



Tipo de documento: Tesina de Grado de Ciencias de la Comunicación

Título del documento: El dispositivo documentario como ensamble entre el período disciplinario y la era del control

Autores (en el caso de tesistas y directores):

María Fernanda Cáceres

Carla Noelia Montes

Beatriz Busaniche, tutora

Datos de edición (fecha, editorial, lugar,

fecha de defensa para el caso de tesis): 2016

Documento disponible para su consulta y descarga en el Repositorio Digital Institucional de la Facultad de Ciencias Sociales de la Universidad de Buenos Aires.
Para más información consulte: <http://repositorio.sociales.uba.ar/>

Esta obra está bajo una licencia Creative Commons Argentina.
Atribución-No comercial-Sin obras derivadas 4.0 (CC BY 4.0 AR)



La imagen se puede sacar de aca: https://creativecommons.org/choose/?lang=es_AR





UNIVERSIDAD DE BUENOS AIRES

Facultad de Ciencias Sociales

Carrera Ciencias de la Comunicación Social

Tesina de grado

*El dispositivo documental como ensamble entre el período
disciplinario y la era del control*

Alumnas:

María Fernanda Cáceres

DNI: 28.232.788

Celular: (15)3595-5193

E-mail: mf_caceres@hotmail.com.ar

Carla Noelia Montes

DNI: 28.383.585

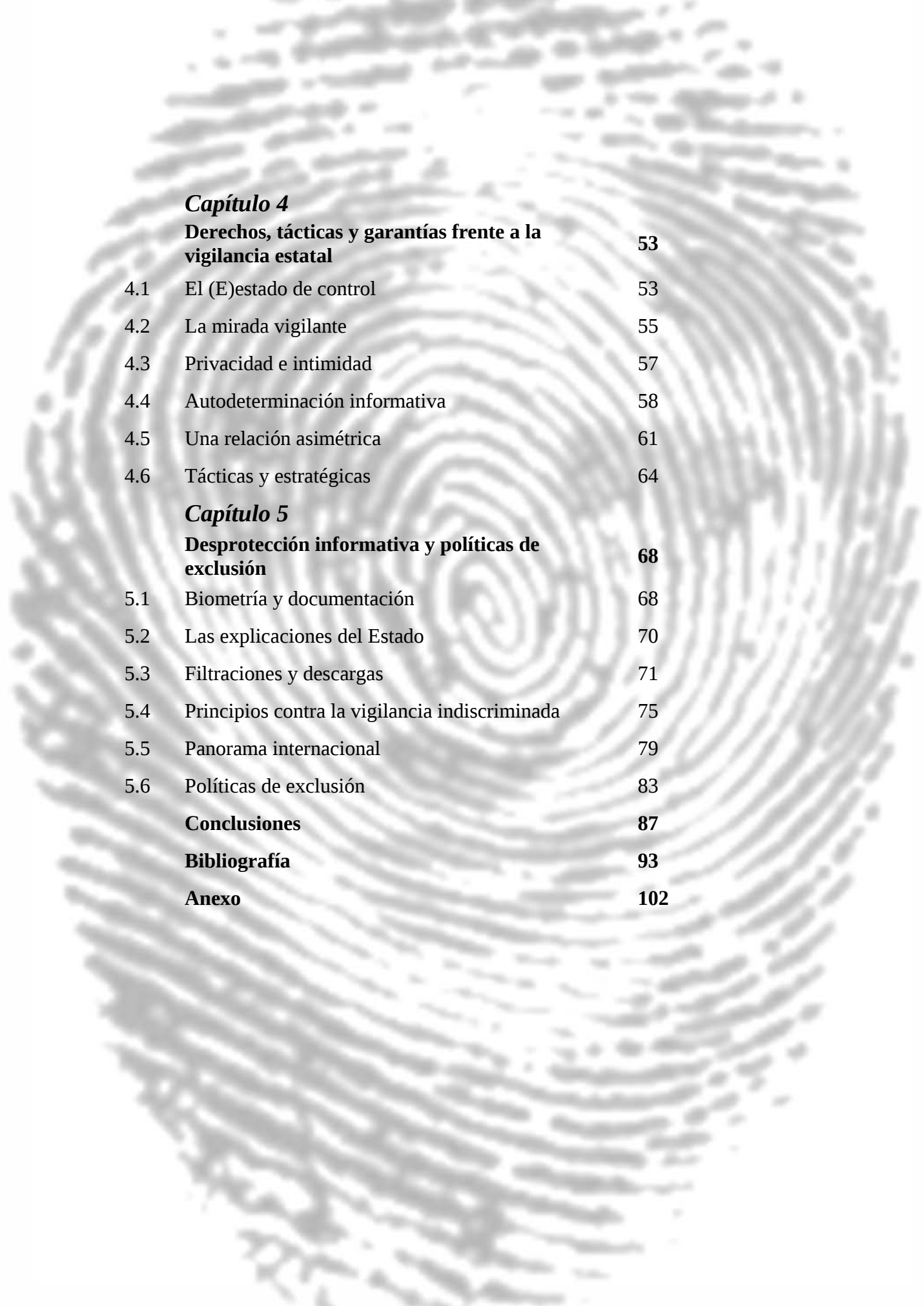
Celular: (15)6583-5191

E-mail: cnmontes@gmail.com

Tutora: Beatriz Busaniche

Índice

Introducción	5
Capítulo 1	
Entre el período disciplinario y la era del control	9
1.1 El Estado como administrador del cuerpo social	9
1.2 Poder de vida y de muerte	10
1.3 Anatomopolíticas y biopolíticas	12
1.4 De la sociedad disciplinaria a la sociedad de control	15
1.5 Matices de la sociedad de control	19
Capítulo 2	
Genealogía del proceso documentario	23
2.1 Pioneros en identificación dactilar	23
2.2 Antecedentes de registro de identificación	25
2.3 Documento Nacional de Identidad	26
2.4 Rastros de un sistema obsoleto	27
2.5 Nueva etapa en el registro de los ciudadanos	28
2.6 Nuevo DNI	30
2.7 Nuevo Pasaporte	33
2.8 SIBIOS, la gran base estatal de datos	35
Capítulo 3	
La identificación en clave biológica	38
3.1 Identificar a la población	38
3.2 Ciencia, tecnología y cuerpo	39
3.3 Un <i>quién es quién</i> estatal	43
3.4 Marcas indelebles	46
3.5 “Documentos, por favor”	47
3.6 Un panóptico de bolsillo	49



Capítulo 4

Derechos, tácticas y garantías frente a la vigilancia estatal 53

- 4.1 El (E)estado de control 53
- 4.2 La mirada vigilante 55
- 4.3 Privacidad e intimidad 57
- 4.4 Autodeterminación informativa 58
- 4.5 Una relación asimétrica 61
- 4.6 Tácticas y estratégicas 64

Capítulo 5

Desprotección informativa y políticas de exclusión 68

- 5.1 Biometría y documentación 68
- 5.2 Las explicaciones del Estado 70
- 5.3 Filtraciones y descargas 71
- 5.4 Principios contra la vigilancia indiscriminada 75
- 5.5 Panorama internacional 79
- 5.6 Políticas de exclusión 83

Conclusiones 87

Bibliografía 93

Anexo 102

“Hasta podemos pensar que, mañana, la noción de identidad, de documento de identidad, será reemplazada por la trazabilidad de las personas. Una vez que se controlan todos los movimientos de un individuo, la cuestión de su identidad pierde todo interés. Basta con recabar informaciones sobre sus movimientos y la velocidad para localizar a la persona o el producto. La trazabilidad es un elemento inquietante de la vigilancia”.

Paul Virilo

Diario Página 12

20 noviembre de 2010



Introducción

La presente tesina busca examinar posibles líneas de investigación sobre el dispositivo documentario como un mecanismo de control estatal desde una perspectiva biopolítica, la cual ofrece interesantes posibilidades analíticas para el estudio de una serie de fenómenos contemporáneos.

Para lograrlo, se realizará un estudio exploratorio considerando que se busca una inicial aproximación a la temática que incluirá desde el origen del proceso documentario argentino hasta la implementación de una innovadora política de Estado en materia identificatoria impulsada por el gobierno de Cristina Fernández de Kirchner, período que abarcará hasta el 10 de diciembre de 2015.

La identificación de la población resulta una cuestión de suma importancia para los Estados modernos, por lo que la ciencia y la tecnología trabajan continuamente en el desarrollo, avance e innovación de nuevas y reconfiguradas técnicas y dispositivos que permiten profundizar y perfeccionar las tareas de reconocer, controlar y vigilar a los individuos.

De manera inicial, el fichaje social comenzó con los considerados grupos de riesgo tales como las clases peligrosas, los sospechosos, los criminales, los terroristas y los sectores vulnerables a la estigmatización, para luego extenderse al conjunto de la población. Históricamente, los documentos de identificación constituyeron herramientas políticas creadas por los Estados con el mencionado objetivo de registrar e identificar a las personas.

La República Argentina fue una nación pionera en estas metodologías identificatorias, lo que funcionó como condición de posibilidad para la incorporación de herramientas tecnológicas en estos dispositivos. Dichas modificaciones se caracterizaron por el uso de tecnología biométrica en el nuevo Documento Nacional de Identidad (DNI), sumada a la potencialidad de convertirlo en un carnet electrónico con la inclusión de dos chips (datos biométricos + información que pueda interactuar con otra contenida en diversos sistemas) y la conformación de una gran base estatal de datos con la finalidad de reunir los registros personales e identificar y monitorear a todos los ciudadanos.

La tecnología biométrica consiste en el estudio de las características cuantitativas de los seres vivos empleando diversas técnicas y se define como un método automatizado de reconocimiento del individuo, basado en características biológicas (anatómicas y fisiológicas) y de comportamiento medible.

La posibilidad de convertir al Nuevo DNI en un carnet inteligente multipropósito se plantea a raíz de la incorporación de un doble chip que, además de los datos biométricos de la persona, se incluirá nueva información como la historia clínica, datos previsionales y jubilatorios y la información de los trayectos de la tarjeta del Sistema Único de Boleto Electrónico (SUBE).

Por otra parte, se llevó a cabo la creación de la base estatal de datos a partir de la puesta en marcha del Sistema Federal de Identificación Biométrica para la Seguridad (SIBIOS), que tiene por objetivo prestar un servicio centralizado de información respecto de los registros patronímicos y biológicos individuales, a fin de contribuir a la comprobación oportuna en materia identificatoria de personas y rostros.

De esta manera, estudiaremos los cambios y transformaciones producidas en el proceso documentario a la luz del concepto de biopoder planteado por Michel Foucault (2006), así como también analizaremos el dispositivo documentario como ensamble entre el período disciplinario y la era del control.

Desde finales del siglo XX, asistimos a una etapa de transición de lo que se denominó sociedades disciplinarias (Foucault, 1975) hacia una sociedad de control (Deleuze, 1990). Mientras que Foucault centra su análisis en las instituciones de encierro -lugares a los que los sujetos ingresaban (escuela, hospital, fábrica, cuartel, etc.) y eran disciplinados de modo tal que pudieran resultar útiles al sistema-, Deleuze plantea que existe una crisis generalizada de estas instituciones, donde el encierro está siendo reemplazado por un control continuo (vigilancia e identificación) y una comunicación basada en la incorporación de nuevas tecnologías, por lo que surgen nuevos o reconfigurados dispositivos tecnológicos contruidos e impulsados en nombre de la seguridad y la protección.

Así, los Estados avanzan sobre la vigilancia y el control con el objeto (o la excusa) de proteger a las poblaciones de fenómenos como el terrorismo o la delincuencia mediante el desarrollo y la aplicación de estos mecanismos que, sirviéndose de las tecnologías de la información, permiten rastrear y monitorear a la ciudadanía de maneras cada vez más sigilosas e intrusivas.

En consonancia, la Argentina asiste a un momento en el que progresivamente se incorpora mayor tecnología en variados dispositivos sin vislumbrar claramente cuáles son los objetivos y sus alcances. Si bien algunas organizaciones manifestaron su preocupación por el avance de identificación de ciudadanos y el uso de múltiples técnicas para la vigilancia, estas cuestiones no reciben el debate público que merecen y

las medidas son tomadas mediante resoluciones administrativas sin la correspondiente instancia de tratamiento y discusión en el Congreso Nacional.

En este contexto decidimos analizar el DNI -principal dispositivo de identificación de la sociedad disciplinaria argentina- con la reciente incorporación de tecnología digital. A su vez, intentaremos reconstruir la genealogía del DNI como dispositivo biopolítico, sus cambios y transformaciones, así como la incidencia en la privacidad, las libertades civiles y la protección de la intimidad garantizada por la Constitución Nacional.

El relevamiento de la evolución histórica nos permitirá exponer la matriz autoritaria del dispositivo documentario, ya que partirá del sistema de identificación por medio de huellas dactilares y hará foco en la Ley N° 17.671 de Identificación, Registro y Clasificación del Potencial Humano Nacional, sancionada en 1968 por el presidente de facto Juan Carlos Onganía; base sobre la que implementó el Nuevo DNI, incluyendo los tres cambios de formato realizados en los últimos cuatro años durante la presidencia de Cristina Fernández de Kirchner.

A modo de hipótesis inicial, consideramos que los acelerados cambios tecnológicos propios de la sociedad actual, -motorizados por la industria securitaria y militar- dificultan percibir la vigilancia y el control continuo al que estamos sometidos, sumado a la falta de una adecuada regulación y un debate en torno a los peligros que esto implica. Tal vez dicha situación responda al hecho de que habitualmente los avances técnicos -en este caso, en materia identificatoria- son presentados de manera positiva e, incluso, como imperiosos y necesarios, lo que imposibilita percibir ciertos riesgos que conllevan como la pérdida de la privacidad, la desprotección de los datos personales y la limitación de las libertades civiles.

Por otra parte, creemos que a partir de la modificación y profundización de la política documentaria/identificatoria se establece una relación asimétrica entre el Estado en su rol de recolector de datos y los individuos como proveedores de información, en la que el primero cuenta con una posición dominante capaz de quebrantar o avasallar el lugar más débil de este vínculo. Sin embargo, advertimos que en diversos momentos la ciudadanía no se compromete o no ejerce activamente la cultura cívica, ya que frente a la dicotomía entre la defensa de un derecho vulnerado y un beneficio inmediato, opta por este último.

El posicionamiento desigual en este vínculo puede convertir al Estado en un generador de políticas de exclusión, a partir de usos discrecionales de la información reunida en bases de datos, la utilización arbitraria de técnicas biométricas, la conformación de



prontuarios o perfilados sociales y la segmentación de categorías al interior del cuerpo social. Todas estas pueden considerarse como modernas formas de ejercer el derecho de muerte por parte de los Estados en el período del denominado biopoder, cuya técnica de gobierno se caracteriza por la administración, intervención y desarrollo de la vida humana.

Capítulo 1

Entre el período disciplinario y la era del control

1.1-El Estado como administrador del cuerpo social

Para dar cuenta de los cambios y transformaciones que sufrió el proceso documentario en la Argentina y analizar el Documento Nacional de Identidad como tecnología política creada por el Estado para registrar e identificar a la población, -sumada la incorporación de tecnología digital que permite la profundización de dichos objetivos-, partiremos de la noción de biopoder planteada por Michel Foucault (2006:15), definida como “el conjunto de mecanismos por medio de los cuales aquello que, en la especie humana, constituye sus rasgos biológicos fundamentales podrá ser parte de una política, una estrategia política, una estrategia general de poder”. En otras palabras, se trata de una técnica del gobierno de los hombres, entendidos y tratados a la vez como individuos (cuerpo-máquina) y como población (cuerpo-especie).

Por primera vez en la historia, la vida biológica ingresa en los cálculos del poder estatal, asumiendo el rol de administrador de la sociedad y garante del orden social a partir del control de los cuerpos y de la vida. Esto significa la entrada de los fenómenos propios de la vida humana en el campo de control del saber y de intervención del poder.

De esta manera, el Estado -concebido como lugar de codificación de las relaciones múltiples de poder y como conjunto de técnicas específicas de intervención en relación a otras tecnologías de gobierno- comienza a ejercer un poder sobre la vida; se trata de “un ejercicio del poder sobre el hombre en cuanto ser viviente, una especie de estatización de lo biológico o al menos una tendencia conducente a lo que podría denominarse la estatización de lo biológico” (Foucault, 2000:217).

Según el autor, a partir de los siglos XVII y principalmente XVIII comienza un período caracterizado por el crecimiento demográfico (dejando atrás las grandes pestes, epidemias y hambrunas), el desarrollo económico -fundamentalmente agrario-, el aumento de la productividad y los recursos naturales y un incipiente proceso de urbanización e industrialización, por lo cual los Estados toman a su cargo la función de administrar la vida y disponer de los cuerpos en tanto singularidades como multiplicidades. De este modo, se comienza a tomar en cuenta el hecho biológico

fundamental de que el hombre constituye una especie humana sobre la que se puede intervenir y en la que se empieza a aplicar ciertas tecnologías de poder.

1.2-Poder de vida y de muerte

En *Historia de la sexualidad I. La voluntad de saber*, Foucault (1992:163-164) sostiene que en el momento en que los Estados deciden comenzar a intervenir y administrar la vida, se produce el abandono de uno de los privilegios característicos del poder soberano de la época clásica que es el derecho de vida y de muerte. Este deriva de la *patria potestas* romana que otorga al padre de familia el derecho de disponer de la vida de sus hijos como la de sus esclavos; quien da la vida, también puede quitarla. Dicho derecho -por demás asimétrico- que tiene el rey o monarca reservado para sí, es el derecho a decidir sobre la vida y la muerte de los súbditos, pues, se consideran subsumidos al ámbito del poder político. De este modo, el soberano ejerce ese derecho de forma pasiva hacia la vida, dejando vivir, pero conduce activamente a la muerte, en la guerra o el suplicio. Por eso el autor concluye que ese derecho que se formula como de vida y de muerte es, en realidad, el derecho de hacer morir o de dejar vivir. Esta forma de dominación centralizada en la voluntad y la persona del soberano caracteriza a las denominadas sociedades de soberanía.

Ahora bien, en la modernidad ese derecho cambia radicalmente junto con los mecanismos de poder, entendiendo a éste como “la multiplicidad de las relaciones de fuerzas inmanentes y propias del dominio en que se ejercen, y que son constitutivas de su organización; el juego que por medio de luchas y enfrentamientos incesantes las transforma, las refuerza, las invierte” (1992:112). Ya no se trata de un derecho de captación de las cosas, del tiempo, los cuerpos y en, última instancia, de la vida sino que consiste en un poder que se ejerce positivamente sobre ésta, que procura administrarla, aumentarla, desarrollarla, multiplicarla y practicarle controles precisos y regulaciones generales. Dicho poder se convierte en un poder de hacer vivir o de rechazar hacia la muerte, una especie de contracara natural del antiguo poder soberano.

Pese a esto, el autor reflexiona que durante este período se llevan a cabo las guerras más sangrientas de los últimos siglos. Sin embargo, estas ya no se realizan en nombre del soberano sino del derecho a la existencia o en defensa de la población; es decir, se educa a las poblaciones para que se aniquilen mutuamente en nombre de la necesidad de vivir o de su derecho a la vida.

Para explicar este fenómeno, Foucault analiza a la raza como el dispositivo a través del cual el poder puede ejercer su derecho de muerte. Define al racismo como el modo de establecer una censura en un ámbito que se presenta como biológico para, en nombre de la supremacía o el mejoramiento de la especie, poder dar muerte. En el sistema del biopoder, el imperativo de la muerte es admisible sólo si se tiende a la eliminación del peligro biológico y al reforzamiento ligado con esta eliminación de la especie o de la raza. Según su análisis, el racismo moderno como cuestión de Estado y con base en la biología alcanza su forma paroxística en el nazismo.

En *Genealogía del racismo*, el autor sostiene que “el racismo asegura entonces la función de la muerte en la economía del biopoder, sobre el principio de que la muerte del otro equivale al reforzamiento biológico de sí mismo como miembro de una raza o una población, como elemento en una pluralidad coherente y viviente” (Foucault, 1996a:209). De esta manera, la guerra de razas es el modo en que el poder soberano puede ejercer positivamente su derecho de muerte en sociedades cuya principal técnica de gobierno es el poder de activar la vida.

Algunos autores centraron su análisis en los rasgos más negativos asumidos por el biopoder como el mencionado racismo biológico y de Estado. Ejemplos de ello son los planteos de los filósofos italianos Giorgio Agamben y Roberto Esposito; mientras que el primero lo denomina tanatopolítica, el segundo lo define como política inmunitaria.

Agamben desarrolla la idea de una política de muerte a partir de ciertos conceptos como estado de excepción, campo y vida nuda. Sostiene que la excepción es un fenómeno por el cual aquello que es excluido de la norma general no pierde relación con ella, sino que se mantiene relacionada en la forma de suspensión; por ello “el estado de excepción no es ni externo ni interno al ordenamiento jurídico, y el problema de su definición concierne precisamente a un umbral, o una zona de indiferenciación, en el cual dentro y fuera no se excluyen sino que se indeterminan” (Agamben, 2004:59). La particularidad de la modernidad, dice Agamben, es que el estado de excepción se convierte en regla.

