de la ciudadanía, este Ministerio se encarga de organizar los procesos electorales, en particular los padrones de votantes. Como parte de la gestión en transporte, también administra el Sistema Único de Boleto Electrónico (SUBE). El uso de la tarjeta que habilita el acceso al transporte con el sistema SUBE es opcional pero, si no se usa, el costo de los viajes es mayor. También es posible usar esa tarjeta sin registrarse con todos los datos personales pero, en caso de no hacerlo, no hay modo de reclamar el saldo no usado en caso de robo o extravío. El sistema arma una base de datos con los movimientos de los usuarios del transporte público registrados.

El RENAPER, por su parte, se ocupa de ejecutar la “Ley de identificación, registro y clasificación del potencial humano nacional”, sancionada en 1968 por un gobierno militar de facto (*cfr*. ADC, 2014). El Documento Nacional de Identidad previsto en esa norma es obligatorio, se requiere para cualquier interacción con el Estado, para trabajar legalmente en el país y para poder hacer transacciones privadas, como las bancarias. Incluye varios elementos biométricos, como la fotografía y la huella digital del pulgar. Objetar el hecho de que toda la población deba aportar sus huellas digitales al sistema es muy inusual, salvo entre activistas de la privacidad. No hay obligación por ley de portar siempre el DNI pero, en la práctica, los argentinos han naturalizado el hábito de hacerlo.

Las respectivas bases de datos administradas por éstos y otros sistemas del Ministerio del Interior y Transporte son entrecruzables con otras de los ministerios de Seguridad, de Justicia y de Economía y Finanzas Públicas. El número de DNI de una persona no se considera un dato sensible para la ley. Sin embargo, es una clave primaria que identifica a cada ciudadano tanto en el padrón electoral, como en el sistema de transporte, si está registrado. Y forma parte del número único de identificación laboral (CUIL) o número único de identificación tributaria (CUIT), que traza la vida laboral o comercial de las personas. De hecho, ahora se le asigna un CUIL al nacer a cada recién nacido y se lo consigna al dorso del DNI, también provisto al nacer.

La Fundación Vía Libre ya ha manifestado su preocupación por el rumbo que está tomando en la Argentina la recolección, almacenamiento y uso de datos personales por parte del Estado (sin que esto implique dejar de cuestionar lo mismo cuando lo hacen las empresas privadas). Es muy cuestionable, por ejemplo, el Sistema Federal de Identificación Biométrica para la Seguridad (SIBIOS), que escanea la ubicación de los ojos, nariz y contorno de las orejas de todas las personas que viajan al exterior y suma estos datos a otros que ya obran en poder de la administración pública (Cfr. Vía Libre, 2012 y 2014; Busaniche, 2012, entre otros).

Un video publicitario de la Dirección Nacional de Migraciones con el eslogan "Si nos conocemos mejor, nos cuidamos más" dejó así en claro el espíritu del sistema:

> […] en pocos segundos ejecuta la búsqueda sobre una base de datos de millones de huellas y rostros previamente registrados, asociados a un número de DNI […] Las fuerzas de seguridad de todo el país quedan integradas en una misma base de datos pudiendo ejercer un mayor control sobre los ciudadanos con prontuario y protegiendo la identidad del resto de la ciudadanía. La alta tecnología del sistema permitirá en el futuro integrar datos de voz, iris ocular e incluso del ADN.

No se ha divulgado aún información precisa sobre qué hace el Estado con todos los datos recabados hasta el momento, cuánto tiempo los almacena, quiénes tienen acceso a ellos, qué tipo de cruces se realizan entre las distintas bases de datos ni exactamente con qué fines.

Esta información es difícil de exigir, entre otras razones, porque la Argentina no cuenta con una ley nacional que obligue al Estado a proveer información. Solo existe un decreto que resulta insuficiente, el 1172/2013. Además, como analizó en detalle la Asociación Derechos Civiles (2014), aunque la ley de protección de datos en nuestro país parezca excelente, tiene dos inconvenientes que, en la práctica, la hacen casi inútil. El primero es que permite omitir la exigencia de permiso previo del interesado cuando los datos se "recaben para el ejercicio de funciones propias de los poderes del Estado o en virtud de una obligación legal". También habilita a las distintas dependencias del Estado a compartir entre sí datos personales. Con lo cual, sería posible que una de ellas tuviera excelentes prácticas de seguridad y los comparta con otra cuyos procedimientos fueran muy deficientes.

El segundo problema es que el órgano de control del cumplimiento de esta ley depende del Poder Ejecutivo. Con lo cual, no puede sorprender que las 137 inspecciones realizadas entre 2008 y 2012 fueron realizadas a empresas privadas, jamás a una dependencia estatal. Y que solo se aplicaron 36 sanciones entre 2005 y 2013, todas a entidades privadas y, en general, por incumplimientos meramente administrativos.

El hecho de que la legislación dificulte monitorear e impedir el mal uso que el Estado o los funcionarios públicos pudieran dar a los datos es motivo de especial inquietud. En efecto, ya se dio el caso de que, por una falla informática, fotos de varios millones de ciudadanos pudieron descargarse fácilmente del sitio del padrón electoral (Fernández, 2013). Nadie del Estado fue sancionado por permitir esa vulnerabilidad. Asimismo, cuando alguien que dijo ser de Anonymous quiso acceder a los datos de SUBE, lo hizo sin inconvenientes y, de nuevo, sin que el Estado asumiera responsabilidad alguna por la escasa seguridad del sistema (*La Nación*, 2012). Del mismo modo, información que la agencia impositiva o la de seguridad social deberían mantener confidencial en ocasiones ha quedado expuesta ante quien la quisiera aprovechar (Sanz, 2011).

En junio de 2014 se anunció una profundización de la política vigente de identificación personal. En efecto, el ministro de Interior y Transporte, Florencio Randazzo, comunicó desde España y sin precisar detalles que, desde 2015, habría un nuevo documento de identidad: una tarjeta inteligente multipropósito que permitiría unificar no solo datos biométricos y domiciliarios, sino también los de ANSES (es decir, la oficina que gestiona los aportes a la seguridad social) y los de SUBE. La comodidad que tendría para el ciudadano el nuevo sistema no fue el único argumento esgrimido en su momento por el ministro. También se refirió a una eventual “prevención del delito” (*Infobae*, 2014, entre otros medios).

Actores sociales como Madres de Plaza de Mayo Línea Fundadora, Asamblea Permanente por los Derechos Humanos, Liga por los Derechos del Hombre, Servicio Paz y Justicia, Comisión Provincial por la Memoria, Asociación por los Derechos Civiles, Fundación Vía Libre y Asociación Pensamiento Penal, entre otros, manifestaron su preocupación ante este nuevo desarrollo del DNI argentino. Principalmente porque un documento nacional basado en tarjetas inteligentes multipropósito genera un punto único de posible falla. Si alguien logra vulnerarlo, no solo podría usurpar identidades,

sino también acceder y usar como guste la información relacionada con salud, educación, trayectos en transporte público o consumo. Y aunque fuera una tecnología totalmente segura, implica un hito más en una tendencia creciente por parte del Estado a la recolección y análisis de datos utilizables para la vigilancia total de la ciudadanía.

LO QUE INFORMÓ EL GOBIERNO

Las fuentes oficiales para conocer fehacientemente cómo será el DNI electrónico argentino son escasas y poco detalladas. Probablemente porque este desarrollo se enmarca en un acuerdo de cooperación con la Casa de la Moneda de España que, en su cláusula sexta, establece para las partes una obligación de confidencialidad. Así que, además del anuncio inicial hecho desde ese país, solo contamos con las antes mencionadas respuestas a los sendos pedidos de informes al Ejecutivo por parte del diputado nacional Manuel Garrido y de la Asociación Pensamiento Penal. Se extracta a continuación lo más relevante expresado en esos documentos:

- El DNI electrónico tendrá dos chips, uno de los cuales está previsto que sea RFID. Éste tendrá la única función de interactuar con el Sistema Único de Boleto Electrónico (SUBE) y tendrá los mismos datos.
- El poseedor del DNI podrá autenticar su identidad en forma automática al momento de realizar ciertos trámites o transacciones en línea, para mayor simplicidad y ahorro de tiempo.
- El Estado se beneficiará por el uso más eficiente y el acceso seguro a información y datos que hoy se encontrarían dispersos.
- El Ministerio del Interior y Transporte, a través del RENAPER, tendrá a cargo la recolección, conservación, ordenación, almacenamiento, relacionamiento, evaluación, bloqueo, destrucción y procesamiento de los datos del Nuevo DNI.
- Afirma que lo hará en forma directa y 100% estatal.
- La modificación de datos que no sean de identificación será responsabilidad del organismo o la entidad responsable de su generación.