La figura del campo se emplea para definir el espacio biopolítico más absoluto y terrorífico, donde la ley se suspende en forma integral, se priva a los individuos de toda condición política y se los reduce a ‘vida desnuda’. Así, se configura una zona de indistinción donde la protección jurídica y los derechos dejan de tener sentido. De esta manera, mediante un cuidadoso procedimiento biopolítico se produce un desgarro o censura al interior de lo social (y de lo individual) que determina que una vida no merece ser vivida ya que es algo menos que humano, lo que el autor define como ‘nuda

vida'. Son aquellas vidas meramente biológicas, esas vidas desnudas, simples vivientes que fueron despojados de sus formas naturales para, una vez así, gestionar sus muertes. La categoría de inmunidad en la obra de Esposito ilumina también el lado negativo de la biopolítica, ya que la caracteriza como una política de exclusión inclusiva, que incluye mediante una exclusión. Se necesita de la provocación de un otro para que la sociedad reaccione (y lo excluya) pero, a su vez, necesita de ese otro para constituirse y construir su identidad (inclusión). Según el autor, en la modernidad la apropiación de la vida por parte del poder se realiza mediante el paradigma inmunitario, para el cual la protección de la vida lleva implícita una política de muerte, “entendiendo con ello la expresión y también la tendencia cada vez más fuerte de proteger la vida de los riesgos implícitos en la relación entre los hombres, en detrimento de la extinción de los vínculos comunitarios (...) Así como para defenderse preventivamente del contagio se inyecta una porción de mal en los cuerpos que se pretende salvaguardar, también en la inmunización social la vida es custodiada en una forma que le niega su sentido más intensamente común” (Esposito, 2006:10).

1.3-Anatomopolíticas y biopolíticas

Como se mencionó anteriormente, de las referencias a la obra de Foucault puede advertirse que el poder sobre la vida se despliega mediante dos formas relacionadas entre sí. La primera, que comienza a desarrollarse en el siglo XVII, se centra en el cuerpo como máquina y apunta a un cuerpo individual convertido en un aparato productivo. Esto se logra mediante su educación, el aumento de sus aptitudes, el arrancamiento de sus fuerzas, el crecimiento paralelo de su utilidad y su docilidad, su integración en sistemas de controles eficaces y económicos. Todo esto queda asegurado mediante determinados procedimientos de poder: son anatomopolíticas del cuerpo humano.

En el texto “Los cuerpos dóciles”, Foucault (2008) analiza detalladamente este fenómeno y asegura que un cuerpo dócil es aquel que puede ser sometido, utilizado, transformado y perfeccionado. Esto se logra mediante una coerción constante e ininterrumpida, que vela sobre los procesos de la actividad y se ejerce mediante una relación imbricada entre el tiempo, el espacio y los movimientos. A estos métodos que permiten el control minucioso de las operaciones del cuerpo, que garantizan la sujeción constante de sus fuerzas y les imponen una relación de docilidad-utilidad, los denomina

disciplinas. El cuerpo humano entra así en un mecanismo de poder que lo explora, lo desarticula y lo recompone.

De este modo, esta mecánica de poder fabrica cuerpos dóciles, sometidos y ejercitados, ya que aumenta las fuerzas del cuerpo -en términos económicos de utilidad- y las disminuye -en términos políticos de obediencia-. Estas técnicas minuciosas, ínfimas y detallistas conforman lo que Foucault denomina una microfísica del poder; una anatomía política del detalle.

Esta cuestión de las técnicas de control disciplinario de los cuerpos es analizada extensamente en el texto “El panoptismo” (2008). Allí parte de una figura arquitectónica diseñada por el inglés Jeremy Bentham (1748-1832), el panóptico (pan: todo, totalidad - opsis, óptico: vista, ver), que posee una forma de anillo dividido en pequeñas celdas y cuenta con una torre central con anchas ventanas que abren hacia el interior del anillo desde la cual se puede observar hacia los cuartos pero no así en sentido inverso. Basta colocar a un vigilante y encerrar en cada celda a un individuo para que, ante el efecto de visibilidad constante y vigilancia permanente, los hombres interioricen las conductas esperables y se garantice su pasividad y control de sus movimientos. “De ahí el efecto mayor del Panóptico: inducir en el detenido un estado conciente y permanente de visibilidad que garantiza el funcionamiento automático del poder. Hacer que la vigilancia sea permanente en sus efectos, incluso si es discontinua en su acción” (2008:233), explica el autor.

Esta estructura, que persigue el adiestramiento minucioso y concreto de las fuerzas útiles, se encuentra en la base de la mayoría de las instituciones de encierro como ser la prisión, la escuela, el cuartel, el hospital o el taller. Poco importa quien es el sujeto o el objeto de la mirada; la garantía de su posible existencia alcanza para poner en marcha el engranaje de la relación dominante-dominado. Por eso, el intelectual francés asegura que “el esquema panóptico es un intensificador para cualquier aparato de poder: garantiza su economía (en material, en tiempo); garantiza su eficacia por su carácter preventivo, su funcionamiento continuo y sus mecanismos automáticos” (2008:238).

Por otra parte, Foucault destaca el doble efecto que produce la vigilancia permanente e ininterrumpida sobre los individuos. Aquel que vigila ejerce sobre los sujetos un poder en dos sentidos, ya que “tiene la posibilidad no sólo de vigilar sino también de construir un saber sobre aquellos a quienes vigila” (1996b:91). Consiste en un saber de vigilancia y de examen, organizado alrededor de la norma por el control de los individuos durante toda su existencia. Esta es la forma del saber-poder; se trata de una red de relaciones en

las que está implicada una forma determinada de ejercicio del poder y de configuración del saber que hacen posibles determinados efectos de verdad y realidad, asegura el autor.

Las instituciones de encierro apuntan a disciplinar los cuerpos individuales que interiorizan la vigilancia mediante castigos normalizadores, además de caracterizarse por el ordenamiento racional del tiempo y la distribución de los cuerpos en el espacio. A esto se suman los saberes que se obtienen de aquellos cuerpos mediante métodos clásicos como la observación, la confesión y el examen, lo que permite un mayor control logrando la docilización de los cuerpos y la domesticación de las almas.

Así, el poder disciplinario es concebido como “una cierta forma capilar, una modalidad mediante la cual el poder político y los poderes en general logran, en última instancia, tocar los cuerpos, aferrarse a ellos, tomar en cuenta los gestos, los comportamientos, los hábitos, las palabras; la manera, en síntesis, como todos esos poderes, al concentrarse en el descenso hacia los propios cuerpos y tocarlos, trabajan, modifican y dirigen (...) las fibras blandas del cerebro” (Foucault, 2005:59). Basada en el esquema panóptico - principio general de una anatomía política que tiene la capacidad de difundirse a todo el cuerpo social y a definir las relaciones de poder en la vida cotidiana de los hombres-, se caracteriza la formación de las denominadas sociedades disciplinarias.

El segundo polo del poder sobre la vida que permite el desarrollo del biopoder se despliega hacia mediados del siglo XVIII y se centra en el cuerpo concebido como especie, aquel cuerpo atravesado por la mecánica de lo viviente y que sirve de soporte a los procesos biológicos: los nacimientos, la mortandad, la proliferación, el nivel de salud, la duración de la vida y la longevidad, acompañado de todas las condiciones que puedan hacerlo variar, a través de una serie de intervenciones y controles reguladores. En otras palabras, se trata de la manera en que se agrupa y estudia, desde la práctica gubernamental, los fenómenos propios de un conjunto de seres vivos organizados. Consiste en la gestión de los procesos biológicos, una forma de poder que se ocupa de los fenómenos de masa, es una biopolítica de la población.

En *Las grietas del control. Vida, vigilancia y caos*, Esther Díaz da cuenta de este mismo fenómeno y del cambio en las formas de poder: “En el pasaje del siglo XVII al XVIII se dieron dos formas antitéticas de poder sobre los cuerpos. Por un lado, se desarrolló una anatomía política mediante el ejercicio de disciplinas ejercidas sobre cada cuerpo individual, a través de una vigilancia panóptica y microfísica sobre las conductas de los sujetos. El cuerpo se concebía como máquina. Y, por otro, se fue

extendiendo el control de lo individual a lo poblacional. En el primer caso, el anatomopoder vigilaba las posturas, la dedicación a las tareas, la disposición de los cuerpos en el espacio, las pautas en el uso del tiempo, las conductas públicas y privadas, las aspiraciones y deseos (...) En el segundo caso, al avanzar sobre la regulación de la vida, la biopolítica comenzó a preocuparse por las tasas de nacimiento, los índices de mortalidad, las condiciones de lactancia, el cuidado de la salud, la extensión de los ciclos vitales” (2010:103-104).

El dispositivo para convertir a los pueblos en población forma un conglomerado de ciencias humanas, entre las que se destacan la estadística, la demografía, la medicina, la sociología, el trabajo social, la biología, entre otras. Estas se ocupan de distintos fenómenos sociales tales como la proporción de nacimientos y decesos, la tasa de reproducción, la densidad demográfica, las enfermedades, la higiene pública, la vejez, la vivienda, la migración, los seguros, la jubilación, las relaciones con el urbanismo y los efectos del ambiente en general.

En este contexto cabe destacar el surgimiento del proceso documentario como una gran tecnología biopolítica mediante la cual se transforma al individuo en ciudadano, y, a su vez, el Documento Nacional de Identidad -objeto de análisis del presente trabajo-, como el principal dispositivo de identificación de la sociedad disciplinaria argentina. Ambos serán desarrollados extensamente más adelante.

A partir de lo planteado se evidencia que el biopoder caracteriza a un poder cuya función más alta es la de invadir la vida por completo y apunta a la administración de los cuerpos y la gestión calculadora de la vida. Además, tal como asegura Foucault, el biopoder fue un elemento indispensable en el desarrollo del capitalismo, ya que se sirvió de numerosas técnicas para la inserción de los cuerpos en el aparato de producción y el ajuste de los fenómenos de población a los procesos económicos.

1.4-De la sociedad disciplinaria a la sociedad de control

Las sociedades disciplinarias -cuya forma de dominación social se construye a través de una red de dispositivos y aparatos que producen y regulan las costumbres, los hábitos y las prácticas productivas- tienen su punto cúlmine (en el doble sentido del término) en la primera mitad del siglo XX con el modelo fordista de producción industrial y el Estado de Bienestar como modelo político (pleno empleo, implementación de programas sociales, intervención estatal en la economía, solidaridad sistemática, etc.).

A medida que avanza el siglo XX, estas formas sociales comienzan a mutar, produciéndose una transformación en las tecnologías del poder y una crisis de los lugares de encierro y su mecánica disciplinaria, lo que permite vislumbrar una transición sociohistórica hacia lo que Gilles Deleuze (1999) denomina sociedades de control.

En su texto “Posdata sobre las sociedades de control”, el autor sostiene que éste toma nuevas formas a través de redes flexibles y fluctuantes; ya no se circunscribe a espacios cerrados porque ahora la vigilancia no requiere de instituciones sociales y se relaciona más con las nuevas tecnologías. Además, los mecanismos tienden a diversificarse y el control se vuelve continuo e ilimitado, sirviéndose de la comunicación instantánea y la informatización, donde el marketing y la publicidad funcionan como instrumentos normalizadores.

El autor explica que los encierros son moldes -pretenden que el sujeto sea una masa inerte dispuesta a adquirir forma-, mientras que los controles son modulaciones -una suerte de molde que va cambiando de forma y va dando a la sustancia nuevas configuraciones variables-. Por eso, las prácticas de gestión de este período ya no consisten en encerrar y programar la multiplicidad sino que apuntan a las subjetividades modulando sus actuaciones en el espacio abierto. El sociólogo italiano Maurizio Lazzarato en *Políticas del acontecimiento* afirma que “si las disciplinas moldeaban los cuerpos constituyendo hábitos principalmente en la memoria corporal, las sociedades de control modulan los cerebros y constituyen hábitos principalmente en la memoria espiritual” (2006:100).

Por otra parte, Deleuze asegura que al cambiar las formas de control se producen modificaciones en el espacio laboral, la educación y el entretenimiento: la fábrica es reemplazada por la empresa; mientras en la primera se contiene a los trabajadores, en la otra se introduce el condimento de la rivalidad por medio de la competencia como motivación, que opone a los individuos entre ellos y atraviesa a cada uno. Además, se pasa de una economía de bienes basada en productos tangibles a una economía de servicios. En cuanto al aprendizaje, la formación permanente tiende a sustituir a la institución educativa, y la evaluación continua al examen. Por su parte, los medios de comunicación y los sistemas digitales de información son los dispositivos que organizan los tiempos de ocio, conformando nuevos hábitos y prácticas de consumo. En relación a esto, Michael Hardt y Antonio Negri en *Imperio* sostienen que “el poder se ejerce ahora a través de máquinas que organizan directamente los cerebros (en los sistemas de

comunicación, las redes de información, etcétera) y los cuerpos (en los sistemas de asistencia social, las actividades controladas, etcétera) con el propósito de llevarlos hacia un estado autónomo de alienación, de enajenación del sentido de la vida y del deseo de la creatividad” (2002:36).

Al igual que las tecnologías de poder que caracterizan a este período, todo parece haberse vuelto intangible: cifras, contraseñas, ordenadores, virus, datos, mercados, servicios, acciones, etc. El lenguaje numérico del control marca el acceso a la información o lo rechaza; los individuos se convierten en ‘dividuos’ y las masas en muestras, mercados o bancos. Según Hardt y Negri, “la maquinaria del poder invade el conjunto del cuerpo social que se desarrolla en su virtualidad. Esta relación es abierta, cualitativa y afectiva. La sociedad, absorbida dentro de un poder que se extiende hasta los ganglios de la estructura social y sus procesos de desarrollo, reacciona como un solo cuerpo. El poder se expresa pues como un control que se hunde en las profundidades de la conciencia y los cuerpos de la población y, al mismo tiempo, penetra en la totalidad de las relaciones sociales” (2002:37).

Como el control no necesita de la modalidad del encierro como ocurre con la disciplina, la clásica representación del poder -basada en la arquitectura de un modelo panóptico unidireccional, jerárquico y centrado en una posición fija- ya no sirve para explicar la forma en que se ejerce la vigilancia en estos tiempos. Atrás quedaron los viejos esquemas que sostienen la idea de mantener a los individuos fijados y aislados bajo inspección y examen mediante la coerción, propios de las sociedades industriales. Ahora, las nuevas tecnologías posibilitan mecanismos y prácticas de seguridad ubicuas, descentralizadas, multidireccionales y potentes que ofrecen opciones de vigilancia omnisciente, real y efectiva, posibilitando un entramado muy diferente del poder.

Los actuales dispositivos, entendidos como “un régimen social productor de subjetividades, es decir, productor de sujetos-sujetados a un orden del discurso cuya estructura sostiene un régimen de verdad (...) Si bien cada dispositivo tiene una función específica, conforman entre todos una ‘red de poder-saber’ que los articula, los complementa y los potencia mutuamente, también dicha red contiene contradicciones porque no todos los individuos circulan sistemática y uniformemente por la red de poder-saber, y porque cada dispositivo porta una especificidad en cuanto al tipo de sujeto que pretende producir”¹, no reemplazan a los antiguos mecanismos disciplinarios

¹ García Fanlo, Luis (2011, marzo). ¿Qué es un dispositivo?: Foucault, Deleuze, Agamben. *Parte Rei Revista de Filosofía*, 74, p.7.

y jurídico-legales (soberanos) sino que los subsumen, complementan o reactualizan, configurando una red de poder con nuevas y múltiples herramientas.

Casi paradójicamente, en esta etapa de nueva y reconfigurada vigilancia el concepto de libertad es clave. Esto se debe a que el control no opera por encierro sino que implica de medios abiertos que presuponen la libertad de los individuos a controlar. Foucault asegura que las nuevas formas de gobernar se caracterizan por “mecanismos cuya función consiste en producir, insuflar, incrementar las libertades, introducir un plus de libertad mediante un plus de control e intervención. Es decir que en este caso el control ya no se limita a ser, como en el caso del panoptismo, el contrapeso necesario a la libertad. Es su principio motor” (Foucault, 2007:89).

Por otra parte, en *Seguridad, territorio, población* (2006:66-71) el autor francés diferencia el carácter centrípeto de la disciplina que funciona en la circunscripción de un espacio y así concentra y encierra, de la forma centrífuga de los dispositivos de seguridad que incorporan nuevos elementos abriendo el espacio a una circulación intensiva. A su vez, la disciplina utiliza el reglamento como herramienta primordial, sanciona el detalle y no deja nada librado al azar; mientras que la seguridad establece holgados niveles de permisividad y posibilita un ‘dejar hacer’.

Según Foucault, estos dispositivos de seguridad se vinculan con una forma de concebir y ejecutar políticas de gobierno de las poblaciones que se corresponde con el liberalismo, que consiste en el uso técnico de la libertad como condición para el desarrollo de las formas modernas o capitalistas de economía.

En este contexto, los dispositivos vigilantes -algunos reconfigurados al entrelazarse con el desarrollo de tecnologías informáticas- invaden los espacios por los que circulan y se relacionan los sujetos sociales y promueven formas de control más sofisticadas e insidiosas, dando lugar a lo que Armand Mattelart denomina *Un mundo vigilado* (2009). En paralelo, Foucault sostiene que “la libertad no es otra cosa que el correlato de la introducción de los dispositivos de seguridad. Un dispositivo de seguridad (...) sólo puede funcionar bien con la condición de que se dé algo que es justamente la libertad, en el sentido moderno (...) de la posibilidad de movimiento, desplazamiento, proceso de circulación de la gente y las cosas. Y es esa libertad de circulación en el sentido amplio de la expresión, esa facultad de circulación, lo que es menester entender, creo, cuando se habla de libertad, y comprender como una de las facetas, uno de los aspectos, una de las dimensiones de la introducción de los dispositivos de seguridad” (2006:71).

1.5-Matices de la sociedad de control

Una nueva racionalidad biopolítica parece gobernar y caracterizar a las sociedades contemporáneas que se corresponden con el ascenso del neoliberalismo y se asocian a la crisis del modelo fordista y a la emergencia de un capitalista financiero, especular y de consumo. En consonancia a esto, el ahora caduco Estado de Bienestar ya no planifica, refuerza ni ejecuta la vida; su tarea no es crear trabajadores sino incitar a los consumidores y gestionar a una reducida población, una reserva de vida biológica. Esto es lo que Esteban Rodríguez define como Estado de Malestar: “Es la forma que asume el Estado durante el neoliberalismo, etapa superior del capitalismo. Lo llamamos Estado de Malestar por oposición al Estado de Bienestar. Si este último tenía por objeto la vida, el sostenimiento de la vida que el capital productivo necesitaba para continuar valorizándose; el Estado de Malestar se concentrará sobre la muerte, es decir sobre la vida de la que ha prescindido el capital cuando éste se ha reconstituido desde la especulación. Su objetivo no será la vida sino la muerte. Un Estado que se ha ido descomprometiendo (desregulando, ajustando, privatizando) de un cierto número de problemas que hasta ahora (hasta el desmantelamiento del Estado Social), constituía su razón de ser, su fundamento. El Estado de Malestar es, para las clases populares, ya no la administración de la vida sino la administración de la muerte: el pasaje de una biopolítica a una tanatopolítica. Gestionar la muerte es gestionar la vida que no vale casi nada, que el capital (ahora financiero y especulador) ya no necesita para valorizarse”².

Todas estas transformaciones dan lugar al mencionado pasaje de un modelo de inclusión por disciplina bajo la mirada de los cuerpos a un modelo de exclusión por vigilancia y control a distancia. Este cambio conforma una nueva matriz técnico-social basada en la comunicación y sistemas digitales de información, con los cuales se desdibuja la frontera entre lo público y lo privado. Así, los antiguos dispositivos disciplinarios se digitalizan al mismo tiempo que surgen otros nuevos basados en tecnologías de control y de seguridad que ya no operan sobre individuos encerrados institucionalmente sino, como se dijo, sobre el conjunto de la población que circula en espacios abiertos.

Con algunos matices, diversos autores plantean esta misma transición de etapas. El ensayista Zygmunt Bauman describe la mencionada mutación de formas sociales como un pasaje de una modernidad pesada o primera modernidad hacia la modernidad líquida

² Rodríguez, Esteban (s.f). Galpones y patrones de estancia. *Revista Lote*, 94. Recuperado el 12 de junio de 2015, de <http://www.revistalote.com.ar/nro094/patrones.htm>.

o pospanóptica. A su vez, contrapone el poder panóptico en el que unos pocos controlan y vigilan a muchos -característico de la etapa anterior-, con el actual poder sinóptico, término acuñado por el sociólogo noruego Thomas Mathiesen, en el que muchos vigilan y controlan a pocos, siendo el objeto de ese control ya no los asuntos públicos sino la vida privada del vigilado. Según el autor, esta red que conforma los actuales dispositivos representa la matriz social a través de la cual se procesan los nuevos sujetos consumidores de las sociedades contemporáneas.

Bauman asegura que el mecanismo de poder del sinóptico se desespacializa y ya no funciona mediante la vigilancia sino mediante la seducción, la cual lleva a adquirir determinadas formas de comportamiento y a fomentar ciertas imágenes en consonancia con las sociedades de mercado en las que el principal objetivo es el consumo.

En este contexto, los consumidores interiorizan nuevos hábitos y conductas del mercado, ya que predomina una concepción del deseo como placer inmediato. Así, el sinóptico resulta un potente mecanismo regulador de la subjetividad de la masa, concebida como la suma de individuos individualizados. En relación a esto, el filósofo Peter Sloterdijk sostiene que “en lo esencial, las masas actuales han dejado de ser masas capaces de reunirse en tumultos; han entrado en un régimen en el que su propiedad de masa ya no se expresa de manera adecuada en la asamblea física, sino en la participación en programas relacionados con medios de comunicación masivos. De la masa tumultuosa hemos pasado a una masa involucrada en programas generales. En ella uno es masa en tanto individuo. Ahora se es masa sin ver a los otros. El resultado de todo ello es que las sociedades actuales o, si se prefiere, posmodernas han dejado de orientarse a sí mismas de manera inmediata por experiencias corporales: sólo se perciben a sí mismas a través de símbolos mediáticos de masas, discursos, modas, programas y personalidades famosas. Es en este punto donde el individualismo de masas propio de nuestra época tiene su fundamento sistémico” (2002:17).

El sinóptico que, gracias a la tecnología de los medios de comunicación, permite que muchos sean capaces de mirar a unos pocos -el centro de atención- los cuales imponen ciertas normas sociales de comportamiento y constituyen un modelo de realidad basado en el éxito, funciona como mecanismo de control que posibilita a los sujetos aceptar e incorporar determinadas relaciones de poder. En *Vigilancia líquida*, escrito en coautoría con David Lyon, Bauman explica que “nuestra actual vigilancia por parte del mercado asume que la manipulación del gusto (a través de la seducción, y no la coerción) es la vía más segura para llevar a los individuos a la demanda. La voluntad, ni

siquiera entusiasta, y la cooperación de los manipulados es el principal recurso empleado por los sistemas sinópticos de marketing” (2013:140).

Por otra parte, ya en la década del 80 el teórico de la vigilancia Gary Marx plantea la tesis del advenimiento del control total de la población, que se refleja en la tecnología informática y en los distintos sistemas de vigilancia implementados, dando lugar al surgimiento del panóptico electrónico. Esto supera las formas tradicionales de control ya que la nueva metodología trasciende la distancia y el tiempo, haciéndola cada vez más efectiva pero de modos sutiles y casi imperceptibles. Los avances tecnológicos posibilitan que “los ordenadores modifi[quen] cualitativamente la naturaleza de la vigilancia, haciéndola rutinaria, ampliándola y profundizándola” (1988:208).

En este marco, Roy Boyne denomina postpanoptismo al conjunto de categorías analíticas que defienden la necesidad de abandonar la figura del panóptico tradicional debido a que no se ajustan a las circunstancias socioculturales actuales³. En consonancia, Mark Poster indica la noción de superpanóptico para dar cuenta de la analizada tecnología de poder que se extendió electrónicamente a finales del siglo XX. La población es supervisada y observada de manera silenciosa y automática, a la vez que proporciona voluntariamente su información personal que se almacena en bases de datos. Además de la consecuente indistinción entre lo público y lo privado, esto lleva a la multiplicación del individuo y a la creación de sujetos inmovilizados informáticamente; se trata de otros ‘yos’ de cada individuo que puede ser “tan efectivo socialmente como el yo que camina en la calle” (1995:232).

Por su parte, William Bogard denomina sociedades del hipercontrol a aquellas que operan mediante términos predictivos y de actuación previa al hecho. Esta nueva lógica de control maximizado excede los instrumentos espaciales y temporales propios del tipo de sociedad disciplinaria y apunta a estrategias reguladoras preventivas⁴ (2009: 173).

Esta caracterización de la sociedad de vigilancia de Bogard plantea nuevas lógicas e inaugura la era de la sospecha, en donde todos los individuos se convierten en potenciales delincuentes a los que hay que observar, controlar y tener bajo mirada muy de cerca. En consonancia, el psicoanalista Gérard Wajcman, en su libro *El ojo absoluto* sostiene que “si el enemigo está entre nosotros, si está en nosotros, esto conduce a esa suerte de generalización democrática de la ideología securitaria consistente en poner a

³ Castro Orellana, Rodrigo (2009). La ciudad apestanda. Neoliberalismo y postpanoptismo. *Revista de Ciencia Política*, 1 (29).

⁴ Id.

todo el mundo igualitariamente bajo vigilancia. La sociedad misma se pone bajo vigilancia, se vigila y se combate a sí misma” (2011:91).

De este modo, la estrategia moderna de vigilar y castigar se sustituye por la de vigilar y prevenir, ya que toda la población es virtualmente peligrosa. Con tecnología altamente sofisticada a su servicio, en este nuevo período parece dominar el imperativo de la previdencia. “Los inocentes son criminales futuros, criminales provisoriamente inocentes. Culpables potenciales o no conocidos como tales (...) es la generalización de la vigilancia la que engendra sospecha generalizada (...) Al colocar a la sociedad entera bajo la mirada, al arrojar así sobre todos la presunción de culpabilidad, ella borra la frontera entre culpables e inocentes” (2001:92-97), apunta Wajcman.

Es así como los diversificados mecanismos basados en el desarrollo tecnológico o “la camisa de fuerza tecnológica que los Estados pusieron en los individuos”⁵, en términos del teórico cultural Paul Virilio (2010), posibilita una multiplicidad de formas de vigilancia y control hacia todas las direcciones, que penetra en las diversas capas del entramado social y configura nuevos modos de comportamiento.

Teniendo en cuenta el panorama trazado, en los capítulos siguientes analizaremos la incorporación de tecnología digital en el Documento Nacional de Identidad, un emblemático dispositivo disciplinario transformado y reconfigurado en la era de la sociedad de control, que mediante un método automático de reconocimiento de individuos basado en características biológicas y de comportamiento, profundiza el control y posibilita la construcción de una gran base de datos estatal que permite rastrear y monitorear a todos los ciudadanos.

⁵ Febbro, Eduardo (2010, noviembre 20). Siempre se infunde miedo en nombre del bien. Diálogo con el intelectual francés Paul Virilio. *Página 12*, p.1.

Capítulo 2

Genealogía del proceso documentario

2.1- Pioneros en identificación dactilar

La identificación en la Argentina es responsabilidad del Estado nacional (Ministerio del Interior y Transporte y Registro Nacional de las Personas) pero históricamente no estuvo organizado de esta manera. Durante más de tres siglos, el registro de la identidad de los habitantes del país dependió de la Iglesia Católica que asentaba los bautismos y matrimonios en los libros parroquiales, únicos datos de la vida de la población.

La Revolución de Mayo de 1810 marca un hito en la historia, a partir del cual comienza a discutirse y cuestionarse la relación entre la esfera eclesiástica, la política y la sociedad civil. Recién en 1857 el Estado empieza a tener un papel relevante en materia identificatoria cuando Valentín Alsina, gobernador de la provincia de Buenos Aires, firma el Decreto N° 1740 donde se establece las normas para controlar el registro de los ciudadanos, entre las cuales se destaca la obligatoriedad de las iglesias de realizar una copia de sus archivos -denominado Libro Gemelar-, para ser entregado a los municipios y a las guarniciones militares.

Estas normas impuestas tienen vigor desde su sanción hasta que, en 1884 bajo la presidencia de Julio Argentino Roca, se dicta la Ley N° 1.565 que establece la creación del Registro Civil de la Capital de la República Argentina y Territorios Nacionales, donde se reglamenta el registro de nacimientos, matrimonios, defunciones y procedimientos de las inhumaciones. Este cambio pone fin a la primacía del poder eclesiástico en el registro poblacional y marca el inicio del proceso documentario bajo la tutela y el control del Estado nación.

Hacia fines del siglo XIX, bajo el lema “gobernar es poblar”, se produce en el país el arribo de millones de extranjeros que genera una radical transformación de la estructura social y de las relaciones de poder. Con intención homogeneizadora y con voluntad de garantizar el orden social, el Estado comienza a idear dispositivos de identificación y control de sus habitantes a fin de reprimir ciertas formas de criminalidad y protesta impulsadas por ideas anarquistas traídas por inmigrantes provenientes de Europa, que ponían en riesgo la privilegiada posición de la elite.

Durante este período se destacan dos disposiciones que corresponden a la sanción de la Ley N° 4.144, conocida como Ley de Residencia de 1902, que habilita al gobierno

argentino a expulsar del país a cualquier extranjero sin juicio previo, y la resolución de extender el proyecto de registros de huellas digitales a los inmigrantes.

Este sistema de identificación dactiloscópico ideado por el jefe de estadísticas de la policía de la ciudad de La Plata, Juan Vucetich, comienza a utilizarse en el país en 1891 para identificar a los delincuentes y finalmente se amplía a todos los habitantes. Dicho procedimiento se basa en la impresión de los dibujos formados en las yemas de los dedos que genera una marca individual de cada persona y reemplaza al procedimiento antropométrico, primer sistema de fichas descriptivas adoptado durante 30 años como prueba judicial en los procesos de investigación de orden criminal.

El antiguo sistema de identificación, implementado por Alphonse Bertillon, se basaba en la medición de las principales partes del cuerpo (medidas generales del cuerpo -talla, busto y aberturas de brazos-, extremidades y longitud del cráneo) pero no contempla diferencias en las medidas óseas afectadas por enfermedad, no registra a menores de 20 años -por cambios físicos de crecimiento-, ni a las mujeres. Frente a las deficiencias que muestra este método, el jefe de estadísticas decide llevar a la práctica los estudios de Francis Galton, antropólogo inglés quien establece las tres leyes fundamentales de la dactiloscopia: perennidad, inmutabilidad y diversidad infinita en cada persona. “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”, tal como indica Gabriel Anitua en su artículo ““¡Identifíquese!’. Apuntes para una historia del control de las poblaciones” (2005:16).

Finalmente en 1906 se implementa la utilización de la Cédula de Identificación⁶ expedida por la Policía Federal, en la que además de figurar los datos biográficos (lugar de domicilio, estado civil, fecha de nacimiento, sexo y nacionalidad de origen), la fotografía y la firma, se utiliza por primera vez las huellas dactilares como instrumento de identificación en el registro documentario. Hasta ese momento, los únicos instrumentos que certificaban la existencia de una persona son la partida de nacimiento (otorgada por los registros civiles de cada jurisdicción) o el certificado de bautismo (emitido por la Iglesia).

Si bien en un período inicial algunos sectores de la población se resisten al sistema, luego de una insistente campaña pública que destaca las facilidades que ofrece al ciudadano poder identificarse y no ser confundido con aquellos combativos que defendían sus ideales por medio de la acción directa, comenzaron a aceptarlo. Tal fue el

⁶ Documento que tiene vigencia hasta el 1 de marzo de 2011 (ver apartado Nuevo DNI).

éxito de esta medida que, con los años, la portación de documentación para salir a la calle se convirtió en un auténtico hábito. “En esos ámbitos resuenan los discursos sobre ‘defensa social que supone un enemigo’. La figura emblemática es el emigrante procedente de Europa. No el que vive de un trabajo honrado”, describe Mattelart en su libro *Un mundo vigilado* (2009:32).

2.2-Antecedentes de registro de identificación

Camino a la ley electoral Roque Sáenz Peña de 1912 que establece el voto “secreto, individual y obligatorio”, en 1911 se sanciona la Ley N° 8.129 que dispone que los ciudadanos de sexo masculino al cumplir los 18 años debían enrolarse a los efectos de cumplir con el servicio militar obligatorio.

Las autoridades militares encargadas de esta tarea utilizan los datos de los registros civiles para confeccionar el patrón electoral de las elecciones presidenciales a realizarse en 1916, creándose así el archivo dactiloscópico tras decretar que en las cartas de ciudadanía debía figurar la impresión del dígito pulgar derecho. Este hecho resulta un antecedente de la Ley N° 11.386 de 1926 que reglamenta, durante la presidencia Marcelo T. de Alvear, la Libreta de Enrolamiento como documento de identificación personal para el sexo masculino en la que se registra, al igual que en la Cédula de Identidad, las huellas digitales y la fotografía para certificar su autenticidad. De esta manera, la Libreta cumple con tres funciones: de identidad, certificado del cumplimiento del servicio militar obligatorio e instrumento habilitante para emitir el sufragio.

Si bien en 1911 el diputado socialista Alfredo Palacio había presentado el primer proyecto de ley para el voto femenino, pasaron más de treinta años para que las mujeres, al cumplir la mayoría de edad, recibieran la Libreta Cívica. Así, con la sanción de la Ley N° 13.010 de los Derechos Políticos de la Mujer de 1947, las ciudadanas argentinas contaron con el instrumento legal que les permitía elegir y ser elegidas. Este documento habilitante para emitir el voto fue impulsado por Eva Duarte y establece el sufragio universal durante el primer gobierno de Juan Domingo Perón.

Al año siguiente, mediante la Ley N° 13.482⁷ se crea el Registro Nacional de las Personas (Renaper), “organismo nacional que tiene por cometido realizar el registro e identificación de todas las personas físicas que se domicilien en el territorio argentino o en jurisdicción argentina y de todos los argentinos cualquiera sea el lugar de su

⁷ Modificado por la Ley N° 17.671.

domicilio, llevando un registro permanente y actualizado de los antecedentes de mayor importancia, desde su nacimiento y a través de las distintas etapas de su vida”⁸, dependiente del Ministerio del Interior. Además de cumplir con la tarea de inscribir a las personas, otorga un número de matrícula y expide la Libreta Nacional de Identidad, el Certificado Nacional o la Condicional de Identidad y el Pasaporte Nacional (documento internacional de viaje que acredita una autorización legal para que el individuo ingrese o egrese del país).

2.3-Documento Nacional de Identidad

En 1968, los distintos tipos de identificaciones que existen en el país son reemplazados por el Documento Nacional de Identidad (DNI), cuyo formato y uso es reglamentado por la Ley N° 17.671⁹ de Identificación, Registro y Clasificación del Potencial Humano Nacional sancionada por el presidente de facto Juan Carlos Onganía, la cual se mantiene vigente en la actualidad.

A partir de esa normativa se establece que el Renaper (creado en 1948, como se indicó anteriormente) -organismo autárquico y descentralizado con dependencia del Ministerio del Interior- es el responsable del registro y el encargado de la emisión del DNI en todo el territorio nacional.

Para la confección de dicho registro se consideran los mismos datos que en los anteriores tipos de documentos: partida de nacimiento (emitida por el registro civil), fotografía carnet y se toma las impresiones digitales de los dedos que se incluyen en el legajo de identificación, tal como se indica en el artículo 7 de dicha disposición: “Las constancias del legajo de identificación deberán puntualizar con precisión los comprobantes que las justifiquen. En la sede central del Registro Nacional de las Personas se llevarán por lo menos ficheros patronímicos, numéricos y dactiloscópicos según el sistema argentino Vucetich u otro que en el futuro aconseje la evolución de la técnica”¹⁰. Así, se otorga un número en el DNI que certifica la inscripción y se mantiene inmutable durante toda la vida.

⁸ Argentina. Ministerio del Interior y Transporte. Recuperado el 12 de marzo de 2015, de <http://www.mininterior.gov.ar/renaper/renaper.php>

⁹ La Ley N° 17.671 sufrió más de 100 modificaciones, entre las que se destacan los siguientes cambios y complementos: Ley N° 20.078/73, 20.509/73, 20.974/75, 21.807/78, 22.435/81, 24.569/95, 24.961/98, 24.810/97 y 24.961/98.

¹⁰ Ley N° 17.671 de Identificación, Registro y Clasificación del Potencial Humano Nacional. Boletín Oficial, Buenos Aires, Argentina, 29 de febrero de 1968.

La jurisprudencia determina que deben efectuarse tres actualizaciones obligatorias o, de lo contrario, el ciudadano es sancionado con una multa: la primera al llegar a la edad escolar (6 años) hasta los 8, la segunda a los 14 y la última a los 30 años de edad, en las cuales se actualiza tanto la fotografía como las impresiones de los dedos. De esta manera, el Estado mantiene un seguimiento en la identificación de los miembros de la población en cada etapa de la vida con sus correspondientes cambios corporales y biológicos significativos.

Esta normativa determina la responsabilidad del ciudadano en mantener actualizados sus datos ante el organismo responsable por considerarlo el único registro válido para identificar a la persona, tal como se establece en el artículo 13. “La presentación del documento nacional de identidad expedido por el Registro Nacional de las Personas será obligatoria en todas las circunstancias en que sea necesario probar la identidad de las personas comprendidas en esta ley, sin que pueda ser suplido por ningún otro documento de identidad cualquiera fuere su naturaleza y origen”¹¹, siendo la acreditación autorizada para emitir el sufragio a partir de los 18 años.

2.4-Rastros de un sistema obsoleto

Durante los años siguientes crece la población y el sistema manual en la confección de documentos se vuelve obsoleto, lo que genera importantes complicaciones a la hora de tramitar el DNI o realizar sus actualizaciones, transformándose en tareas casi imposible: filas interminables, trámites engorrosos, papeles extraviados y esperas de hasta dos años para finalmente recibir una libreta hecha a mano.

En el proceso de expedición y confección interviene tanto el Estado nacional, a través del Renaper, como los Estados provinciales con los registros civiles. El trámite comienza en estas oficinas locales y los formularios se envían a la ciudad capital de la provincia para ser remitidos a la sede central del Registro Nacional de las Personas, ubicada en la Ciudad Autónoma de Buenos Aires, para su confección; recorriendo el mismo circuito de vuelta para la entrega.

Frente a estos inconvenientes, se instalan nuevas oficinas de registro civil pero esta implementación sólo genera mayores complicaciones porque aumentan los trámites que ingresan sin solucionar la precariedad del sistema.

En los años 90, acorde al modelo socioeconómico imperante, se plantea que la solución viene del exterior. De este modo, durante el gobierno de Carlos Menem y mediante el

¹¹ Id.

Decreto N° 1.310/1994, se lanza una licitación pública nacional e internacional para la contratación de un Sistema de Control Migratorio, de Identificación de las Personas y de Información Eleccionaria, “con la finalidad de dotar al Estado de un sistema confiable y eficaz de acopio, control, fiscalización y sistematización de información, que refleje el potencial humano que desarrolla sus actividades en el territorio nacional”, mediante la incorporación de las innovaciones tecnológicas y herramientas informáticas que permitan la “implementación de un sistema eficiente y seguro que sea una solución integral para el manejo de la información migratoria y de identificación de personas” (Villarruel, 2011:69), según se establece en la normativa. Seis son las compañías que adquieren el pliego de la licitación por un valor de 80.000 pesos, siendo Siemens It Service S.A. la empresa a la que se le adjudica el contrato.

A poco de terminar el mandato presidencial, en 1998 se firma el acuerdo entre autoridades de la empresa alemana y el Estado nacional (representado por el entonces ministro de Interior Carlos Corach y ratificado por decreto del presidente Carlos Menem) por 1.260 millones de dólares para la elaboración de un nuevo sistema de confección de DNI. Entre sus cláusulas se establece la obligación de cambiar el documento de identidad cada 10 años con un costo de 30 dólares por ejemplar (valor que duplica la tarifa vigente de esa época). Además, el contrato establece que la empresa Siemens recauda por los trámites migratorios y las tasas aeroportuarias.

Al año siguiente, con Fernando de la Rúa a cargo de la presidencia, el contrato fue suspendido con el argumento de renegociar sus términos para finalmente rescindirlo mediante el Decreto N° 669/2001, en el marco de Emergencia Económica Financiera que afecta al país.

En lo sucesivo, proliferan denuncias de corrupción por esta adjudicación y finalmente el contrato privatizador del sistema de confección de DNI jamás se implementa y deja una deuda de 1.5 millones de trámites sin resolver. Aquel proyecto escandaloso a nivel mundial termina con la caída del CEO de la multinacional en Alemania, en reclamos llevados a tribunales económicos internacionales y multas de cientos de millones de dólares a Siemens tanto por parte de la Unión Europea como de la Bolsa de Nueva York.

2.5-Nueva etapa en el registro de los ciudadanos

A raíz de esta coyuntura, en 2008 la presidenta Cristina Fernández implementa una política de Estado para actualizar el sistema de confección de DNI. Con una inversión

de 18,6 millones de dólares, se lleva a cabo un acelerado proceso de modernización que, a diferencia de las etapas anteriores mencionadas, se destina a la adquisición de equipamiento y nuevos recursos a fin de no tercerizar ninguna fase del proceso de elaboración y se capacita al personal vigente del Renaper y de las oficinas de los registros civiles del país.