- El chip es un nuevo elemento de seguridad que reduciría las posibilidades de falsificación o adulteración de los documentos.
- Se tomarán las mismas medidas de seguridad que hoy existen para el almacenamiento de los datos de identificación de los ciudadanos existentes en los Archivos y bases de datos del Registro Nacional de las Personas, así como el mismo tratamiento, restricción en su acceso y protección de datos personales que rige en la actualidad (esta cita es del informe para el Sr. Garrido. En la de la APP en cambio decía en cambio que la nueva tecnología "consiste en dotar de mayores medidas de seguridad al DNI", lo cual es contradictorio).
- El cambio previsto no guardaría relación con posibles deficiencias en las medidas de seguridad del actual DNI.
- El DNI electrónico no representaría modificación alguna a las interfases entre el RENAPER y el SIBIOS, por lo que los datos de identificación biográficos y biométricos continuarán siendo transferidos de igual forma que en la actualidad.
- No será obligatorio cambiar de tarjeta. Este cambio no implica modificaciones en la validez ni la convivencia con los DNI en circulación [claro está, quienes sí deban volver a tramitar el DNI, no es de esperar que puedan elegir entre el que tiene chip y el que no lo tiene]

QUÉ IMPLICA QUE EL DNI SEA UNA TARJETA INTELIGENTE MULTIPROPÓSITO

Los documentos de identidad tradicionales, aunque contengan datos biométricos como fotos y huellas digitales, no incluyen ni transmiten información desconocida para el portador. Y, cuando son exhibidos a otras personas, no interactúan con sistemas externos. ¿Qué ocurre si el documento de identidad es una tarjeta inteligente?

Para responder, es útil no usar como referencia una fuente crítica hacia este tipo de dispositivos sino una que, por el contrario, privilegie sus supuestas ventajas y aun así permita dejar claros posibles cuestionamientos. No es el único, pero un libro clásico al respecto es el manual técnico de Mike Hendry (2007) *Multiapplication Smart Cards*. Como explica este autor, las tarjetas inteligentes no solo contienen datos, sino que

pueden realizar operaciones, como compararlos contra una fuente externa, procesar una firma electrónica y almacenarlos en áreas secretas, solo accesibles en principio por el software de la tarjeta. Por lo tanto, un documento de identidad así podría contener información sobre su portador que éste desconociera y que hasta pudiera eventualmente incriminarlo. También podría disparar al ser utilizado interacciones cuyas consecuencias, buenas o malas, resultaran imprevisibles. Asimismo, aunque teóricamente es posible y deseable diseñar la seguridad de las tarjetas inteligentes de modo que no todo funcionario público o privado pueda acceder a todo dato, en la práctica el ciudadano no tiene modo de saber si el sistema fue programado de ese modo y, si así fue, si un error involuntario permitió por ejemplo a un policía de tránsito mirar lo que solo debía ver su médico.

Hendry (*op. cit*.) también destaca que la industria de tarjetas inteligentes está avanzando hacia aquellas que son multipropósito. Según el autor, la razón principal es que así los proveedores pueden vender un producto más costoso y argumentar que tanto la entidad emisora (el gobierno, en el caso de los documentos de identidad) como los usuarios podrán usarlo en diferentes entornos, ganando en comodidad y rapidez de las transacciones. Es así que la tarjeta de identidad de Malasia incluye también el carnet de conducir, un monedero electrónico, el acceso al sistema de salud y firma digital para comercio electrónico.

Se supone que las distintas aplicaciones que puede contener el chip inteligente multipropósito pueden mantener sus respectivos datos separados y la terminal simplemente elige unos u otros según permisos preasignados. Sin embargo, es técnicamente posible que esos datos sí sean compartidos entre aplicaciones y, de hecho, esa es la manera usual para que dichas aplicaciones puedan cooperar.

También una tarjeta puede tener dos chips. Típicamente, uno de ellos es una antena RFID (tecnología especialmente cuestionada en cuanto a sus implicancias para la privacidad). Es el caso del futuro DNI argentino. Al ser chips distintos, las aplicaciones de ambos no pueden cooperar y, en realidad es como si fueran dos tarjetas distintas. En el DNI argentino, sin embargo, parece irrelevante desde el punto de vista de la privacidad si las aplicaciones de cada chip comparten datos o no. Porque, por lo explicado anteriormente, cada dependencia pública por ley puede compartirlos con otras. Así que los datos ya pueden integrarse a nivel de sistemas centrales. No hay

mucha diferencia si también lo son en la tarjeta misma. Además, es insustancial que solo uno de los chips contenga los datos del DNI y el otro los de información relativa a servicios públicos que utilice el portador, dado que los datos del DNI siempre son un subconjunto de aquellos relativos al acceso a dichos servicios públicos.