El sistema de producción de DNI se mantuvo inalterable por más de 40 años hasta que comienza un proceso de reingeniería en el procedimiento de confección, por lo que se pasa de un documento que se elabora manualmente a uno totalmente digitalizado. Para implementar esta política nacional se designa a Florencio Randazzo como ministro del Interior¹². La primera etapa, denominada “Deuda Cero”, tiene como principal objetivo regularizar el estado de los trámites comenzados durante gestiones anteriores y que no habían sido concluidos. Para cumplir con las metas de este período, tal como se describe en la Quinta Carta Compromiso del Renaper (2012)¹³, se incorporan 50 peritos dactiloscópicos y se escanean las fichas identificatorias. La digitalización de las huellas digitales posibilita la validación y confron­te en pantalla, un procedimiento que deja atrás el retraso que genera realizar este trabajo de forma manual ya que requería buscar e identificar cada ficha personal en papel.

A mediados de 2009, se complementa el escaneo de 50 millones de impresiones dactilares y se crea una Base de Datos Identificatoria Nacional Única. Por otra parte, profesionales y agentes públicos desarrollan un software libre, propiedad del Estado argentino y se evita pagar licencias a empresas privadas.

Otro de los puntos importantes en este proceso de modernización es la construcción de una planta de producción con la implementación de nueva tecnología y el traslado físico del fichero central existente para almacenar todos los legajos de los ciudadanos con medidas de seguridad para conservar esos datos.

Para finalizar esta primera etapa, se actualizan los datos del Padrón Electoral Nacional -responsabilidad del Renaper- y se destinan recursos humanos y nuevos insumos tecnológicos (cámaras web, impresoras, entre otros) para establecer comunicaciones atrasadas: actualización a los 16 años, cambios de domicilio, fallecimientos, etc.

También se dicta el Decreto de Necesidad y Urgencia N° 90/2009 que establece un régimen administrativo gratuito para la inscripción de nacimientos de niños menores de

¹² A partir de junio de 2012 pasa a ser Ministerio del Interior y Transporte.

¹³ Quinta Carta Compromiso con los Ciudadanos. (2012). Registro Nacional de las Personas. Recuperado el 25 de noviembre de 2014, de http://www.sgp.gov.ar/contenidos/onig/carta_compromiso/docs/RENAPER-Quinta_Carta.pdf

12 años no registrados, con lo que se evita que el trámite se realice vía judicial según lo dispuesto en la Ley N° 26.413.

2.6-Nuevo DNI

Una vez alcanzados estos objetivos, se da inicio a la transición del nuevo sistema de producción documentaria y lanzamiento del Nuevo DNI. Así, el 20 de octubre de 2009 la presidenta Cristina Fernández dicta el Decreto N° 1.501 de la Ley N° 17.671 que establece “la utilización de tecnologías digitales en la identificación de los ciudadanos nacionales y extranjeros como así también en la emisión del Documento Nacional de Identidad”. Esta innovación significa la apertura para la utilización del sistema de identificación biométrica en la Argentina.

La biometría, según la información oficial¹⁴, es un método automático de reconocimiento de individuos, basado en características biológicas (anatómicas y psicológicas) y de comportamiento que se pueden medir. El Nuevo DNI posee “UN (1) código de barras de DOS (2) dimensiones el cual contenga datos biográficos y biométricos cuya lectura permita certificar su autenticidad, señalándose que ambos documentos se confeccionarán con un soporte papel de seguridad”¹⁵, según indica la normativa mencionada.

A fin de adecuarse a esta renovación tecnológica, se rediseña el sistema de expedición: los formularios que se completaban de forma manual, la obligatoriedad de llevar fotografía al momento de realizar el trámite y ensuciarse los dedos con tinta para dejar las huellas digital son reemplazados por un formulario único en donde se incluye la captura de foto, firma e impresiones dactilares digitalizadas.

Se crean dos canales de información (página web y línea de atención telefónica gratuita¹⁶), para que el ciudadano acceda personalmente a realizar la reserva del turno para tramitar el DNI (se elige día, hora y sede). Además, ambas vías sirven para consultar el estado de situación del trámite.

La confección del Nuevo DNI se puede diferenciar en dos etapas: en la primera se cargan los datos biográficos (información que se obtiene de la partida de nacimiento) y se digitalizan los datos biométricos (escaneo de las características físicas del

¹⁴ Argentina. Biometría. Recuperado el 12 de marzo de 2015, de <http://www.biometria.gov.ar/>

¹⁵ Decreto N° 1.501/2009 de Autorícese la utilización de tecnologías digitales en la identificación de los ciudadanos nacionales y extranjeros como así también en la emisión del Documento Nacional de Identidad.

¹⁶ Argentina. Ministerio del Interior y Transporte. Recuperado el 19 de noviembre de 2014, de <http://turnos.mininterior.gov.ar/turnosWeb/> y 0800-999-9364.

ciudadano), mientras que en la segunda fase se realiza un corte electrónico de esos datos biométricos y se los asocia con la imagen capturada. Luego se realiza el cotejo de las huellas dactilares digitalizadas con la firma digital que sirve para la verificación de datos. Una vez concluido este procedimiento, se imprime el nuevo ejemplar y se entrega en el domicilio del ciudadano.

Al centralizar el proceso de confección y el equipamiento de impresión en la nueva planta de producción ubicada en el barrio de Parque Patricios de la Ciudad Autónoma de Buenos Aires, el plazo de entrega del Nuevo DNI es de cinco días de realizado el trámite en contraposición a la anterior demora que oscilaba entre seis meses a dos años. Tanto para la digitalización del fichero central como para la informatización del circuito previo a la emisión del Nuevo DNI, se firman convenios de asistencia técnica destinados al desarrollo de aplicaciones informáticas y tareas de digitalización con la Universidad Tecnológica Nacional (UTN).

A principios de 2011, la ministra de Defensa Nilda Garré informa cambios en los documentos a cargo de la Policía Federal, ya que, por un lado, se deja de emitir la Cédula de Identidad y, por el otro, el Pasaporte pasa a ser confeccionado por el Renaper. Por primera vez en el recorrido documentario del país, el registro de los ciudadanos no depende de la órbita policial.

Para garantizar el cumplimiento de las tareas asignadas, según datos oficiales, se instalan más de 3000 oficinas de registro civil equipadas con el nuevo sistema informático mencionado, se abren centros de gestión rápida en centros comerciales y se equipan fábricas en camiones satelitales para llegar a zonas apartadas del país, así como también a las principales fiestas populares y destinos turísticos en las temporadas de verano y vacaciones de invierno. Además, para facilitar su acceso, el trámite del primer DNI es gratuito, el costo de la primera renovación obligatoria (16 años)¹⁷ es de 15 pesos y las demás renovaciones de 35 pesos.

Con el fin de ajustarse al registro biométrico que se implementa en el Nuevo DNI, se decide derogar la resolución donde se establece que la fotografía no puede generar confusión con respecto al sexo del individuo y se dicta la Resolución N° 169/2011, en donde se determina que “el derecho a la identidad demanda que la fotografía refleje de modo unívoco y lo más fielmente posible la imagen de la persona, reconociendo el derecho personal de todo individuo a ser representado fielmente tanto en sus aspectos

¹⁷ A partir que la Ley N° 26.774 de Ciudadanía Argentina, que habilita a los ciudadanos argentinos mayores de 16 años a votar, en noviembre de 2012 se modifica el artículo 10 de la Ley N° 17.671 estableciendo que la actualización del DNI debe realizarse a los 14 años.

dinámicos como estáticos; y en tal sentido el proceso identificatorio debe respetar los rasgos físicos del individuo, sus creencias y su historia personal signada de libres elecciones de vida, al momento de solicitar la expedición de un ejemplar de su DNI”.

Las modificaciones en el proceso documentario también se hacen visibles en cuanto al formato, en tanto que se realizan tres cambios en un período de cuatro años. En la primera etapa sólo se reemplaza el color verde por el celeste, manteniendo el formato libreta y se emite una tarjeta (similar al formato de la cédula de identidad) con los mismos datos identificatorios pero sin validez para realizar el sufragio. En 2012 se dictan dos resoluciones: la N° 585 que aprueba un cambio en el diseño para aplicar las “adaptaciones a las últimas tecnologías y materiales de seguridad” en la emisión de los DNI para mayores de 16 años, en la versión de ambos formatos; y la N° 797 que finalmente establece como válido el soporte tarjeta (deroga la Resolución N° 1.800/2009), ya que habilita este formato para realizar trámites públicos y privados e incluso para emitir el voto.

Por otra parte, en 2014 se dicta una normativa que establece la incorporación del número del CUIL -Código Único de Identificación Laboral- en el reverso del Nuevo DNI (Resolución N° 2.566). A partir de la firma de este convenio entre el ministro del Interior y Transporte y el titular de la Administración Nacional de la Seguridad Social (ANSES), Diego Bossio, se habilita un intercambio de información entre dichos organismos para facilitar los trámites que exigen ambos datos. “El CUIL sirve para que se registren todos los aportes a la Seguridad Social durante toda la vida laboral de las personas. También sirve para realizar el cambio de Obra Social, solicitar créditos personales, realizar trámites bancarios, o para la compra de un automóvil”¹⁸, según se indica en la página oficial de la entidad.

El acuerdo de ambos organismos comienza a fines de 2013 cuando se determina que se entregue automáticamente el CUIL a quienes gestionen el nuevo DNI o realicen su actualización. La información registrada en la base del Renaper, datos personales y vinculación entre menores de 18 años con sus progenitores o tutores, es incorporada en la plataforma del ANSES, sin necesidad de realizar ningún trámite.

Desde la implementación de esta política nacional, el discurso oficial alude a que el Nuevo DNI es más confiable debido a la incorporación de técnicas modernas y medidas de seguridad bajo estándares internacionales: papel de seguridad, hologramas, códigos de barras, tintas invisibles y de variación óptica. Por otra parte, asegura que es casi

¹⁸

Argentina. ANSES. Recuperado el 12 de marzo de 2015, de <http://www.anses.gob.ar/>

imposible su falsificación porque no se puede borrar datos, cambiar la fotografía ni alterar las huellas digitales.

Antes de finalizar su gestión, en diciembre de 2015, el ministro Randazzo anuncia que el DNI y pasaporte alcanzan la norma de calidad ISO 9001¹⁹. De esta manera, “el Renaper se convierte en la primera organización estatal en Argentina y la segunda a nivel mundial que certifica de manera internacional su estándar de producción y gestión”²⁰.

Según la normativa vigente, el Nuevo DNI es el único documento válido para los habitantes argentinos y se debe reemplazar los ejemplares expedidos con anterioridad (con excepción de mayores de 75 años e incapaces declarados judicialmente). De esta manera, a partir del 1 de abril de 2016 la libreta de enrolamiento, libreta cívica o el DNI formato verde, confeccionado a mano, quedan fuera de circulación, tal lo dispuesto en la Resolución N° 2.030/2015, firmada por la directora del Registro Nacional de las Personas, Mora Arqueta.

2.7-Nuevo Pasaporte

Tal como se mencionó anteriormente, a partir del Decreto N° 261/2011 se establece que el Registro Nacional de las Personas es el organismo responsable de la emisión del pasaporte, tarea que estaba a cargo de la Policía Federal desde 1968. Según la normativa, “el pasaporte es un documento que acredita la identidad y nacionalidad de su titular salvo prueba en contrario, resulta imprescindible establecer las previsiones adecuadas en orden a coordinar y centralizar la información entre los distintos órganos y unidades que han de llevar a cabo las tareas de expedición de dicho documento, con el objeto de impedir su utilización fraudulenta, especialmente en el ámbito de la delincuencia organizada y el tráfico de seres humanos”²¹. Establecido este cambio, el pasaporte y el DNI se tramitan en las mismas oficinas habilitadas y equipadas para dichos fines.

Un año después se realiza una nueva modificación, por lo que el ministro Florencio Randazzo anuncia que el Nuevo Pasaporte contará con un chip RFID (Radio Frequency

¹⁹ Normas 9000. Recuperado el 10 de diciembre de 2015, de <http://www.normas9000.com/que-es-iso-9000.html>.

²⁰ El DNI y el pasaporte argentinos obtuvieron la norma de calidad ISO 9001. (2015, diciembre 7). *Télam*. Recuperado el 10 de diciembre de 2015, de <http://www.telam.com.ar/notas/201512/129377-dni-pasaporte-norma-de-calidad-iso-9001.html>.

²¹ Decreto N° 261/2011 de Reglamento para la Emisión de Pasaportes. Boletín Oficial, Buenos Aires, Argentina, 2 de marzo de 2011.

IDentification; en español, identificación por radiofrecuencia) que permite incorporar los datos biométricos del titular del documento de viaje. Este sistema se basa en un dispositivo de captación y un software biométrico. El mecanismo de captación consiste en un chip que se coloca de forma interna en la contratapa del pasaporte, confeccionado con policarbonato, que distingue las singularidades del individuo, y el software biométrico capta la muestra física y la transforma en una secuencia numérica para lograr el reconocimiento automatizado del individuo. “La validación de la identidad de las personas se hace por dos vías. Mediante el escaneo del mismo cuando llega a los puestos migratorios de todo el mundo y a través de la incorporación de los datos biométricos y biográficos de la persona que aparecen en una pantalla y están encriptados en el chip, lo que hace que sea inviolable”²², indicó el funcionario.

Este documento de viaje tiene una validez de 10 años y el trámite cuenta con tres modalidades de expedición: una ordinaria, con una demora 15 días aproximadamente; otra que tarda 48 horas, denominada express (rápido) y, por último, modalidad “al instante” que se gestiona en el aeropuerto de Ezeiza, aeroparque Jorge Newbery, aeropuertos de Rosario, Córdoba y Mendoza, y que -mediante el pago de una tarifa diferencial- se entrega en el momento.

Por otra parte, el 27 de agosto de 2015 se presenta la primera puerta biométrica en la Terminal C en el aeropuerto de Ezeiza, (instalación denominada “Solución de Proceso Migratorio Autorizado”, Automated Border Control -ABC eGate por sus siglas en inglés-), que en un futuro próximo permitirá incrementar la agilidad en el registro del control migratorio de pasajeros y resolver el trámite de habilitación de entrada/salida del territorio en menos de 30 segundos. Luego de iniciar las pruebas pilotos en determinados vuelos, se extenderá la operatoria con 18 puertas que paulatinamente se colocarán en dicha terminal aérea, el aeroparque Jorge Newbery y el aeropuerto de Córdoba.

En términos generales y según información oficial de la Dirección Nacional de Migraciones²³, el pasajero se presenta frente a un eGate de doble esclusa, a fin de la lectura automática de su documento de viaje. En este primer tramo se verifica la elegibilidad del pasajero de realizar el trámite autoasistido. Si la evaluación resulta

²² El DNI y el pasaporte argentinos obtuvieron la norma de calidad ISO 9001. (2015, diciembre 7). *Télam*. Recuperado el 10 de diciembre de 2015, de <http://www.telam.com.ar/notas/201512/129377-dni-pasaporte-norma-de-calidad-iso-9001.html>

²³ Randazzo presentó las puertas biométricas en Ezeiza. (2015, agosto 27). Dirección Nacional de Migraciones. Recuperado el 27 de agosto de 2015, de http://www.migraciones.gov.ar/accesible/indexN.php?mostrar_novedad=2867

satisfactoria, se abre la primera esclusa permitiendo el acceso a la zona interna del eGate y cerrándose tras su paso, asegurando que se encuentra solo en dicha área. La segunda instancia consiste en la verificación de identidad del pasajero y cotejos adicionales. La verificación de la identidad es multi-biométrica (rostro y huella) y de resultar fructuosa, se abre la segunda esclusa dando fin al proceso.

Estos cambios tecnológicos apuntan a reemplazar la identificación tradicional manual por una identificación remota. De este modo, la veracidad del pasaporte ya no requerirá realizarse cara a cara entre el pasajero y el inspector de Migraciones, sino que al pasar el documento de viaje por el lector de la terminal estos datos se cotejan automáticamente con los registros que existen en una base de datos centralizada para permitir o denegar el ingreso/egreso de la persona.

2.8- SIBIOS, la gran base estatal de datos

Hacia fines de 2011, a partir de un convenio entre los Ministerios del Interior y de Seguridad, la presidenta Cristina Fernández dicta el Decreto 1.766/2011 que establece la puesta en funcionamiento del nuevo Sistema Federal de Identificación Biométrica (SIBIOS). Se trata de un software de propiedad intelectual y desarrollo de profesionales cubanos que tiene como finalidad instrumentar un servicio informático para permitir la comprobación de identificación de personas y rastros para fines de seguridad pública y de investigación judicial. Así se conforma en una base de registro de datos biométricos masiva y centralizada que incluye además de las huellas digitales (AFIS - Automated Fingerprint Identification System; en español, Sistema Automatizado de Huellas Digitales), un escaneo facial que permite identificar a una persona en tiempo real con sólo tomar una fotografía y registrar su huella digital.

De esta manera, una vez que se captura la huella dactilar de una persona, el sistema ejecuta la búsqueda en la base de datos y lleva a cabo la identificación automática de esa muestra con los datos vinculados previamente a un número de documento.

Hasta el momento, el registro más completo pertenecía a la Policía Federal y correspondía a la tramitación de cédulas y pasaportes. Con este nuevo sistema se busca posibilitar un acceso descentralizado a una única base de datos.

La segunda etapa del sistema de identificación se lanza en octubre de 2015 cuando se incorpora mayor tecnología biométrica a la base de datos del Renaper. Esta nueva fase también cuenta con la colaboración de profesionales cubanos, y consiste en obtener la identidad de una persona con solo una imagen. En la etapa previa se la podía verificar

comparando dos fotografías pero, con esta actualización, se realiza la identificación del ciudadano contrastando una imagen contra toda la base de datos del organismo, innovación que ayuda a las autoridades judiciales a esclarecer casos delictivos.

Según describió el ministro del Interior y Transporte, “hoy las bases de datos del Renaper están compuestas por huellas dactilares y fotografías de rostros de más de 40 millones de argentinos que ya tramitaron el Nuevo DNI (...) esto nos permite verificar con un 100% de efectividad la identidad de cada argentino”²⁴. Previamente, en junio de 2014, había firmado un acta de acuerdo con la Real Casa de la Moneda de España para la implementación de mayor tecnología en el Nuevo DNI. Se trata de la incorporación de un doble chip que, además de los datos identificatorios de la persona, incluirá los datos de su historia clínica, datos previsionales, jubilatorios (otorgados por la ANSES y el Programa de Atención Médica Integral -PAMI-) y del Sistema Único de Boleto Electrónico (SUBE)²⁵.

De esta manera, a partir de la implementación de SIBIOS, se podrá cruzar la información filiatoria, domicilio, declaraciones impositivas, viajes en servicios públicos, entradas y salidas del país con el uso de las huellas digitales o datos biométricos faciales.

Aunque no existe una confirmación oficial, autoridades de gobierno manifestaron que a la base de datos de identificación tienen acceso los organismos de seguridad y otros tales como Dirección Nacional de Migraciones, Policía Aeroportuaria y Gendarmería Nacional. A su vez, estará disponible también para las fuerzas policiales y entidades provinciales, a través de acuerdos con el Estado.

Desde el inicio de la implementación de la política identificatoria/documentaria, el gobierno nacional asocia la idea del derecho a la identidad con el acceso y la garantía a otros derechos básicos, a la vez que refuerza la importancia de la tramitación y

²⁴ Randazzo anunció que “Argentina incorporará tecnología biométrica que permitirá ayudar a la justicia a identificar identidades desde imágenes”. (2015, octubre 13). *Ministerio del Interior y Transporte*. Recuperado el 30 de noviembre de 2015, de <http://www.mininterior.gov.ar/prensa/prensa.php?i=4594>.

²⁵ Sistema para el transporte y microconsumo comercial creado por el Decreto N° 84/2009 y su complementario Decreto N° 1.580/2013. Se implementa el 3 de marzo de 2012 para el transporte público del Área Metropolitana de Buenos Aires y en las líneas de colectivos de Mar del Plata, Villa Gesell, Paraná, Santa Fe y Bariloche. A partir de la Resolución N° 2.391/2015, firmada por el ministro del Interior y Transporte, se informa que desde el 1 de diciembre de 2015 dejan de coexistir los dos sistemas de pago, monedas y tarjeta, siendo el SUBE la única forma de pago en Área Metropolitana. En cuanto a los servicios provinciales, se establece el 30 de junio de 2016 como plazo máximo para instalar el boleto electrónico (la Secretaría de Transporte entregará un incentivo económico para su implementación) o aquellos que no hayan optado por el sistema SUBE deberán instalar el Módulo de Posicionamiento Global (GPS - Global Positioning System) homologado por el Banco de la Nación a través de Nación Servicios S.A.

obtención del dispositivo documentario. “El derecho a la identidad es la puerta de acceso que permite el ejercicio de otros múltiples derechos esenciales que hoy están más vigentes que nunca en nuestro país: el derecho al voto, al trabajo, a un beneficio previsional, a la salud, la educación o a la Asignación Universal por Hijo. En la Argentina, sin DNI, tales derechos se vuelven abstractos”, aseguró el ministro Florencio Randazzo en una entrevista publicada en *DNI, Hacia una identidad sin trampas* (Villarruel, 2011:130).