Por otra parte, una de las características más poderosas de las este tipo de tarjetas es que pueden descargar o actualizar aplicaciones después de que han sido emitidas y entregadas al usuario. Con lo cual, cada vez que el documento interactúa con una terminal de reconocimiento, podría estar recibiendo datos, con o sin el conocimiento del portador. En el caso de los documentos de identidad sería posible, por lo tanto, que la aplicación A efectivamente no comparta datos con la B pero que, al interactuar con una terminal de reconocimiento, la A envíe datos actualizados a un sistema central del gobierno, que ese sistema central cruce datos con los de la B y luego descargue en la A de la tarjeta la actualización del estatus correspondiente. Todo sin conocimiento del portador y, por lo tanto, sin posibilidad real de hacer una denuncia en caso de una eventual violación de las leyes de protección de la privacidad u otros derechos civiles.

Otro punto digno de subrayar es que es técnicamente posible en un chip integrar aplicaciones estatales como privadas. De hecho, las respuestas a los pedidos de informes dadas por el Ejecutivo sugieren que ése será efectivamente el caso en la Argentina, ya que hablan de acceso a “servicios públicos”. Que un servicio sea público no implica que lo brinde el Estado. El documento de identidad biométrico con chip de Nigeria, por ejemplo, no solo puede usarse como medio de pago, sino que generó controversias porque hasta incluía el logo de la empresa Mastercard (Ekott, 2014).

Además, cuando todas las aplicaciones cargadas en la tarjeta son del mismo emisor, por ejemplo el Estado, pueden diseñarse y probarse juntas para satisfacer determinados criterios de buen funcionamiento y eventuales restricciones de interoperabilidad. Si se suman aplicaciones de otros actores, en cambio, la complejidad aumenta. Por otra parte, cuantas más funciones tiene la tarjeta, mayor es el inconveniente para el usuario en caso de pérdida o robo, debido a que deja de poder acceder a varios sistemas transaccionales a la vez hasta que se le otorga una nueva.

En cuanto a la seguridad para el usuario, Hendry (*op. cit*.) advierte que, del mismo modo que con el software de una PC, no es posible garantizar al 100 por 100 que una aplicación en una tarjeta inteligente estará libre de errores o comportamientos

inesperados. El autor enumera una lista de posibles ataques o errores involuntarios a la seguridad del sistema y resalta que, a lo largo de la vida útil de una tarjeta inteligente, más posibles vulnerabilidades podrían descubrirse. Sin omitir el hecho de que todo esquema de seguridad no depende solo de tecnología, sino de un correcto diseño de políticas y procedimientos, y de que las autoridades a cargo los hagan cumplir.

Acerca de la seguridad nacional, el autor expresa que:

> […] a menudo es citada como parte del caso de negocios de emitir tarjetas de identidad. Sin embargo, un análisis de riesgos detallado muestra que en muchas situaciones los beneficios de seguridad serían marginales, mientras que se generan riesgos de que usar la tarjeta pueda reducir el incentivo de llevar a cabo otros chequeos, posiblemente más efectivos".

Con respecto a su potencial para la prevención del delito común, en el caso del nuevo DNI argentino ese argumento es aún más débil, sencillamente porque el gobierno afirma que no será obligatorio cambiar el existente. Así que es improbable que los delincuentes profesionales se sientan inclinados a someterse voluntariamente al uso de una tecnología que podría comprometerlos.

ANÁLISIS Y REFLEXIONES

Las tecnologías usadas para identificar ciudadanos no pueden aislarse de los contextos sociales en que se implementan. Es cierto que las tendencias para "modernizarlas" vienen de la mano de grupos de influencia que actúan en todo el mundo, como la Smart Card Association, el Biometric Consortium y la International Civil Aviation Organization (ICAO), y que dichos actores interactúan asiduamente con la mayoría de los gobiernos del mundo. Pero el grado y la forma en que cada país se enrola en este "card cartel" (Lyon, 2009) son siempre específicos.

Por ejemplo, son conocidas las grandes controversias que el intento de implementar documentos de identidad inteligentes biométricos despertó en Australia, Reino Unido, Japón y Francia (Lyon, 2008), entre otros países. En la Argentina, sin embargo, la discusión fue y es muy minoritaria. Es cierto que en el momento del anuncio del futuro DNI apareció una editorial en un diario crítico con el gobierno (*La Nación*, 2014), un

comunicado conjunto de las asociaciones enumeradas al principio[2], los antes mencionados pedidos de informes y algunos artículos de blog. Pero el tema no permaneció en agenda ni se puede decir que haya logrado involucrar masivamente a la población.