En los capítulos que siguen analizaremos el concepto de identidad, el desarrollo de formas específicas de identificación, las prácticas y actores que la constituyen y materializan, los riesgos de la difusión e implementación de tecnologías contemporáneas en la materia y los escasos debates que se suscitan en torno a estas cuestiones.

Capítulo 3

La identificación en clave biológica

3.1-Identificar a la población

“Reconocer si una persona o cosa es la misma que se supone o se busca” y “dar los datos personales necesarios para ser reconocido”²⁶, son dos de las cinco acepciones que el diccionario de la Real Academia Española reconoce para el término identificación.

Desde la aparición de los Estados modernos, la identificación de la población se convirtió en un tema de suma importancia y preocupación. Tal es el caso que continuamente surgen nuevas y reconfiguradas técnicas y dispositivos que permiten profundizar las tareas de vigilar, controlar e identificar a los individuos.

Los gobiernos autoritarios y las experiencias dictatoriales de las que se tienen referencias siguieron un mismo patrón de comportamiento a la hora de fichar a los considerados grupos de riesgo: inicialmente a las clases peligrosas, los sospechosos, criminales o terroristas, luego a los sectores más vulnerables a la estigmatización por motivos raciales, políticos, religiosos o de origen, y finalmente, se extiende a toda la población (About y Denis, 2011). “El cuerpo político deviene en cuerpo criminal”²⁷, apunta Agamben (2005).

Varios de los sistemas y prácticas de matriz autoritaria se mantuvieron e, incluso, perfeccionaron durante los procesos democráticos. Tales circunstancias sumadas a la implementación de la tecnología funcionaron como las condiciones de posibilidad para la instauración de nuevas y extendidas redes de vigilancia y control. En el texto “Gestión de la identidad y procesos de subjetivación en la Argentina actual (2001-2013)”, Luis García Fanlo sostiene que “el impacto de los desarrollos tecnológicos en curso sobre los dispositivos de vigilancia ha producido una doble transformación. Los antiguos dispositivos disciplinarios basados en soportes analógicos y mecánicos se digitalizan y mediatizan al mismo tiempo que aparecen nuevos dispositivos de seguridad digitales que tienen la capacidad de ensamblarse entre sí configurando redes de vigilancia que ya no operan sobre individuos encerrados e identificados

²⁶ Real Academia Española. Recuperado el 17 de agosto de 2015, de <http://lema.rae.es/drae/srv/search?key=identificar>

²⁷ Agamben, Giorgio (2005, diciembre 5). No a la biometría. *Le Monde*. Recuperado el 16 de agosto, de <https:// analisismadrid.wordpress.com/2011/09/05/no-a-la-biometria-giorgio-agamben/>

institucionalmente (prisiones, fábricas, hospitales, escuelas, cuarteles) sino sobre el conjunto de la población (calles, plazas, paseos y edificios públicos, centros comerciales, aeropuertos, terminales de ómnibus, ferrocarriles y trenes subterráneos, cines, rutas, peajes, etc.), es decir, sobre la circulación de los individuos libres y anónimos (....) La ciudad se convierte en un macro dispositivo de encierro habitado por sujetos a los que hay que identificar fehacientemente ya que cualquiera de ellos puede ser un individuo peligroso mezclado entre la multitud”²⁸.

Atento a esta necesidad y en su afán clasificatorio, el Estado argentino fue un gran precursor en la imposición y extensión de una poderosa tecnología como el sistema de documentación para lograr la identificación de todos sus habitantes. En el texto “‘¡Identifíquese!’. Apuntes para una historia del control de las poblaciones”, Anitua sostiene que “el método de identificación dactiloscópica de Vucetich extendió el campo del delito a los electores y posibilitaba el funcionamiento del sistema político a la vez que facilitaba el control del cuerpo social. Argentina se transformó de esa forma en la pionera en exigir un documento obligatorio de identificación con finalidades disciplinarias. El Documento Nacional de Identidad proveyó la doble identificación - nacional e individual- que dejaba a sus portadores a merced de los controles estatales” (2005:18-19).

3.2-Ciencia, tecnología y cuerpo

Con el objetivo de profundizar esta herramienta de control, en el año 2009 el Poder Ejecutivo Nacional aprueba mediante resolución administrativa -sin paso previo ni discusión en el Congreso Nacional-, la utilización de tecnologías digitales en la identificación de los ciudadanos nacionales y extranjeros como así también en la emisión del DNI. Con esta decisión comienza la utilización del sistema de identificación biométrica en la República Argentina.

La palabra biometría deriva de los términos griegos *bios* [vida] y *metron* [medida] y se define como un método automatizado de reconocimiento de un individuo, basado en características biológicas (anatómicas y fisiológicas) y de comportamiento medibles.

Se trata de una ciencia que estudia las características cuantitativas de los seres vivos y emplea diferentes técnicas: por un lado, aquellas que se basan en características o aspectos físicos de las personas como las huellas dactilares, la geometría de manos, la

²⁸ García Fanlo, Luis (2014). Gestión de la identidad y procesos de subjetivación en la Argentina actual (2001-2013). *Revista Trazos universitarios*, pp.4-5.

característica de los ojos, los poros de la piel, el tamaño y la distancia entre boca, nariz y ojos; y por el otro, aquellas vinculadas con la conducta humana como ser la escritura manuscrita, la voz, los gestos y los movimientos corporales. Mientras que al primer grupo de técnicas se denominan estáticas, al segundo se las considera dinámicas.

Con el uso de esta disciplina se puede plantear que las modalidades de identificación se ajustan a determinadas variables biológicas y sociales, que están “ligadas al contexto biotecnológico de la sociedad y participan de una política del cuerpo (...) La biometría hace posible una identificación que ya no parte de la imagen del cuerpo sino de la firma genética. Las impresiones digitales subsisten, pero se les suma el iris del ojo, el contorno del rostro, el de la palma de la mano, la red venosa, la voz, el aspecto o el aliento. La impronta del cuerpo concierne desde ahora a la estructura íntima al ofrecer la imagen del perfil genético: el genetoscopio” (2011:163), asegura el psicoanalista Gérard Wajcman.

A diferencia de otros procedimientos, la biometría utiliza lo que las personas son para poder identificarlas y no lo que saben, tienen o hacen, como puede ser una clave, una tarjeta o una firma. De este modo, los sistemas biométricos actúan sobre el cuerpo de los individuos y pueden implementarse sin el consentimiento de estos.

Los rasgos biométricos representan intrínsecamente las formas corporales del individuo, conforman una combinatoria de anatomía y de comportamiento y son extraídos del cuerpo humano vivo. Estos rasgos utilizados como identificadores biométricos deben satisfacer ciertos requerimientos generales, tales como universalidad (cada persona debe poseer ese rasgo biométrico), particularidad (todas las personas tienen que ser suficientemente diferentes en términos del rasgo biométrico), permanencia (el rasgo biométrico debe ser invariable en el tiempo y a cualquier otro factor), medible (el rasgo biométrico se tiene que poder medir cuantitativamente), rendimiento (el rasgo biométrico debe garantizar precisión y robustez en diferentes factores ambientales), aceptabilidad (los usuarios del sistema deben aceptar el uso de ese rasgo biométrico para su identificación) y no falsificable (el rasgo biométrico tiene que garantizar que su falsificación sea dificultosa).

Según información oficial²⁹, la identidad de una persona está conformada por un conjunto de rasgos propios que lo caracteriza frente a los demás. Con el sistema biométrico, estos datos son recogidos empleando dispositivos denominados sensores,

²⁹

Argentina. Biometría. Recuperado el 12 de marzo de 2015, de <http://www.biometria.gov.ar/>

que son utilizados para recolectar los datos necesarios para el reconocimiento y para convertirlos en información digitalizada.

A partir de esta innovación tecnológica, la identificación se convirtió en la tarea mediante la cual el sistema biométrico intenta determinar la identidad de un individuo. Así, estos datos biométricos son comparados contra todos aquellos que se albergan en una gran base de datos.

En el discurso de presentación del VI Congreso Internacional de Biometría realizado en la República Argentina en noviembre de 2011, el jefe de Gabinete de Ministros Aníbal Fernández expresó que “la biometría es la más noble herramienta de identificación y gracias a ella hoy podemos saber con exactitud que una persona es quien dice ser”³⁰.

Sin embargo, es importante destacar que algunos autores como Joseph Pato y Lynette Millet en *Biometric recognition: Challenges and opportunities* (2010) aseguran que las distintas técnicas de análisis biométrico arrojan resultados en términos de probabilidad por lo que la identificación nunca es perfecta. Esto quiere decir que una identificación biométrica positiva significa una probabilidad de identificación correcta.

Entre las diferentes fuentes de variación que impactan en el proceso, los autores señalan los posibles cambios que sufren los individuos producto de enfermedades, envejecimiento y cirugías, así como también la calibración de los sensores para la captura de datos, el proceso de almacenamiento y la calidad de la información.

Además de la fragilidad y los riesgos de este tipo de procedimiento en materia identificatoria, se puede plantear que con este mecanismo la identidad de las personas queda reducida a su mera naturaleza biológica, anulando otros elementos constitutivos que conforman la caracterización de las personas. En relación a esto, Wajcman asegura que “el problema está en que ese movimiento de una ciencia identitaria que pasa del rostro y de la impresión digital a la impronta genética, al ADN, al iris, a nuestra marcha, a nuestros tics, a nuestra voz, al aspecto y al aliento, se sostiene de una idea rectora incierta y funesta: la de que nuestra identidad se resuelve en nuestra biología, fundamentalmente en nuestro cuerpo. Una de las creencias es que en nuestro cuerpo está contenida enteramente nuestra identidad” (2011:164). En consonancia a este planteo, Bauman y Lyon sostienen que “los cuerpos son reducidos a simples datos. Esto se ve quizás mejor en la utilización de datos biométricos en las fronteras. En el modelo paradigmático, el objetivo de estos datos es controlar la identidad del cuerpo, es decir,

³⁰ Congreso Internacional de Biometría de la República Argentina [CIBRA]. (2011, noviembre 14). Apertura Dr. Aníbal Fernández. Recuperado de 4 de junio de 2015, de <http://www.biometria.gov.ar/congresos/cibra-2011/videos.aspx#.U8cX7DtSZrs.twitter>

de la persona (...) sólo se puede concluir que la información sobre el cuerpo es tratada como si fuera concluyente para determinar la identidad de la persona” (2013:139).

Otro punto importante es que ante la incorporación de estas sofisticadas técnicas para mejorar y profundizar el proceso identificatorio, resulta pertinente cuestionar la finalidad e intencionalidad del Estado nacional en la búsqueda por rastrear y registrar a la población. Casi a modo de respuesta oficial, el texto del seminario *Un Nuevo Estado, un Nuevo DNI*³¹ desarrollado por el Ministerio del Interior y Transporte y firmado por Florencio Randazzo, informa: “Un documento, un pasaporte, una cédula o una partida son sólo el soporte material de un proceso identificatorio que lo precede. Sin embargo, la clasificación que nos importa es la relativa a la finalidad de la identificación. ¿Para qué y por qué el Estado debe identificar a sus ciudadanos? Identificar para promover y proteger la identidad personal, individualizar a cada ciudadano para garantizar sus derechos y el cumplimiento de sus obligaciones. La identificación debe ser un instrumento de promoción ciudadana, un instrumento al servicio del derecho a la identidad y nunca ser utilizada como un mecanismo de control social”.

Pese a esto, la actual política de identificación estatal presentada como novedosa y basada en la premisa del empoderamiento de derechos, no sólo no se corresponde a esta sino que tampoco trajo aparejada ninguna modificación sustancial. Esto queda demostrado con el hecho de que no se efectuaron cambios legislativos sino que se trató de meras actualizaciones tecnológicas. Es decir, los cambios implementados en los documentos de identidad descriptos en el capítulo anterior se ejecutaron manteniendo la Ley N° 17.671 de Identificación, Registro y Clasificación del Potencial Humano Nacional, sancionada en 1968 durante un gobierno de facto presidido por el general Juan Carlos Onganía.

Incluso el texto *Un Nuevo Estado, un Nuevo DNI* recupera el concepto de potencial humano conservando la matriz autoritaria de la normativa sobre la que se sostiene el sistema de registro de identificación argentino, en detrimento de una nominación y/o perspectiva basada en los derechos humanos. Una vez más se evidencia que los ciudadanos quedan subsumidos como capital del Estado: “Es importante destacar que tanto la inscripción como la documentación de todos los sectores de la sociedad, sin

³¹ Un nuevo Estado, un nuevo DNI (s.f). Ministerio del Interior y Transporte. Recuperado el 20 de septiembre de 2015, de <http://www.mininterior.gov.ar/asuntospoliticos/pdf/nuevo-estado-nuevo-DNI.pdf>.

excepción ni discriminación, contribuye a la formación de un registro de datos que refleja el potencial humano de nuestro país”³².

3.3-Un *quién es quién* estatal

Como se mencionó anteriormente, con el objetivo de construir una gran base estatal de datos, el 7 de noviembre de 2011 la presidenta Cristina Fernández anunció la creación del Sistema Federal de Identificación Biométrica para la Seguridad (SIBIOS), mediante el Decreto N° 1.766/2011, que tiene por objeto prestar un servicio centralizado de información respecto de los registros patronímicos y biológicos individuales, a los fines de contribuir a la comprobación oportuna en materia de identificación de personas y rastros.

De este modo, se habilitó al Registro Nacional de las Personas a transferir al Ministerio de Seguridad, autoridad de aplicación, la información identificatoria obtenida con los nuevos documentos. A su vez, este servicio de identificación biométrica centralizado, con cobertura nacional, permite a las agencias de seguridad hacer ‘referencias cruzadas’ de información con datos biométricos y otros datos inicialmente recogidos con el fin de mantener la operatoria del registro nacional del DNI.

Además, el SIBIOS se encuentra integrado con las bases de datos de identificación que sumados a los identificadores biométricos, incluyen imagen digital y otras informaciones básicas que se recolectan desde el nacimiento y a través de la vida de las personas.

Por otra parte, el sistema biométrico para la identificación de personas comenzó a implementarse en el control migratorio de los aeropuertos y puertos internacionales del país a cargo de la Dirección Nacional de Migraciones, con el fin de registrar a todos los argentinos y extranjeros que ingresen o egresen del territorio nacional.

Con la creación de este sistema federal de información biométrica digitalizada, el Estado argentino procuró incorporar a todos los ciudadanos en una gran base de datos a fin de poder cruzar el registro de las huellas dactilares con el rostro de las personas, eliminando incertidumbres acerca de las identidades. Incluso los bebés nacidos a partir del 1 de enero de 2012 fueron incorporados desde su primer día de vida al programa en cuestión, con sus respectivas huellas dactilares y de los pies.

Respeto a los adultos mayores de 75 años que se encuentran exceptuados de tramitar de manera obligatoria el Nuevo DNI, ANSES lanzó el programa denominado Mi huella³³,

³² Id.

el cual requiere la validación de las huellas digitales de los beneficiarios para el cobro de las jubilaciones y pensiones. Así, se prevé que a lo largo de 2015 el Estado registre las huellas de unas siete millones y medio de personas para que puedan percibir sus haberes. Y, mediante la instalación de tótems o equipos de identificación biométrica en las entidades bancarias, se podrá realizar diversos trámites y evitar largas filas.

Con este sistema pareciera que nadie puede escapar de la vigilancia y el control: argentinos, extranjeros, recién nacidos, ancianos. Todos los ciudadanos estarán incluidos e identificados. El discurso de presentación pronunciado por la presidenta Fernández y emitido por cadena nacional, refuerza esta idea: “Es un salto cualitativo muy importante en la seguridad, sobre todo hoy que hay prácticamente en todos los lugares cámaras que permiten filmar e identificar rostros; obviamente no se puede saber quiénes son por las huellas digitales, pero sí a través de esta identificación (...) Va a permitir, en tiempo real, conocer y saber quién es la persona que está ante un personal de seguridad o en cualquier otro lado, si es esa persona y si no es, quién es en realidad”³⁴.

Ahora bien, si en el pasado este fichaje identificatorio se limitaba a sospechosos de delitos o convictos de ofensas criminales y en la actualidad se extiende a toda la población pero con la incorporación de sofisticadas herramientas tecnológicas, se puede plantear que se produjo una inversión en el paradigma jurídico: todos somos culpables hasta que la identificación demuestre lo contrario. O, como expresó el sociólogo Andrés Pérez Esquivel en la jornada *Tecnología, vigilancia y derechos personalísimos*, “todos somos culpables hasta que nuestro cuerpo demuestre lo contrario”³⁵.

Desde el discurso oficial, los argumentos que se esbozaron para justificar la creación e implementación del SIBIOS estuvieron relacionados con el tema de la seguridad y la prevención del delito. En el correspondiente decreto se expresa que dicho sistema “posee como finalidad instrumentar un servicio informático para permitir la comprobación idónea y oportuna de identificación de personas y rastros para fines de seguridad pública y de investigación judicial, contribuyendo al desarrollo de políticas

³³ Diego Bossio: “Con la huella digital los jubilados no van a tener que ir más al banco” (2014, diciembre 30). ANSES. Recuperado el 4 de junio de 2015, de <http://www.anses.gob.ar/noticia/diego-bossio-con-la-huella-digital-los-jubilados-no-van-a-tener-que-ir-mls-al-banco-128>.

³⁴ Presentación del Programa Identificación Biométrica: Palabras de la Presidenta de la Nación (2011, noviembre 7). Casa Rosada. Recuperado el 10 de octubre, de <http://www.casarosada.gob.ar/informacion/discursos/25505-presentacion-del-programa-de-identificacion-biometrica-palabras-de-la-presidenta-de-la-nacion>.

³⁵ Tecnología, vigilancia y derechos personalísimos (2015, agosto 19). Jornada organizada por la Carrera de Especialización en la Facultad de Derecho de la Universidad de Buenos Aires, Argentina.

eficientes de prevención y conjuración de ilícitos en el ámbito de la seguridad ciudadana y al mejoramiento de las diligencias investigativas requeridas por autoridades judiciales”³⁶.

Pese a esto, la recolección, almacenamiento y uso de datos personales por parte del Estado no resulta ser un tema que preocupa a la sociedad ni suele instalarse en la agenda pública, salvo en aislados debates. Pareciera que los argentinos naturalizaron estas formas de vigilancia y control, clausurando posibles tipos de resistencia. Al respecto, García Fanlo sostiene que “SIBIOS es el nuevo paradigma del Gran Hermano orwelliano que gobierna no por la coerción real que implica el sistema de vigilancia e identificación en sus formas actuales sino por el hecho de que su existencia está naturalizada en la subjetividad individual y colectiva de los argentinos de modo tal que nadie se sienta ni vigilado ni controlado. De modo que las formas actuales de la sociedad de vigilancia en Argentina producen, a su vez, efectos de sujeción y subjetivación, gobierno de sí y de los otros, subjetividades sujetas a un poder externo y a sí mismas, interioridades que funcionan como complejos pliegues de una exterioridad. Lo que hacen estos dispositivos no es otra cosa que vigilar e identificar y producir en nuestras subjetividades el deseo de ser vigilados e identificados. Y en ese sentido, la sociedad de vigilancia imaginada por Orwell se ha vuelto realidad en Argentina y ya forma parte de nuestra subjetividad”³⁷.

Otra interesante reflexión acerca de este mismo fenómeno es la que realiza Mattelart en su obra *Un mundo vigilado*, contraponiendo las antiguas modalidades disciplinarias con las actuales en la era del control: “La propia videovigilancia, emblema del Gran Hermano, según sus aplicaciones, o bien prolonga las antiguas disciplinas, o bien constituye una ilustración de este nuevo tipo de control con, entre ambos, una multitud de formas mixtas (...) Pero hay una notable diferencia entre las dos modalidades de vigilancia: mientras que las disciplinas exigen todo un trabajo del individuo sobre sí mismo con el fin de cambiar sus comportamientos naturales, incluso sus formas de ser, el nuevo tipo de control se hace a sus espaldas, de manera indirecta y no exige participación alguna por su parte. Se trata de vigilarlo y de tomar decisiones sobre él a partir de un doble constituido por sus informaciones, sus huellas o su imagen” (2009:234-235).

³⁶ Decreto N° 1.766/2011 de Creación el Sistema Federal de Identificación Biométrica para la Seguridad, Boletín Oficial, Buenos Aires, Argentina, 07 de noviembre de 2011.

³⁷ García Fanlo, Luis (2014). Gestión de la identidad y procesos de subjetivación en la Argentina actual (2001-2013). *Revista Trazos universitarios*, pp. 14-15.

3.4-Marcas indelebles

Desde hace tiempo, distintas voces disidentes a nivel mundial se manifestaron en contra de la aplicación de los controles biométricos. Uno de ellos fue el filósofo italiano Giorgio Agamben, quien publicó un artículo en el periódico *Le Monde* al que tituló “No al tatuaje bio-político”. En este explica que rechazó la invitación a dictar un curso en la Universidad de Nueva York tras su negativa a someterse al procedimiento exigido para ingresar a Estados Unidos con una visa: ser fichado y dejar las huellas digitales.

Al respecto, Agamben sostiene: “No se trata sólo de una reacción epidérmica frente a un procedimiento que fue impuesto durante mucho tiempo a los criminales y acusados políticos. Si sólo se tratara de eso, podríamos con seguridad aceptar moralmente compartir, por solidaridad, las condiciones humillantes a las que son sometidos hoy tantos seres humanos. Lo esencial no está ahí. El problema excede los límites de la sensibilidad personal y concierne al estatuto jurídico-político (sería quizás más simple decir bio-político) de los ciudadanos de los Estados pretendidamente democráticos en los que vivimos”³⁸.

Para explicar sus argumentos ante dicha negativa, el autor define como tatuaje subcutáneo al fichaje electrónico de las huellas digitales y de la retina, como a otras prácticas del mismo género, y considera que este tipo de técnicas de control y manipulación de los cuerpos inaugura una nueva era biopolítica, en el sentido foucaultiano desarrollado más arriba. Esta nueva relación biopolítica entre los ciudadanos y el Estado no contempla una participación libre en la esfera pública sino que concierne a “la inscripción y fichado del elemento más privado e incommunicable de la subjetividad: la vida biológica de los cuerpos”³⁹.

Por otra parte, Agamben asegura que las razones de seguridad que se invocan a la hora de justificar este tipo de procedimientos (tal es el argumento utilizado por el Estado argentino) no son convincentes porque si bien “pueden contribuir a la prevención de la reincidencia, son inútiles contra un atentado terrorista que ocurra por primera vez”⁴⁰. Sin embargo, el autor agrega que estas metodologías “son perfectamente eficaces para el control masivo de individuos. El día que la supervisión biométrica se haya generalizado y la vigencia mediante cámaras de video se extienda a lo largo de las

³⁸ Agamben, Giorgio (2004, enero 11). No al tatuaje bio-político. *Le Monde*.

³⁹ Id.

⁴⁰ Agamben, Giorgio (2005, diciembre 5). No a la biometría. *Le Monde*. Recuperado el 16 de agosto, de <https:// analisismadrid.wordpress.com/2011/09/05/no-a-la-biometria-giorgio-agamben/>

calles, toda crítica y disenso habrá devenido imposible”⁴¹. Tal como afirma Mattelart, “desde los primeros usos de las técnicas biométricas con fines policiales, ha germinado la idea de su extensión a las masas” (2009:31).

Por otra parte, el filósofo italiano recuerda que “la historia nos enseña que las prácticas reservadas al comienzo a los extranjeros, enseguida se aplican al conjunto de los ciudadanos”⁴². Así, al aplicar a todo individuo las técnicas y dispositivos que fueron inventados para las clases peligrosas, los Estados hicieron del ser humano el sospechoso por excelencia, hasta el punto de que es la humanidad misma la que se transformó en clase peligrosa.

A su vez, Agamben recuerda que el tatuaje fue utilizado como el modo más normal y económico de organizar la inscripción y el registro de los deportados en los campos de concentración. Además de la tarea identificatoria, este método reducía al individuo a un número y eliminaba así todo rasgo de humanidad. No tan lejano ni ajeno a esto resulta la idea de Juan Vucetich, pionero en la utilización del sistema dactiloscópico, quien alguna vez sentenció que “el documento de identidad era el equivalente legal del individuo; su representación perfecta, la cifra matemática de su individualidad (...) Algunos años después, el que fuera su discípulo, Luis Reyna Almandós, llegó a afirmar que el ‘documento’ y la asignación de un número a cada persona era en realidad un derecho, pues ese número único e irrepetible facilitaría la existencia de los individuos, protegería su honor de confusiones con otros y garantizaría la verdadera identidad. Finalmente llegó a proponer que para mayor comodidad ese número fuera tatuado en el cuerpo de cada individuo” (Anitua, 2005:19-20).

3.5-“Documentos, por favor”

Teniendo en cuenta el recorrido trazado sobre el proceso documentario y el Documento Nacional de Identidad como gran tecnología biopolítica, así como las relaciones entre tecnología, comportamiento y subjetividad, cabe destacar la falta de cuestionamiento por parte de la sociedad ante la imposición histórica y la condición de obligatoriedad por parte del Estado a tal medida.

Esto se puede analizar a la luz de los aportes de Pierre Bourdieu, quien propone el concepto de habitus para pensar y comprender las prácticas de los sujetos a partir de las estructuras y disposiciones que operan en él. Al respecto, el autor sostiene que “los

⁴¹ Id.

⁴² Agamben, Giorgio (2004, enero 11). No al tatuaje bio-político. *Le Monde*.

condicionamientos asociados a una clase particular de condiciones de existencia producen *habitus*, sistemas de disposiciones duraderas y transferibles, estructuras estructuradas predispuestas para funcionar como estructuras estructurantes, es decir, como principios generadores y organizadores de prácticas y representaciones” (1994:91-111).

El *habitus* es una noción central en Bourdieu y puede ser entendido como un principio generador de prácticas, resultado de la incorporación de las condiciones de existencia. Este implica condicionamientos pero no determinaciones, por tal motivo las prácticas de un sujeto van a estar condicionadas por las disposiciones de su *habitus* primario pero su acción involucra un conjunto infinito de prácticas dentro de los límites de esos condicionamientos. A su vez, puede pensarse como la concreción en actos de cotidianidad de forma de comportamiento social transmitidas desde la ideología dominante, es decir, un mecanismo de reproducción de estructuras mentales y sociales que se encarnan en actividades cotidianas. A este fenómeno caracterizado por mecanismos mediante los cuales se imponen determinadas formas de actuación a la vez que se naturalizan como evidentes, Bourdieu lo denomina violencia simbólica. Es decir, aquellos actos cotidianos que los sujetos ejecutan como algo natural e incuestionable son impuestos mediante la institucionalidad de las fuerzas en conflicto a través de la violencia simbólica. En palabras del autor, “la violencia simbólica es esa violencia que arranca sumisiones que ni siquiera se perciben como tales apoyándose en unas expectativas colectivas, en unas creencias socialmente inculcadas” (1999:173).

De esta manera, se puede plantear que la aceptación y naturalización del proceso documentario en la sociedad argentina así como el éxito de la tramitación, portación y renovación del documento identificador, con la correspondiente entrega de huellas digitales y otros datos personales, se encuentran íntimamente incorporados a la noción de *habitus*, ejercido mediante la violencia simbólica. García Fanlo se ocupa de analizar este fenómeno y lo expresa de la siguiente manera: “Inicialmente la población, en particular los sectores populares, resistieron el sistema pero luego de una insistente campaña pública que asociaba la inseguridad en las calles (por el delito y la violencia anarquista) con las facilidades que el nuevo sistema ofrecía al ciudadano ‘común y corriente’ para diferenciarse y no ser confundido con un delincuente o un revolucionario, fue finalmente aceptado convirtiéndose en un verdadero *habitus* no salir

a la calle sin portar la cédula de identidad”⁴³. En otro tramo del análisis, recuerda su experiencia personal: “Tengo grabada en la memoria la insistente pregunta de mi padre o mi madre cada vez que salía a la calle: ‘no te olvides la cédula de identidad’ cuya contracara era ‘no te metás ahí donde pueda haber algún problema’, es decir, donde alguien pueda llegar a sospechar quién soy”⁴⁴.

Por su parte, la comunicóloga y miembro de la fundación Vía Libre, Laura Siri, estudia el tema y asegura: “Objetar el hecho de que toda la población deba aportar sus huellas digitales al sistema es muy inusual, salvo entre los 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”⁴⁵.

3.6-Un panóptico de bolsillo

Las formas actuales de la sociedad de control en Argentina, en términos de Deleuze, superan lo planteado hasta el momento y pueden pensarse como nuevos modos de subjetivación que hacen del derecho a la identidad así como la lucha contra inseguridad, probables excusas para implementar sofisticados sistemas de vigilancia a la hora de identificar y clasificar a la población.

Tal es el caso que en el lanzamiento del SIBIOS, cuyo slogan sostiene *Si nos conocemos mejor, nos cuidamos más*, circuló un video promocional que asegura: “El sistema realiza el proceso de identificación en forma automática y en pocos segundos ejecuta la búsqueda en una base datos de millones de huellas y rostros previamente registrados asociados a un número de DNI (...) Es una herramienta indispensable en prevención de delitos de suplantación de identidad, tanto de tipo económico como de trata de personas (...) Además, multiplica la posibilidad de esclarecimiento y resolución en caso post delito otorgando un soporte científico para los casos criminales. El reconocimiento fisonómico permite proyectar el rostro de una persona a través del tiempo, aumentando así las posibilidades de encontrarla. De esta manera, las fuerzas de seguridad de todo el país quedan integradas en una misma base de datos pudiendo

⁴³ García Fanlo, Luis (2014). Gestión de la identidad y procesos de subjetivación en la Argentina actual (2001-2013). *Revista Trazos universitarios*, pp. 9-10.

⁴⁴ Id.p.14.

⁴⁵ Siri, Laura (2015, mayo 13-15). El Documento Nacional de Identidad Argentino: una “caja negra” y una política de veridicción. III Simposio Internacional LAVITS Vigilancia, Tecnopolíticas y Territorios. Río de Janeiro, Brasil.

efectuar un mayor control de los ciudadanos con prontuario y protegiendo la identidad del resto de la ciudadanía”⁴⁶.

Las razones de seguridad y prevención del delito planteadas no son las únicas y las posibilidades tecnológicas del sistema implementado no se agotan ahí. Según el mismo video, la alta tecnología del sistema permitirá integrar no sólo los datos biométricos y domiciliarios sino que, en una etapa superadora, se podrá incorporar datos de voz, iris ocular e incluso del ADN.

Por otra parte y tal como se desarrolló en el capítulo anterior, el ministro Florencio Randazzo planteó en junio de 2014 una profundización de la política de identificación personal, a partir de la incorporación de un segundo chip en el DNI (el primero correspondía a la lectura de los datos biométricos), que permitirá incluir la historia clínica, datos previsionales y jubilatorios así como también la información de trayectos de la tarjeta del Sistema Único de Boleto Electrónico (SUBE)⁴⁷.

De esta manera, el actual documento se convertirá en un DNI inteligente multipropósito que, según la autoridad oficial, “se transformará en una tarjeta que permitirá no sólo garantizar la identidad como hasta ahora, sino interactuar con servicios públicos y privados como ocurre en los países más desarrollados en esta materia”⁴⁸. Además, se destacó también una supuesta comodidad para el ciudadano al simplificar la tarea de portar numerosas identificaciones y diversos papeles, y el ahorro de tiempo al momento de realizar los trámites.

Gracias a estas innovaciones tecnológicas, el potencial documento de identidad puede funcionar como un verdadero ‘panóptico de bolsillo’, permitiendo la trazabilidad de las personas que lo portan y posibilitando el control absoluto de todos sus movimientos. Al respecto, en el marco de una entrevista personal realizada al sociólogo Andrés Pérez Esquivel, expresó: “El segundo chip incluido en el DNI, al igual que el de la tarjeta SUBE, permite la trazabilidad y como la normativa nacional nos obliga a llevarlo en

⁴⁶ Conozca SIBIOS: La masiva y Orwelliana base de datos biométrica de Argentina (2013, octubre 28). *El Nuevo despertar*. Recuperado el 10 de diciembre de 2014, de <https://elnuevodespertar.wordpress.com/2013/10/28/conozca-sibios-la-masiva-y-orwelliana-base-de-datos-biometrica-de-argentina/>

⁴⁷ Inicialmente, cada tarjeta del SUBE se encontraba asociada al número de documento del portador y otros datos personales que eran exigidos al momento de tramitarla. Si bien esta información ya no es condicionante para la obtención de dicho boleto electrónico no biométrico, existen incentivos para que el portador registre sus datos personales. Este sistema permitió al Estado la confección de una detallada base de datos de los usuarios así como el historial de sus desplazamientos.

⁴⁸ Randazzo promete DNI inteligente (2014, junio 27). *Clarín*. Recuperado el 10 de abril de 2015, de http://www.clarin.com/sociedad/Randazzo-promete-DNI-inteligente-viene_0_1164483877.html

todo momento, tenemos un problema (...) Es cuestión de que avance un poco la tecnología para que uno esté viajando, use la tarjeta SUBE y, al mismo tiempo, si hay una comunicación directa en tiempo real y surge una alerta, debido a que la tarjeta ya está marcada e identificada con el nombre, se empieza a realizar el seguimiento con la cámara. En cuanto a estas, hay que esperar que avance un poco más la tecnología para que se realice el reconocimiento facial”⁴⁹.

A raíz de estas potencialidades, se puede plantear que este tipo de documentación conformará una futura representación metonímica de los individuos, ya que se tratará de una tácita e involuntaria biografía de las personas que contará con los más variados datos inscriptos y sus interacciones diarias. Al respecto, Carmen Romero Bachiller en su texto “Documentos y otras extensiones protésicas, o como apuntalar la ‘identidad’” realiza un interesante análisis: “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. Los documentos de identidad/identificación pasan a convertirse en los habilitadores y garantes de verdad ‘humana’ de los ‘sujetos-cuerpo-ciudadanos’ que los ostentan (...) Las personas concretas quedan reducidas a esas extensiones protésicas que son sus documentos de identidad, que las enrolan en regímenes concretos de cuerpos y objetos, que son reactualizados con cada interpelación a la identificación y con los reconocimientos que posibilita”⁵⁰.

Ahora bien, la posibilidad de contar con un DNI inteligente multipropósito trae aparejado ciertos inconvenientes. Por un lado, si se produce una falla en el sistema o se logra vulnerarlo, se podría usurpar identidades y acceder a un enorme caudal de información vinculada a la salud, aportes, consumos, viajes en transporte público y demás, dando lugar a cualquier tipo de especulaciones y negocios ilícitos.

Por otro lado, contar con toda esa información en una misma tarjeta puede resultar peligroso a la hora de realizar interacciones con el Estado, ya que un funcionario o agente podría acceder a datos ajenos a la operación a realizar generándose posibles actitudes o situaciones discriminatorias, abusos de autoridad, comportamientos discrecionales y violaciones a la privacidad, temas que se desarrollarán en el próximo capítulo.

⁴⁹ Entrevista con Andrés Pérez Esquivel realizada en Buenos Aires el 23 de septiembre de 2015.

⁵⁰ Romero Bachiller, Carmen (2008). Documentos y otras extensiones protésicas, o como apuntalar la ‘identidad’. *Política y Sociedad*, 45 (3). pp. 141-152.

Otra de las supuestas virtudes destacadas por los impulsores de este tipo de dispositivo se relaciona con el avance tecnológico y las innovaciones técnicas que este implica, colocando a la Argentina a la vanguardia en dicha materia. Pese a esto, desde la administración nacional no se manifestó la necesidad de un análisis previo respecto del impacto que este tipo de medidas puede implicar en los derechos de los ciudadanos.

Siguiendo el análisis planteado por Laura Siri⁵¹ sobre el DNI electrónico, el potencial para intimidar, reprimir y restringir libertades que posee así como la pérdida de privacidad y seguridad personal se encuentra “cajanegrizado”.

Este concepto es tomado del filósofo y antropólogo Bruno Latour, quien recupera la expresión “cajanegrización” de la sociología de la ciencia y la define como “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 sólo 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” (2001:362).

De esta manera, se puede plantear que el Nuevo DNI como dispositivo se cajanegriza, es decir, se evita problematizar sobre su contenido y se invisibiliza sus posibles riesgos y amenazas debido al éxito en cuanto a su supuesta comodidad y rapidez en la tramitación. Al respecto, Carmen Romero Bachiller recupera el concepto acuñado por Latour y sostiene: “(...) elementos tecnológicos como los documentos de identidad, en tanto convenciones legales nacionales e internacionales inscriptas y solidificadas en objetos capaces de circular -pequeñas tarjetas plastificadas, pasaportes, fotografías, firmas, sellos, etc.-, se constituyen en auténticas ‘cajas negras’ no cuestionadas, que se emplean cotidianamente en la consolidación de una articulación específica de la sociedad en la que se inscriben”⁵².

Posiblemente, el futuro DNI electrónico argentino se descajanegrizaría si se avivara y cobrara masiva repercusión el debate público sobre el tema, invitando a la ciudadanía en su conjunto a reflexionar sobre la violación a la privacidad, los riesgos en la seguridad y la privación de ciertas libertades civiles, interpelándola para que sea más conciente y activa en el ejercicio de la cultura cívica y en la defensa de sus derechos vulnerados.

⁵¹ Siri, Laura (2015, mayo 13-15). El Documento Nacional de Identidad Argentino: una “caja negra” y una política de veridicción. III Simposio Internacional LAVITS Vigilancia, Tecnopolíticas y Territorios. Río de Janeiro, Brasil.

⁵² Romero Bachiller, Carmen (2008). Documentos y otras extensiones protésicas, o como apuntalar la ‘identidad’. *Política y Sociedad*, 45 (3). p. 148.

Capítulo 4

Derechos, tácticas y garantías frente a la vigilancia estatal

4.1-El (E)estado de control

“Es mi última visita a Argentina. El próximo lunes, saldré del país y, sin un milagro, nunca más lo veré”⁵³, declaró a mediados de 2012 Richard Stallman, uno de los impulsores del software libre y pensador clave sobre las tensiones que genera la tecnología, tras recibir la noticia de la creación del sistema de identificación SIBIOS.

Con esta decisión y manifestación de protesta, Stallman evitó someterse al invasivo procedimiento y se opuso al mecanismo de control creado por el Estado argentino. “Hay injusticias que debemos resistir aunque cueste. No doy mis huellas dactilares; sólo pueden sacarlas con fuerza. Si un país me las exige, no voy (...) La injusticia de exigir datos biométricos a los visitantes se originó, como tanto mal, en los Estados Unidos (...) Hay mucha tendencia a la vigilancia en la Argentina actual”⁵⁴, expresó en esa misma oportunidad.

Desde la creación del Sistema Federal de Identificación Biométrica para la Seguridad (SIBIOS), que incluye -entre otras bases de datos- la información recabada de los documentos de identidad, ciertas voces críticas no se hicieron esperar. La disconformidad manifestada por el referente de la información y la tecnología con la que abre este apartado no representa la única voz de alarma.

Es que a lo largo de la historia, el Estado moderno avanzó sobre el control de la población con el pretexto de protegerla de acciones externas e intimidaciones, reforzando así los mecanismos de rastreo y monitoreo. Con la explosión de las nuevas tecnologías, cada vez más universalizantes, la puesta en funcionamiento de un conjunto de nuevos sistemas de seguridad conformado por dispositivos más sofisticados y precisos se transformó en una práctica habitual y efectiva pero, a la vez, por demás coercitiva. Los riesgos y amenazas que trae aparejada esta red de vigilancia son también más complejos y peligrosos. “Las rápidas transformaciones que hemos presenciado en los sistemas sociotécnicos, causadas por la tecnología de computación e información, con frecuencia han impuesto cambios a personas y sociedades sin una cuidadosa

⁵³ Stallman, Richard (2012, 7 de junio). Mi última visita a la Argentina. *Fundación Vía Libre*. Recuperado del 27 de agosto de 2015, de <http://www.vialibre.org.ar/2012/06/07/mi-ultima-visita-a-argentina/>

⁵⁴ Id.

evaluación de perjuicios y beneficios, de perturbación de valores sociales y culturales, y de si esos cambios son necesarios o deseados, por quién”, afirma Helen Nissenbaum en su libro *Privacidad amenazada. Tecnología, política y la integridad de la vida social* (2011:163), en consonancia a lo planteado.

La recolección compulsiva de datos personales impulsada por el Estado argentino permite la confección de una gran base de información, a partir de la cual todos los individuos se encuentran fichados e identificados. Esto pone en riesgo la privacidad de las personas y atenta contra sus libertades civiles así como también vulnera ciertos derechos básicos.

La filósofa especializada en medios de comunicación y políticas de la tecnología, Helen Nissenbaum, sostiene que “la captura y análisis de información personal ha provocado ansiedad por sus amenazas a la privacidad y sigue siendo una fuente de quejas, protestas y resistencias continuas” (2011:63). Asimismo, la autora asegura que la informática es concebida como una gran amenaza para la privacidad porque posibilita la vigilancia omnipresente, por lo que se vuelve necesario una reforma legal y política para garantizarla. Esto no significa restringir el flujo de la información sino asegurarse que fluya apropiadamente.