Por otra parte, en la Argentina se puede observar, tanto en el texto de la ley como en la percepción general del tema, que el concepto de privacidad está resignificado como una simple "protección de datos". Esta resignificación sustituye como bien protegido a las personas y sus derechos por objetos abstractos: los datos (Bonner y Chiasson, 2005). Por ejemplo, en las típicas encuestas sobre los temas que más preocupan a la población aparece siempre la inseguridad. Sin embargo, no se manifiesta igual preocupación por la privacidad, cuando sin ésta también se compromete gravemente la seguridad.

Otra particularidad argentina es que existe una alta polarización política entre quienes apoyan al partido actualmente gobernante y quienes se le oponen. De este modo, es muy difícil hablar mal o bien en público sobre una política en particular sin que se interprete como oposición u adhesión generalizadas al gobierno como un todo. A la inversa, algunos critican o alaban determinada política porque en realidad lo que cuestionan o defienden es la totalidad de lo que hace el oficialismo.

Lyon (2009) subraya el atentado a las Torres Gemelas y el giro desde el bienestar hacia la seguridad como prioridad de los Estados entre los grandes disparadores de la voluntad política de emitir tarjetas de identidad biométricas obligatorias. Esta reflexión, sin embargo, no es aplicable a la Argentina, porque el atentado en New York no impulsó localmente la misma sensación de peligro generalizada y porque en este país la seguridad no parece la mayor preocupación de la política gubernamental actual. El control inmigratorio tampoco es un objetivo particularmente relevante. No es que estas metas no existan, no es que no haya abusos de poder, pero el discurso oficial pone el énfasis en otras cosas.

El objetivo manifestado, más bien, parece ligado a poder discriminar a quién otorgar y a quién no determinados beneficios sociales. Así lo explicó el entonces Subsecretario de Tecnologías de Gestión, Eduardo Thill en el VI Congreso Internacional de Biometría de la República Argentina desarrollado en Buenos Aires en noviembre de 2011:

[2] Ver http://www.pensamientopenal.org.ar/dni/

> El ejercicio de los derechos requiere necesariamente la identificación plena de las personas. Este rol en nuestro país lo cumple el Estado. […] La identificación electrónica es necesaria para el acceso a sistemas informáticos, a las aplicaciones de gobierno electrónico, de comercio electrónico, pero también para la ejecución de políticas sociales. […] el mundo ha avanzado en el uso de tecnologías biométricas para los documentos nacionales que acreditan las identidades de las personas. […] Por esta razón, desde el año 2003 se ha ido trabajando en la digitalización del trámite de dicho documento […].

Por supuesto, la actual infraestructura de identificación de personas puede en cualquier momento privilegiar más su potencial para reprimir, intimidar y restringir libertades, y no tanto el de distribuir beneficios sociales. Mientras, el DNI electrónico es presentado por el gobierno como una simple y positiva "innovación técnica". Gran parte de la población probablemente lo vea del mismo modo. En efecto, como siempre fue obligatorio poseer un DNI y siempre se han tomado las huellas digitales de toda la población, cualquier controversia al respecto está anestesiada desde hace mucho. Además, era tradicional que en caso de pérdida o robo del documento, tramitar otro llevara meses y, mientras tanto, los inconvenientes cotidianos eran enormes. Ahora se expide en menos de media hora, sin hacer fila y se recibe en días. Lo que hay detrás de estas "innovaciones técnicas" y si tiene esta comodidad un precio en términos de privacidad, seguridad y libertad se encuentra "cajanegrizado". El DNI electrónico multipropósito es de prever que será igualmente "cajanegrizado".

Recordemos que, para la sociología de la traducción, la cajanegrización es "el camino mediante el cual el trabajo científico o técnico se vuelve invisible a causa de su propio éxito. Cuando una máquina funciona eficientemente o un hecho está establecido con firmeza, uno solo necesita concentrarse en los beneficios que genere y no en su complejidad interior. Así, paradójicamente, sucede que la ciencia y la tecnología cuanto más éxito obtienen más opacas se vuelven" (Latour, 2001:362).

La sociología de la traducción es una teoría útil para estudiar los documentos de identidad, porque pone especial atención a las "cajas negras" empleadas por los "actantes". Es decir, aquellos que actúan o llevan a otros a actuar. Las cajas negras, una vez "enroladas", se convierten ellas mismas en actantes y contribuyen a dar forma a la conducta de quienes las usan. La caja negra expresa una verdad que se asume como garantizada, una simple etiqueta que reemplaza y evita la problematización de su contenido.

Por cierto, la idea misma de que el DNI inteligente es seguro y cómodo también es una caja negra. Es un intento de no problematizar algo que otros actores sociales consideran (consideramos) altamente problematizable. Pero, al mismo tiempo, apunta a enrolar o convertir en aliados a otros actores que, en la Argentina, hasta el momento parecen mayoritarios: quienes simplemente usan los artefactos técnicos disponibles por su funcionalidad o comodidad y solo los descajanegrizarán si ocasionan algún problema serio y masivo contra la seguridad, integridad física o libertad de individuos o grupos con los cuales se identifiquen.

A esta altura es interesante mencionar un trabajo de Carmen Romero Bachiller (2008), donde afirma que:

> Ciertos elementos "no-humanos", en concreto los documentos de identidad/identificación, adquieren una preeminencia particular, convirtiéndose en auténticas "extensiones protésicas" que permiten asegurar la legitimidad de los "cuerpos" y garantizan la posibilidad de que sean siempre reconocibles en los regímenes fijados.

Las extensiones protésicas son artículos, como los lentes para ver, que de algún modo pasan a constituir nuestro ser, sin importar que no formen parte del equipamiento natural de nuestro cuerpo sin ellos. Y, como a toda caja negra, solo las problematizamos si en algún momento funcionan mal. ¿Han devenido los DNI en extensiones protésicas?

En la Argentina sin duda la respuesta es que tradicionalmente sí. Sin embargo, la evolución del DNI obligatorio hizo de este importante documento una pequeña parte de un sistema mucho mayor que vincula a una persona no solo con los datos inscriptos en él, sino con archivos de la policía, la AFIP, el registro de reincidencias, el padrón electoral, la ANSES y el sistema de transporte público. El DNI argentino, de este modo, tiende a dejar de ser una simple extensión protésica, para convertirse en una representación metonímica de la persona misma y en un instrumento que produce verdades sobre el individuo en cada una de sus interacciones diarias. Y así como hay en la sociedad escasa vocación de "descajanegrizar" el DNI en su estatus de extensión protésica, tampoco es de esperar que la haya para hacerlo en su estatus de política de veridicción.

Es aquí que se puede establecer una complementariedad en el análisis del DNI argentino entre el enfoque basado en la sociología de la traducción y los análisis sobre

poder, verdad, sujeto y dispositivos de Michel Foucault. Una complementariedad que no necesariamente sería aplicable del mismo modo a la implementación de un documento de identidad electrónico en cualquier país.

Recordemos que el poder, según Foucault, necesita para producirse reglas para discriminar lo verdadero de lo falso en el sujeto. Dichas reglas están históricamente constituidas y se puede hablar de tecnologías de la verdad, o de veridicción, para referirse a los medios de producir verdad en cada contexto histórico. Un ejemplo de tecnología de la verdad es la producción de la confesión: "un acto verbal mediante el cual el sujeto plantea una afirmación sobre lo que él mismo es, se compromete con esa verdad, se pone en una relación de dependencia con respecto a otro y modifica a la vez la relación que tiene consigo mismo" (Foucault, 1981:p27). La confesión requiere de un interlocutor, o una instancia de interlocución. Puede ser espontánea o dictada por un imperativo moral. Pero también arrancada por la fuerza. Además, "ya no se la percibe como el efecto de un poder que nos constriñe" (Foucault, 1978, p. 60). Se "cajanegriza", diría Latour. Más aún: "La confesión de la verdad se ha inscripto en el corazón de los procedimientos de individualización por parte del poder y [ha devenido en] una de las técnicas más valiosas en Occidente para producir la verdad" (Foucault, *op. cit*., p. 59). Si para la Iglesia la confesión prometía la salvación del alma, para la sociedad occidental también promete una salvación, pero secular y orientada a la salud y al bienestar. El precio es que a través de la confesión los individuos en realidad están tomando un rol activo en su propia vigilancia.