La mencionada base nacional de datos en manos de las fuerzas de seguridad que tiene el potencial de identificar en tiempo real, de forma automatizable y con efectos retroactivos a cualquier persona a través de las múltiples cámaras de videovigilancia diseminadas en el espacio público, que permite en forma indetectable e ineludible el reconocimiento biométrico y el seguimiento de todos los habitantes del país, posibilita la conformación de un Estado todopoderoso y omnipresente, lo que genera una situación de vigilancia permanente e ilimitada. En este contexto, resonantes se vuelven las palabras de Julian Assange, fundador del sitio web WikiLeaks, al referirse a las medidas de identificación lanzadas por el país: “Argentina tiene el régimen de vigilancia más agresivo de América Latina”⁵⁵.

A raíz de lo analizado, se puede afirmar que el presagio anunciado por Nissenbaum ya es una realidad en este país: “En el período previo a la propagación de esas tecnologías digitales de información, la gente podía contar con que pasaría inadvertida y no reconocida en espacios públicos; podía contar con el desinterés de los miles de detalles dispersos acerca de ella (...) Pero en poder de tecnologías digitales de información, los

⁵⁵ Assange: “Argentina tiene la vigilancia más agresiva de América Latina” (2013, junio 27). *Infobae*. Recuperado el 27 de agosto de 2015, de <http://www.infobae.com/2013/06/27/717385-assange-argentina-tiene-la-vigilancia-mas-agresiva-america-latina>.

observadores podrían coordinarse: interconectar sistemas de cámaras de video, y almacenar y analizar secuencias en un punto central, donde se les podría registrar y asociar con registros pasados” (2011:123-124).

4.2-La mirada vigilante

La sociedad avanza raudamente en la incorporación de tecnologías de información que aportan versatilidad en sus múltiples funciones y posibilitan transformar en registrable lo que hasta hace un tiempo no lo era. Bajo este estado de vigilancia y control permanente, el cuerpo social se organiza a partir de las premisas de la doctrina de la seguridad, transformándose en una sociedad menos segura en términos de derechos ciudadanos. Célida Godina Herrera en su artículo “El panóptico moderno” sostiene que “todo pasa por la mirada de la vigilancia (...) La vigilancia es el discurso que pretende dar legitimidad al ejercicio del poder. En otras palabras, la vigilancia como discurso legitimador del poder”⁵⁶. Por su parte, el sociólogo David Lyon analiza el fenómeno de la vigilancia basada en el procesamiento de la información y asegura: “La vigilancia ocurre cuando las organizaciones prestan atención, de manera rutinaria y sistemática, a los datos personales. 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 nuevos sistemas digitales representan un salto cualitativo comparado con los viejos sistemas de archivos físicos” (2009:5-6).

De esta manera, los avances informáticos implementados en nuevos métodos de vigilancia transforman las relaciones sociales e interpersonales, lo que produce importantes cambios en las prácticas de los individuos y, por ende, en sus propias subjetividades. Jacob Bañuelos en su artículo “Videovigilancia en la sociedad panóptica contemporánea” apunta que “el desenvolvimiento de la vigilancia en el actual Estado-Nación y el desarrollo de las nuevas tecnologías digitales son factores fundamentales para comprender la vigilancia contemporánea. La vigilancia en términos de Gilles Deleuze es un montaje y ha dejado de ser una práctica discreta de tecnologías

⁵⁶ Godina Herrera, Célida (2006, julio). El panóptico moderno. *A Parte Rei Revista de Filosofía*, 46, p.9.

específicas. Esta maquinaria de la visión trastoca igualmente la idea de privacidad. Vida pública, vida privada e intimidad son términos que se confunden y se pierden bajo estas circunstancias (...) La vigilancia panóptica lo trastoca todo, confunde lo público con lo privado (y viceversa), lo privado con lo íntimo, y finalmente lo íntimo con lo público”⁵⁷.

Retomando el concepto de poder planteado por Foucault y desarrollado en el capítulo 1, en esta situación de vigilancia permanente donde los límites entre las esferas mencionadas son cada vez más difusos, opera un poder que logra invisibilizarse y volverse más efectivo, modificando o, incluso, forjando la propia subjetividad de los individuos. Al ser concientes de estar siendo observados, se genera un determinado impacto psicológico y social por lo que las conductas y comportamientos se modifican o se falsean; esa mirada constante tiende a producir efectos inhibitorios o coercitivos por lo que resulta también una herramienta para asegurar el cumplimiento de las normas sociales. Funciona una forma de poder que no sólo domina y oprime, sino que forma; se trata de una mirada que recae e impacta en el cuerpo y que no sólo es controladora sino también subjetivadora en su repetición.

En relación a esto, Nissenbaum plantea una posible relación causal entre privacidad y autonomía debido a que la mirada del otro constituye y, a la vez, condiciona la propia subjetividad. El conocimiento de los actos de un sujeto por parte de los demás puede restringir, acotar o modificar su accionar de múltiples maneras: “El acceso irrestricto a la información puede frustrar directamente la autodeterminación de muchas maneras. Al buscar la aprobación y tratar de evitar la reprobación, la gente puede sentirse compelida a actuar de cierto modo; mientras seamos observados, monitoreados y posiblemente juzgados, y tomemos en cuenta a los demás al determinar cursos de acción y decisiones, nuestros actos no serán verdaderamente voluntarios. Pero también existen efectos disciplinarios indirectos que sabemos incorporados a la noción fundamental de panóptico; porque aunque no sepamos si se nos observa o no, debemos actuar como si se nos observara. Cuando esto ocurre, cuando hemos interiorizado la mirada de los observadores y nos vemos a través de sus ojos, actuamos según sus principios, no los nuestros. Sin embargo, los efectos panópticos podrían ser aún más insidiosos, y producir una disminución de nuestra capacidad para formular principios, planes y deseos con los que nos identificamos de verdad” (2011:92).

⁵⁷ Bañuelos, Jacob (2003, febrero-marzo). Videovigilancia en la sociedad panóptica contemporánea. *Razón y Palabra*, 31.p.9.

4.3-Privacidad e intimidad

El concepto de privacidad, defendido y rescatado por aquellos detractores de estos sistemas vigilantes e invasivos, suele confundirse con el de intimidad. En el artículo “Fenomenología de la intimidad; aproximación jurídica y ontológica a los conceptos de intimidad y privacidad”⁵⁸, Liliana Vásquez Rocca diferencia y explica estas dos nociones. Mientras que la intimidad se relaciona con lo más cercano y profundo del alma humana, la privacidad se refiere a lo personal y particular, es decir, aquello que se mantiene alejado del público y se halla libre de intromisión. “La intimidad es el conjunto de sentimientos, pensamientos e inclinaciones más internos -la ideología, la religión o las creencias-, las tendencias personales que deseamos mantener en total secreto (...) La privacidad, por su parte, es el ámbito de la persona formado por su vida familiar, sus aficiones, sus bienes particulares y sus actividades personales, alejadas de su faceta profesional o pública. Todos estos aspectos, además de los íntimos, constituyen una esfera de la vida que se tiene derecho a proteger de cualquier intromisión”⁵⁹. La autora sostiene que el ámbito de la intimidad forma parte de la privacidad pero no a la inversa, y asegura que la intimidad es una necesidad primordial en el desarrollo de la persona, mientras que la esfera privada “será pasto de toda suerte de desmanes a no ser que esté legalmente protegida”⁶⁰. Esta necesidad de amparo se relaciona con el planteo de Helen Nissenbaum, quien afirma que “la privacidad merece que se la tome en serio porque se cuenta entre los derechos, deberes o valores de todo sistema social y político moralmente legítimo” (2011:78).

Frente al potencial invasivo de las nuevas tecnologías que tienen capacidades de almacenamiento, procesamiento, difusión y utilización de informaciones personales en el ámbito telemático, surge la necesidad de repensar y reformular el derecho a la intimidad y la privacidad, junto a la demanda de nuevos mecanismos de protección para responder a los nuevos desafíos que trae consigo la proliferación de tecnologías de información y comunicación.

En relación a los riesgos que despiertan las nuevas modalidades tecnológicas, Isabel Lucena Cid en su texto “La protección de la intimidad en la era tecnológica: hacia una

⁵⁸ Vásquez Roca, Liliana (2007). Fenomenología de la intimidad; aproximación jurídica y ontológica a los conceptos de intimidad y privacidad. *Psikeba: Revista de Psicoanálisis y Estudios Culturales*, 5.

⁵⁹ Id.p.3.

⁶⁰ Id.p.4.

reconceptualización”, sostiene que “la función del derecho a la intimidad es la de proteger frente a cualquier invasión que pueda realizarse en aquel ámbito de la vida personal y familiar que el individuo desea excluir del conocimiento ajeno y de las intromisiones de terceros en contra de su voluntad, pero no sólo en el espacio físico sino en el ciberespacio, donde se pierde el sentido tradicional de la territorialidad y donde es más difícil establecer fronteras de protección”⁶¹.

Por su parte, el fundador de TeachPrivacy -empresa que ofrece programas de privacidad y seguridad de datos- y especialista en la temática, Daniel Solove explica que existe “una imposibilidad de definir la privacidad de manera satisfactoria y concluyente, ya que ésta no tiene una esencia singular o denominador común; en otras palabras, no se le puede dar un carácter universal y abstracto”⁶². Según su opinión, el valor de la privacidad depende de la importancia social que las distintas actividades proporcionan por lo que no se la puede interpretar de manera uniforme en todas las circunstancias. Por ello plantea una clasificación diferenciada en cuatro grupos de actividades susceptibles de menoscabar la privacidad: recopilación, procesamiento de información, diseminación e invasión.

Por otra parte vale aclarar que en casi todos los Estados se reconoce y protege el derecho a la intimidad, pero la extensión de su tutela varía en cada país. En la Argentina, el artículo 19 de la Constitución Nacional ofrece garantías al respecto, refiriéndose de forma explícita a dicha cuestión: “Las acciones privadas de los hombres que de ningún modo ofendan al orden y a la moral pública, ni perjudiquen a un tercero, están sólo reservadas a Dios, y exentas de la autoridad de los magistrados. Ningún habitante de la Nación será obligado a hacer lo que no manda la ley, ni privado de lo que ella no prohíbe”⁶³.

4.4-Autodeterminación informativa

El derecho a la intimidad reconocido por la Carta Magna y sobre el que parece avanzar el Estado con la implementación de los mecanismos de identificación analizados, converge con la protección de datos personales que se encuentra garantizada a través de la acción de hábeas data incorporada en el artículo 43, tercer párrafo, de la Constitución Nacional, en oportunidad de la reforma constitucional de 1994.

⁶¹ Lucena Cid, Isabel (2012). La protección de la intimidad en la era tecnológica: hacia una reconceptualización. *Revista Internacional de Pensamiento Político*, I Época, (7), pp. 134-135.

⁶² Id.p.137.

⁶³ Constitución de la Nacional Argentina, art. 19.

Posteriormente, en el año 2000 se sanciona y promulga la Ley N° 25.326 de Protección de Datos Personales, norma de orden público que regula los principios aplicables en la materia, así como también el procedimiento de la acción de hábeas data cuando corresponda la jurisdicción federal. Dicha normativa establece una serie de principios y pautas para la recolección, cesión y transferencia de los datos personales con el fin de proteger a sus respectivos titulares.

Los datos personales son aquellos elementos que identifican de manera directa e indirecta a un individuo en una sociedad. Según la definición del artículo 2° de la ley en cuestión, se trata de “información de cualquier tipo referida a personas físicas o de existencia ideal determinadas o determinables”⁶⁴.

En el texto “Principios Nacionales e Internacionales en el marco de la Protección de Datos Personales. Deficiencias. Recomendaciones”⁶⁵ de María Eugenia Piccirilli, se realiza un interesante análisis del concepto de autodeterminación informativa. Por un lado, la autora lo define como el derecho del individuo a elegir qué tipo y cantidad de su información personal puede ser procesada por un tercero. Se trata de la posibilidad que tiene el titular de los datos personales de ejercer el control sobre dicha información almacenada en medios informáticos tanto por las administraciones públicas como entidades u organizaciones privadas, y de controlar quiénes serán destinatarios de esos datos y qué uso les darán. Por otra parte, Piccirilli asegura que dicho concepto converge con el derecho a la privacidad, a la autonomía individual, al acceso de información y al derecho de rectificación, supresión y actualización.

La autodeterminación informativa implica que sin la información necesaria el titular no sólo está vedado de ejercer su derecho de rectificación o supresión sino que resulta menoscabado en su derecho a la autonomía individual. Esto se debe a que si la persona no cuenta con la información adecuada sobre qué bases poseen sus datos y la identificación de sus responsables, no tiene posibilidad de solicitar el acceso a aquellos registros para poder evaluar si reúnen características de calidad, es decir, si son adecuados, exactos, pertinentes, no exceden la finalidad con la cual se recolectaron, etc. En relación a esto, Piccirilli recupera el extracto de una sentencia judicial que sostiene:

⁶⁴ Ley N° 25.326 de Protección de Datos Personales. Boletín Oficial, Buenos Aires, Argentina, 30 de octubre de 2000.

⁶⁵ Piccirilli, María Eugenia (s.f). Principios Nacionales e Internacionales en el marco de la Protección de Datos Personales. Deficiencias. Recomendaciones. *Tensiones que genera la aplicación de las Tecnologías de la Información y las Comunicaciones (TICs) y los derechos a la protección de datos personales, intimidad e imagen*. Proyecto de Investigación UBACYT. Programación científica 2014-2016.

“Si un ciudadano no tiene información sobre quién ha obtenido información sobre él, qué tipo de información y con qué medios la ha obtenido, ya no podrá participar en la vida pública sin miedo”. (Sentencia del 15/12/1983 Tribunal Constitucional Alemán. Ref. 1 BvR 209/83)⁶⁶ (Id.).

De este modo, la autora explica que el derecho a la información es esencial para la protección de los datos personales, la privacidad, la intimidad, la autonomía individual y la autodeterminación informativa, que no sólo se desprenden de la Carta Magna sino que también son reconocidos por la Convención Americana de Derechos Humanos, la Declaración Universal de Derechos Humanos, así como en diversos tratados internacionales y regionales.

Claramente, esto pone en jaque la conformación de una gran base de datos que está llevando a cabo el Estado argentino a partir del SIBIOS, la recopilación compulsiva de información, el entrecruzamiento de datos, los medios utilizados para obtener dicha información identificatoria y las futuras potencialidades del sistema, ya que todo ello representa una contradicción con las garantías y derechos constitucionales consagrados en la Constitución Nacional.

Por otra parte, es importante destacar que la Ley N° 25.326 de Protección de Datos Personales data del año 2000, mientras que los cambios tecnológicos que incluyen el uso de biometría implementados en el Nuevo DNI se llevaron a cabo en 2009 y la puesta en funcionamiento del Sistema Federal de Identificación Biométrica es de fines de 2011. Esto quiere decir que, posiblemente, ciertas situaciones e implicancias de los nuevos sistemas de información no se encuentran contempladas ni se ajustan a la correspondiente normativa. Al respecto, en la jornada *Te estamos vigilando*, la integrante de la Asociación por los Derechos Civiles Valeria Milanés, expresó que “es sabido que las leyes tienen un ciclo de revisión muy largo, si es que lo tienen, y en el caso de las tecnologías, la revisión debe ser permanente porque se desarrollan a una velocidad que deja atrás los métodos normales de actualización de datos”⁶⁷. Similar planteo realiza Helen Nissenbaum a la hora de explicar la relación entre tecnología y privacidad así como también las razones que impulsaron la escritura de su obra *Privacidad amenazada. Tecnología, política y la integridad de la vida social*: “Este libro fue motivado por el desafío de los sistemas y prácticas sociotécnicos que han

⁶⁶ Id.

⁶⁷ *Te estamos vigilando* (2015, diciembre 2). Jornada organizada por la Asociación por los Derechos Civiles, Argentina.

alterado radicalmente el flujo de la información en las sociedades, y afectado por tanto a instituciones, estructuras de poder, relaciones y demás. Las concepciones de la privacidad que habían sido adecuadas hasta ahora, son incapaces ya, en mi opinión, de adaptarse al nuevo panorama, por su escasa aptitud para ajustarse al ir y venir de las ansiedades que esos sistemas y prácticas provocan” (2011:151).

4.5-Una relación asimétrica

La conformación y administración de esta base estatal de datos coloca al Estado en una privilegiada posición de poder y, por ende, de desigualdad respecto a la ciudadanía. Esta situación puede dar lugar a todo tipo de irregularidades, a partir de las cuales el actor social perjudicado resulta ser la población, ya que no dispone de los mismos o suficientes medios y herramientas para evitar posibles abusos o avances sobre sus derechos ni la posibilidad de fiscalizar a quienes la controlan. Como sostienen Zygmunt Bauman y David Lyon en *Vigilancia líquida*, “la nueva vigilancia, basada en el procesamiento de la información, más que en lo que afirmaba Foucault, permite una nueva transparencia en la que no solamente los ciudadanos como tal sino todos nosotros, en cada uno de los roles que asumimos en nuestra vida cotidiana, somos constantemente controlados, observados, examinados, evaluados, valorados y juzgados. Pero no ocurre lo mismo en el sentido contrario. A medida que los detalles de nuestra vida cotidiana se hacen más transparentes para los organismos que nos vigilan, más difícil resulta discernir cuáles son sus propias actividades. A medida que el poder se mueve con la velocidad de las señales electrónicas en la fluidez de la modernidad líquida, el grado de transparencia crece para unos y disminuye para otros” (2013:20-21). Por otro lado, esta relación asimétrica se pone en evidencia a partir de las técnicas biométricas utilizadas para la recolección y almacenamiento de datos debido a que reducen a los individuos en dividualos, en términos de Deleuze, quien apunta que “los individuos se han convertido en ‘dividualos’, y las masas, en muestras, datos, mercados o bancos” (1999:3), ya que se toman rasgos únicos e irrepetibles, posibilitando la creación de perfilados sociales o especies de prontuarios de todos los sujetos. Según el miembro de la Asociación Pensamiento Penal y de la Red Latinoamericana para el Estudio de Vigilancia, Tecnología y Sociedad, Andrés Pérez Esquivel, “la utilidad de estos perfilados sociales puede tener fines de carácter social, comercial, policial e incluso militar. A nivel mundial, los principales interesados son las potencias militares, las agencias internacionales de seguridad como Interpol o entidades financieras como el

Banco Mundial, que están promoviendo bases y programas de identificación nacional en distintos países periféricos para usos múltiples y de modo experimental”⁶⁸.

De acuerdo al sociólogo argentino, la extracción y copia de datos biométricos de forma masiva y compulsiva es un paso clave para la conformación de las sociedades predelictivas o una instancia que permite habilitar el paradigma del policiamiento predictivo. Este se basa en la idea de que los Estados deben reunir toda la información disponible de la mayor cantidad de personas, a fin de combatir la delincuencia y abordar más fácilmente al sujeto que decida delinquir o en un futuro lo hiciera. Así, se produce un pasaje del estado de la prevención a la anticipación, lo cual no sólo afecta la presunción de inocencia al revertir la carga de la prueba, sino que atenta contra el derecho de la autodeterminación informativa sobre la propia biología, concepto que fue explicado más arriba.

Los postulados de Pérez Esquivel coinciden con la categorización de las sociedades del hipercontrol realizada por Bogard y con el imperativo de la previdencia planteado por Wajcman, ambas ideas desarrolladas en el capítulo 1. Asimismo, casi a modo ilustrativo, cabe mencionar el análisis sobre la previdencia que realiza el psicoanalista francés en su libro *El ojo absoluto* a partir del film *Minority Report* (2002) de Steven Spielberg, basado en una novela de Philip K. Dick (1956). Con un acertado slogan que reza ‘No puedes esconderte, el futuro te atrapa’, la película demuestra cómo la sociedad de vigilancia necesita castigar el delito antes de que se produzca, el mal de manera anticipada, prevenir el crimen hipotético, el pre-crimen como se denomina en la cinta, para lo cual se coloca a todos los individuos bajo vigilancia preventiva y se opera criminalizando potenciales delincuentes. “La historia de *Minority Report* inscribe la previdencia como un absoluto y de manera literal. Es el pensamiento de la época (...) Enuncia estrictamente que gobernar es pre-ver. Ver antes está en la lógica de verlo todo, incluso lo que todavía no se realizó” (2011:173), analiza Wajcman.