Así, complementando a Latour con Foucault, podría decirse que el DNI argentino, como representación metonímica cajanegrizada del individuo, "confiesa" en su lugar. El ciudadano no necesita autoincriminarse ni explicar sus acciones. Hay un dispositivo técnico, del cual su DNI es solo la cara visible, que permanentemente va produciendo verdad sobre él. Y lo que confiesa este artefacto se considera mucho más verosímil que lo que el sujeto pudiera decir de sí mismo. Tiene la fuerza convincente de la creencia en la infalibilidad de la ciencia y la ingeniería. Si un sistema técnico reconoce en una persona a un criminal buscado o alguien a quien se le debe denegar un servicio o acceso, es muy difícil para la persona argumentar que está equivocado (Feldman, 2003).

La confesión generada por las huellas que va dejando la representación metonímica de la persona (su documento) es en parte forzosa en la Argentina, por el hecho de que

todo ciudadano debe tener DNI desde que nace. Pero en parte será “voluntaria”, si decide aprovechar la comodidad de poder hacer más de una transacción con una misma tarjeta cuando el DNI sea “inteligente”. Claro está, como ya se argumentó en Gran Bretaña ante el intento de imponer un sistema análogo, lo “voluntario” pueden fácilmente convertirse en obligatorio “de facto”, como ya ocurrió en la India. El Estado no tiene más que dar incentivos “positivos” (como mejores condiciones de acceso a ciertos servicios) para el cambio de DNI, o negativos (como la denegación de otros en caso de no tener el nuevo). Quien opte por ejercer su derecho a no colaborar “voluntariamente” con el creciente escrutinio, sabrá que no hará más que singularizarse como un excéntrico sospechoso y probablemente se convierta en blanco de mayor vigilancia. Pero, por las razones ya expuestas, en la Argentina por el momento parece improbable que tengan éxito estos argumentos para detener el eDNI, como sí lo tuvieron en el Reino Unido.

La solución, desde el punto de vista de quienes sí se preocupan por las consecuencias del sistema técnico y político cuya cara más visible es el DNI, podría ser tan simple como no dejar morir el debate al respecto. En efecto, para la «sociotecnología» de Trevor Pinch y Wiebe Bijker (1987), una tecnología específica no resulta adoptada o rechazada por la sociedad debido a sus virtudes o defectos intrínsecos, sino a cómo ciertos grupos sociales relevantes atribuyen a los artefactos involucrados y cómo piensan los problemas y soluciones generados por éstos. En el proceso, los artefactos en cuestión pasan de una etapa de flexibilidad interpretativa (caracterizada por la controversia) hacia otra de estabilización o clausura. La consecuencia lógica es que, mientras exista un solo grupo social relevante que mantenga viva la controversia, podrá haber tendencias fuertes, grandes consensos, imposiciones por la fuerza, pero no clausura. La tarea del activista, por lo tanto, debería ser “descajanegrizar”, en un contexto donde nadie quiere ver lo que hay dentro de esas cajas negras que parecen funcionar tan bien. O producir verdad, pero no a la manera de quien confiesa a requerimiento de otros, sino a la del “parresiastés” (Foucault, 2010) que insiste en manifestar ciertas cosas cuando su sociedad preferiría no oírlas.

REFERENCIAS

Asociación Derechos Civiles [ADC]. *El Estado recolector: Un estudio sobre la Argentina y los datos personales de los ciudadanos*. Buenos Aires. Recuperado de http://www.adc.org.ar/wp-content/uploads/2014/09/El-estado-recolectorInformeADC.pdf

Bonner, W., & Chiasson, M. (2005). If fair information principles are the answer, what was the question? An actor-network theory investigation of the modern constitution of privacy. *Information and Organization*, *15*(4), 267–293. doi:10.1016/j.infoandorg.2005.03.001

Busaniche, B. (14 de agosto de 2012). El fin del derecho a la intimidad. *La Nación*. Recuperado de http://www.lanacion.com.ar/1499039-el-fin-del-derecho-a-la-intimidad

Hendry, M. (2007). *Multi-application Smart Cards: Technology and Applications*. New York: Cambridge University Press.

Feldman, R. (2003). Considerations on the Emerging Implementation of Biometric Technology. *Hastings Communications and Entertainment Law Journal*, *25*(654). Recuperado de http://repository.uchastings.edu/faculty_scholarship/160

Foucault, M. (1978). *The history of sexuality Volume 1: An Introduction*. New York: Vintage Books.

Foucault, M. (1981). *Mal faire, dire vrai. Fonction de l'aveu en justice. Cours de Louvaine* Presses Universitaires de Louvaine - Trad. cast.: *Obrar mal, decir la verdad*, Buenos Aires, Siglo XXI, 2014.

Foucault, M. (2010) *El coraje de la verdad. El gobierno de sí y de los otros II*. Curso en el Collège de France. Fondo de Cultura Económica, Buenos Aires.

Latour, B. (1994/1998): "De la mediación técnica: filosofía, sociología, genealogía", en Miquel Domènech y Francisco Javier Tirado (comps.), Sociología Simétrica. Ensayos sobre ciencia, tecnología y sociedad, Barcelona, Gedisa: 249-302.

Latour, B. (2001). *La esperanza de Pandora: Ensayos sobre la realidad de los estudios de la ciencia*. Barcelona: Gedisa.

Lyon, D., & Bennet, C. (Eds.). (2008). *Playing the ID card: Understanding the significance of identity card systems*. London and New York: Routledge.

Lyon, D. (2009). *Identifying Citizens: ID Cards as Surveillance*: Polity Books.

Pérez Esquivel, A. (2 de octubre de 2014). *APP frente al anuncio de los nuevos DNI electrónicos*. Buenos Aires. Recuperado de http://www.pensamientopenal.org.ar/app-frente-al-anuncio-de-los-nuevos-dni-electronicos

Pinch, T. J. y Bijker, W. E. (1987) The social construction of facts and artifacts. W. BIJKER, T. HUGHES, y T. PINCH (Eds.) *The social construction of technological syst*ems. Cambridge, MA: MIT Press, p. 17-50.

Registro Nacional de las Personas [RENAPER] (5 de agosto de 2014). *Respuesta al pedido de informes del diputado Manuel Garrido sobre DNI electrónicos*. Buenos Aires. Recuperado de http://www.vialibre.org.ar/files/escanear0113.pdf

Registro Nacional de las Personas [RENAPER] (16 de septiembre de 2014). *Respuesta del PEN a la Asociación Pensamiento Penal.*

Romero Bachiller, C. (2008). Documentos y otras extensiones protésicas, o como apuntalar la "identidad". *Política y Sociedad*, *45*(3), 139–157.

Thill, E. (2011) El rol de la identificación de personas en las políticas de desarrollo e inclusión digital: el Marco para la Identificación Electrónica Social Iberoamericana. Thill, E. (Ed.). (2011). *Biometrías 2*. Buenos Aires, 11-32.

Fundación Vía Libre (27 de enero de 2012). Con SUBE sí vas a pagar más caro: el fin de la privacidad. Recuperado de http://www.vialibre.org.ar/2012/01/27/con-sube-si-vas-a-pagar-mas-caro-el-fin-de-la-privacidad/

Fundación Vía Libre (11 de agosto de 2014). Acceso a Información Pública: Magras respuestas sobre el proyecto de nuevo DNI. Recuperado de http://www.vialibre.org.ar/2014/08/11/acceso-a-informacion-publica-magras-respuestas-sobre-el-proyecto-de-nuevo-dni/

Artículos periodísticos

Ekott, I. (29 de agosto de 2014). Scandalous: Outrage in Nigeria as government brands National ID Card with MasterCard's logo. *Premium Times*. Recuperado de http://www.premiumtimesng.com/news/headlines/167479-scandalous-outrage-in-nigeria-as-government-brands-national-id-card-with-mastercards-logo.html

Fernández, P. (4 de noviembre de 2013). Por una falla de seguridad se pueden descargar fotos del padrón electoral. *Infotechnology.com*. Recuperado de http://www.infotechnology.com/internet/Por-una-falla-de-seguridad-se-pueden-descargar-fotos-del-padron-electoral-20131104-0001.html

El nuevo DNI tendrá un chip que incluirá la historia clínica de las personas y los datos de su SUBE (27 de junio de 2014). *Infobae*. Recuperado de http://www.infobae.com/2014/06/27/1576438-el-nuevo-dni-tendra-un-chip-que-incluira-la-historia-clinica-las-personas-y-los-datos-su-sube

Exponen en la Red los registros de viajes de la tarjeta SUBE (30 de enero de 2012). *La Nación*. Recuperado de http://www.lanacion.com.ar/1444623-exponen-en-la-red-los-registros-de-viajes-de-la-tarjeta-sube

Sanz, F. Filtración de información privada en AFIP (2 de enero de 2011). *Fernando.com.ar*. Recuperado de http://www.fernando.com.ar/2011/afip-filtra-informacion-privada/

La peligrosa pulsión por controlarlo todo (10 de julio de 2014). *La Nación*. Recuperado de http://www.lanacion.com.ar/1708516-la-peligrosa-pulsion-por-controlarlo-todo