Otro punto de esta relación asimétrica entre el Estado y los individuos producto del uso estatal de tecnología para el registro y control de los ciudadanos, se evidencia en el hecho de que estos perfilados de peligrosidad o prontuarios de sujetos inocentes potencialmente sospechosos mencionados más arriba abarcan al conjunto de la población, con las consecuencias que esto conlleva. En relación a este planteo, en la jornada *El impacto de la recolección obligatoria de información biométrica por parte*

⁶⁸ Tecnología, vigilancia y derechos personalísimos (2015, agosto19). Jornada organizada por la Carrera de Especialización en la Facultad de Derecho de la Universidad de Buenos Aires, Argentina.

del Estado, en los derechos humanos, la abogada y presidenta de la fundación polaca Panoptykon, Katarzyna Szymielewicz, expresó: “El mayor cambio que estamos viendo es que incluso ciudadanos libres que tienen una buena relación con el Estado y que no son sujetos de ningún tipo de sospechas, son objeto de recolección de datos biométricos. Los Estados modernos deben darles a los ciudadanos la opción de elegir, debe existir un libre intercambio en el cual el ciudadano tenga la opción de no entregar los datos”⁶⁹.

Pese a esto, en la Argentina no existe esta posibilidad por lo que todos los individuos se encuentran incluidos en esa gran base de datos, lo que puede dar lugar a políticas de registro y clasificación de personas, mediante las cuales se tracen comparaciones o se generen segmentaciones a partir de múltiples criterios como niveles socioeconómico, educativo, ingresos, entre otros. Estas posibles categorías de sujetos violan el principio de recibir un trato justo y equitativo así como también las garantías constitucionales que resguardan la igualdad ante la ley y la posibilidad de gozar autonomía y libertad, propias de un sistema democrático. Si bien la Ley N° 25.326 de Protección de Datos Personales citada anteriormente, en su artículo 7.3 establece que “queda prohibida la formación de archivos, bancos o registros que almacenen información que directa o indirectamente revele datos sensibles”⁷⁰, los cuales -según la propia normativa- se definen como aquellos “datos personales que revelan origen racial y étnico, opiniones políticas, convicciones religiosas, filosóficas o morales, afiliación sindical e información referente a la salud o a la vida sexual”⁷¹, limita la situación planteada no quedan exentos otros tipos de clasificaciones.

De igual manera, posibles abusos o usos arbitrarios en la administración y aplicación de los datos reunidos en el sistema de identificación biométrica deja expuesta la asimetría anteriormente planteada. Por ejemplo, en aquellos casos relacionados con la distribución de derechos, acceso a recursos, asignación de beneficios o planes sociales y aplicación de penalidades, lo cual quebranta principios de igualdad y equidad.

Vale aclarar que los mencionados riesgos y amenazas de estas innovaciones tecnológicas en materia identificatoria se pensaron en un contexto democrático. Resulta casi una obviedad agregar que estas políticas de registro masivo así como la construcción de una base de datos centralizada en poder de un gobierno de régimen

⁶⁹ El impacto de la recolección obligatoria de información biométrica por parte del Estado, en los Derechos Humanos (2014, noviembre 20). Jornada organizada por El Observatorio de Género y Derechos Humanos de los Bloques Legislativos Nacionales de la UCR y la Fundación Vía Libre, Argentina.

⁷⁰ Ley N° 25.326, artículo 7.3.

⁷¹ Id., artículo 2.

autoritario, aumentarían enormemente los peligros y podrían dar lugar a todo tipo de persecuciones, represión y muerte. “No sabemos si en diez años puede cambiar la perspectiva sociopolítica y haya un gobierno que decida discriminar, excluir o, incluso, eliminar a un grupo de la sociedad por distintas razones. Tenemos que colocar este tema en el centro de la discusión y advertir de los potenciales riesgos que existen porque, aunque no parece posible ahora, nunca se sabe cuando una dictadura o gobierno opresivo puede repetirse”⁷², aseguró Katarzyna Szymielewicz en la jornada citada.

4.6-Tácticas y estratégicas

Para pensar más profundamente esta relación asimétrica podemos recuperar ciertas categorías de análisis desarrolladas en *La invención de lo cotidiano I. Artes de hacer* por Michel De Certeau (1996), quien estudia las relaciones de dominación presentes en el campo cultural a partir de la teoría de la enunciación. Si bien su marco teórico escapa al objeto de estudio del presente trabajo, ciertos planteos resultan interesantes y pertinentes para su aplicación.

El autor da cuenta de las operaciones que realizan los usuarios, quienes no se configuran como individuos libres que toman decisiones sino que están condicionados por hallarse situados en ciertas posiciones, las cuales van a determinar sus subjetividades y, por ende, sus operaciones de producción. Para describir estas posiciones, De Certeau utiliza los términos de tácticas y estrategias de Sun Tzu, y sostiene que todo enfrenamiento se produce en un repertorio de esquemas complejos en donde las prácticas son entendidas como modos de hacer en contexto de lucha desigual por el poder entre dominantes y dominados.

Por un lado, denomina estrategia al cálculo de relaciones de fuerza que se hace posible a partir del momento en que un sujeto de voluntad y de poder resulta aislable de un ambiente. Se relaciona con el espacio que ocupa el dominante, una posición fuerte y poderosa que tiene dominio del tiempo y plantea relaciones con otros. En contraposición, llama táctica a la acción calculada que no puede contar con un lugar propio ni con una frontera que distinga al otro como una totalidad visible. La táctica no tiene más lugar que el del otro, es débil y no puede acumular fuerza para cambiar el sistema; se trata de la condición del dominado. Pese a esto, el autor asegura que desde

⁷² El impacto de la recolección obligatoria de información biométrica por parte del Estado, en los Derechos Humanos (2014, noviembre 20). Jornada organizada por El Observatorio de Género y Derechos Humanos de los Bloques Legislativos Nacionales de la UCR y la Fundación Vía Libre, Argentina.

esta posición existe la posibilidad de realizar ciertas prácticas de desvíos; son las argucias del débil frente al poderoso.

Con estas categorías teóricas podemos analizar la relación asimétrica entre el Estado en su rol de recolector de datos y los individuos como proveedores de información, a partir de la cual el primer actor social se ubica en una posición de productor de estrategias y la ciudadanía en el rol de creadora de tácticas.

El uso de la biometría en materia identificatoria con la correspondiente extracción de información biológica y social de las personas, posiciona al Estado -generador de estrategias- en un lugar susceptible de ser circunscrito como algo propio así como también concibe “un dominio de los lugares mediante la vista. La partición del espacio permite una práctica panóptica a partir de un lugar desde donde la mirada transforma las fuerzas extrañas en objetos que se pueden observar y medir, controlar por tanto e ‘incluir’ en su visión. Ver (de lejos) será también prever, adelantar el tiempo mediante la lectura en un espacio” (De Certeau, 1996:42-43).

Ahora bien, ante esta perspectiva panóptica y, consecuentemente, fuerte posición de poder, los individuos -generadores de tácticas- pueden efectuar ciertas ‘trampas’ para escapar ocasionalmente de este vínculo desigual. En relación a esto, el autor sostiene que “si es cierto que por todos lados se extiende y se precisa la cuadrícula de la ‘vigilancia’, resulta tanto más urgente señalar cómo una sociedad entera no se reduce a ella; qué procedimientos populares (también ‘minúsculos’ y cotidianos’) juegan con los mecanismos de la disciplina que y sólo se conforman con cambiarlos; en fin, qué ‘maneras de hacer’ forman la contrapartida, del lado de los consumidores (o ¿dominados?), de los procedimientos mudos que organizan el orden sociopolítico”⁷³ (1996:44).

Un ejemplo de ello es la situación relatada por Katarzyna Szymielewicz en la jornada anteriormente mencionada: “En ciertas ocasiones desapegarse de la identidad o modificar ciertos datos personales es válido, por ejemplo en la Alemania nazi algunas personas tuvieron que cambiar su identidad y reidentificarse de otro modo porque el Estado los perseguía. Quizás estoy planteando una apología de engañar al Estado pero no siempre se trata de una entidad buena y garante, ya que puede cambiar y tomar medidas agresivas contra sus propios ciudadanos, por lo tanto hay momentos en la

⁷³ Id.

historia en que engañar al Estado puede ser legítimo”⁷⁴. En consonancia, Agamben recuerda esta situación pasada y plantea un interrogante a futuro: “Las fotos que originalmente eran documentos de identidad o tarjetas profesionales, fueron las que permitieron a la policía nazi en los países ocupados localizar y registrar judíos, facilitando su deportación. ¿Qué ocurre cuando el poder despótico hace uso de los registros biométricos sobre una población entera?”⁷⁵.

La especialista polaca asegura que con el uso de tecnologías biométricas y el correspondiente pasaje de la simple identificación a una identificación basada en las características del cuerpo, se cierra esa “puerta de emergencia” utilizada por algunos judíos durante la Segunda Guerra Mundial, ya que no es una tarea sencilla cambiar la biología y el propio cuerpo a fin de modificar la identidad. En relación a esto, Agamben explica que a partir de este cambio, “la relación normal del Estado con lo que Rousseau llamó los ‘miembros del soberano’ será biométrica, es decir, de sospecha generalizada”⁷⁶.

Pese a esto, existen algunos otros casos de desvíos o escamoteos, en términos de De Certeau, que lograron superar este escollo. Un ejemplo de ello es la experiencia de un grupo de inmigrantes clandestinos que se pasan un tornillo al rojo vivo por todos los dedos de las manos. Con esta mutilación logran el objetivo de borrar sus propias huellas digitales para no ser fichados y detectados por la policía, situación retratada en el documental *Figuras de guerra* de 2010 (Qu'ils reposent en révolte), del director y guionista Sylvain George.

Sin intención de avalar acciones delictivas, se puede mencionar también el caso del narcotraficante colombiano apodado El Loco Barrera, quien realizó diversos procedimientos para disolver su identidad, tales como operaciones estéticas, uso de documentos falsos y el borrado de sus huellas dactilares, a fin de evadir la acción de la justicia. Finalmente fue capturado pero las autoridades no terminan de definir si el hombre apresado es, efectivamente, el delincuente buscado. Algunas versiones aseguran que Barrera continúa delinquiendo con otro nombre, diferente rostro y sin huellas digitales en sus manos.

⁷⁴ El impacto de la recolección obligatoria de información biométrica por parte del Estado, en los Derechos Humanos (2014, noviembre 20). Jornada organizada por El Observatorio de Género y Derechos Humanos de los Bloques Legislativos Nacionales de la UCR y la Fundación Vía Libre, Argentina.

⁷⁵ Agamben, Giorgio (2005, diciembre 5). No a la biometría. *Le Monde*.

⁷⁶ Id.

Desde esta posición las operaciones son mínimas, dispersas y fragmentarias, por ello consideramos necesario un mayor compromiso y responsabilidad por parte del actor más débil del vínculo Estado-ciudadanía, ya que si bien el primero se encarga de recolectar, almacenar y unificar los datos personales de todo el cuerpo social, en muchos casos los individuos vuelcan o entregan voluntariamente información y al ser advertidos de ciertos hipotéticos o probables daños, frente a la opción de beneficios concretos, optan por esta última. En relación a esto, Godina Herrera en “El panóptico moderno”, asegura: “La nueva fuerza de este panóptico moderno reside en la participación voluntaria de la gente gracias a sus beneficios y ventajas que puede apreciar, con lo cual es menos propensa a percibir los inconvenientes y las amenazas; por ejemplo el control que se ejerce sobre su libertad y la total pérdida de su vida privada. Los beneficios son directos, reales y tangibles mientras que los inconvenientes son menos tangibles, más indirectos y complejos”⁷⁷. En consonancia, Nissenbaum confirma que “en casi toda situación en que la gente tiene que elegir entre privacidad y casi cualquier otro bien, prefiere el otro bien (...) La gente elige las opciones que brindan comodidad, paso rápido, ahorros, conectividad y seguridad sobre las que ofrecen privacidad” (2011:112-113).

Sin bien es cierto que, como sostiene Deleuze, las sociedades disciplinarias eran máquinas extractoras de energía, mientras que las de control son extractoras de información, resulta fundamental la toma de conciencia y estar alertas al momento de intercambiar o proveer información. “Los datos son un recurso extraordinario, son una herramienta muy poderosa y una vez que nos desprendemos de éstos es difícil recuperarlos. Cuando esos datos están en manos de las corporaciones o el gobierno es muy dificultoso saber que va a pasar porque hemos perdido el lazo. Los datos son una parte fundamental del ser humano”⁷⁸, aseveró la especialista Katarzyna Szymielewicz. En consonancia pero con una perspectiva aún más global, Pérez Esquivel afirmó que “la protección de datos personales es cada día más un derecho de los pueblos”⁷⁹.

⁷⁷ Godina Herrera, Célida (2006, julio). El panóptico moderno. *A Parte Rei Revista de Filosofía*, 46, p.7.

⁷⁸ El impacto de la recolección obligatoria de información biométrica por parte del Estado, en los derechos humanos (2014, noviembre 20). Jornada organizada por El Observatorio de Género y Derechos Humanos de los Bloques Legislativos Nacionales de la UCR y la Fundación Vía Libre, Argentina.

⁷⁹ Entrevista con Andrés Pérez Esquivel realizada en Buenos Aires el 23 de septiembre de 2015.

Capítulo 5

Desprotección informativa y políticas de exclusión

5.1-Biometría y documentación

“Cuando participo de exposiciones, charlas o debates sobre tecnología y seguridad me preguntan, a menudo, acerca de la biometría y sus mitos y realidades. Lógicamente, y es atendible la confusión, algunos la consideran como el paradigma del panóptico, o en otras palabras; como un ejemplo de una tecnología de observación y trazabilidad”⁸⁰, sostiene Pedro Janices, consultor en tecnología, seguridad y biometría en un artículo publicado en la web oficial sobre el tema.

Para desarticular esta creencia, el consultor enumera una serie de puntos y observaciones, a la vez que asegura que la herramienta en cuestión no persigue esos fines y que los datos estrictamente biométricos que se manejan por Internet son escasos, de modo tal que no se pone en juego la violación de los datos personales o la privacidad de las personas.

Por otra parte apunta que, según las estadísticas y registros, los datos patronímicos o textos como nombres, domicilios, números de tarjetas de crédito, entre otros componen la información más perdida, robada o entregada y no sucede así con los datos biométricos.

Atendiendo a la preocupación de “los detractores de la biometría o de quienes argumentan sobre cierta condición panóptica de la herramienta”⁸¹, aconseja leer los acuerdos de confidencialidad de buscadores y aplicaciones al momento de entrega de información personal.

A la hora de analizar los posibles puntos que generan mayor resistencia en el uso de herramientas biométricas, el especialista Janices plantea tres cuestiones: la tecnología, la legislación y la costumbre. Respecto a la primera considera que no es un impedimento, ya que el desarrollo de la tecnología biométrica así como los instrumentos que garantizan su seguridad crecieron fuertemente en los últimos cinco años, en términos de avance e inversión.

⁸⁰ Janices, Pedro (2012, julio 03). Mitos y Realidades de la Biometría en Argentina. Biometría. Recuperado el 25 de junio de 2015, de <http://www.biometria.gov.ar/editoriales/2012/07/03/mitos-y-realidades-de-la-biometria-en-argentina.aspx>.

⁸¹ Id.

En cuanto a la categoría que denomina costumbres, el experto realiza un breve análisis que se pudo vincular con el concepto de *habitus* planteado por Pierre Bourdieu y desarrollado extensamente en el capítulo 3. En síntesis, plantea que los argentinos históricamente contaron con un documento de identificación (Libreta Cívica o la Libreta de Enrolamiento -según el sexo-, Cédula de Identidad, Documento Nacional de Identidad y Pasaporte) con datos, huellas dactilares y fotografías del rostro, lo que resulta una “metodología común”⁸², que se encuentra adaptada a la práctica y que no trae aparejada ningún tipo de resistencia.

Por último, se refiere a la Ley N° 17.671 de Identificación, Registro y Clasificación del Potencial Humano Nacional que rige desde 1968 y que tuvo numerosas modificaciones al día de hoy. Si bien Janices destaca esto como un hecho positivo que denota la “constante actualización” en cuanto a “los datos personales, documentos y la utilización de los medios digitales y biométricos con el fin de mejorar y asegurar la identificación”⁸³, se puede plantear que dicha normativa mantiene la matriz autoritaria propia del gobierno de facto a la que corresponde su sanción, como se desarrolló en los capítulos anteriores. Probablemente, plantear y diseñar un nuevo marco legal adecuado a la actualidad que se ajuste a los pertinentes cambios tecnológicos en la materia, con la previa discusión y correspondiente aprobación en el parlamento de la nación, resulta ser el camino más democrático.

Como esta opción no fue la que tomó y ejecutó el gobierno de turno, las modificaciones de la ley en cuestión permitieron que, de modo arbitrario y sin consenso, profundizaran los cambios en la materia. Fue así que en junio de 2014, el ministro Florencio Randazzo firma un convenio con la Real Casa de la Moneda de España para que el documento argentino incorpore más tecnología a partir de la implementación de un doble chip capaz de contener más y nueva información personal, tal como se explicó en los capítulos anteriores.

A raíz de estas modernas innovaciones y ante la escasa información al respecto brindada por los funcionarios de gobierno, ciertos actores sociales encendieron la alarma y procuraron interiorizarse en el tema. Fue así que el 28 de julio de 2014, el diputado nacional por la Unión Cívica Radical, Manuel Garrido, y el 26 de agosto del mismo año la Asociación Pensamiento Penal (APP) presentaron pedidos de informes ante el Poder Ejecutivo Nacional en el marco del Decreto N° 1.172/2003 de Acceso a la Información

⁸² Id.

⁸³ Id.

Pública, solicitando especificaciones acerca de los documentos electrónicos y el alcance de este proyecto. Ambas solicitudes fueron respondidas y firmadas por la directora Nacional del Renaper, Mora Arqueta.

5.2-Las explicaciones del Estado

Diferentes cuestiones destacan e intentan responder las fuentes oficiales en los documentos mencionados. Algunos extractos se reproducen de manera idéntica en ambos informes (ver anexo). Por un lado, se informa que el DNI electrónico posee dos chips. El primero contiene los datos de identificación del ciudadano, mediante un certificado de firma digital que permite confirmar la identidad digital en Internet, y el segundo corresponde a información complementaria del titular existente en distintas bases de datos y/o soportes físicos. Este último cuenta con tecnología RFID y tiene la función de interactuar con el Sistema Único de Boleto Electrónico (SUBE).

Por otra parte, se explica que el poseedor del documento puede autenticar su identidad en forma automática al momento de realizar ciertos trámites o transacciones en línea, lo que puede ser de gran utilidad para el ciudadano en su interacción con el Estado o en el uso de bienes y servicios públicos, permitiendo mayor simplicidad, practicidad y ahorro de tiempo.

Respecto al Estado, se afirma que con esta implementación resulta beneficiado debido a un uso más eficiente y el acceso seguro a información y datos que se encontraban dispersos, al tiempo que se ahorran recursos públicos que conlleva la unificación en un único soporte de credenciales y/o comprobantes emitidos a nombre de los ciudadanos en sus roles de usuarios de distintos servicios.

En cuanto a la obligatoriedad de la obtención de este tipo de documento, la información oficial asegura que aquellos ciudadanos que cuenten con alguna de las versiones anteriores del Nuevo DNI, no deben cambiar al nuevo formato. El costo de este es de 35 pesos y no se prevé una modificación de la tasa hasta el momento. Asimismo, se informa que la gestión, desarrollo y administración se realiza en forma directa y 100% estatal.

Respecto a la autoridad competente, se explicita que el Ministerio del Interior y Transporte, a través del Renaper, tiene a cargo la recolección, conservación, ordenación, almacenamiento, relacionamiento, evaluación, bloqueo, destrucción y procesamiento de los datos que contiene el Nuevo DNI; tareas realizada en forma directa e intransferible. Seguidamente, se aclara que la administración de datos que no son generados por dicha

cartera es responsabilidad de la autoridad de aplicación de esos datos y/o información, o del organismo o la entidad responsable de su generación.

En cuanto a las disposiciones de seguridad, se informa que esta innovación tecnológica consiste en dotar de mayores medidas de seguridad al DNI. Por lo tanto, resulta más eficiente en términos de seguridad debido a que la incorporación del segundo chip consiste en un nuevo elemento que reduce las posibilidades de falsificación o adulteración de documentos.

En otro tramo de uno de los informes, correspondiente a la respuesta enviada al diputado Manuel Garrido, se explica que se toman las mismas medidas de seguridad que existen para el almacenamiento de los datos de identificación de los ciudadanos existentes en los archivos y bases de datos del Renaper, así como igual tratamiento, restricción en su acceso y protección de datos personales que rige en el accionar de dicho organismo.

Por su parte, en el informe respondido a la Asociación Pensamiento Penal respecto a la misma cuestión, se afirma que el cambio previsto no guarda relación con posibles deficiencias en las medidas de seguridad que contiene el DNI, sino que consiste en una actualización tecnológica que sigue las tendencias de la mayoría de los países que cuentan con un sistema de identificación nacional y de documentación de sus ciudadanos.

Pese a las explicaciones brindadas por el Estado nacional respecto al Nuevo DNI, se percibe un detenimiento en el avance de las potencialidades en materia documentaria a partir de la implementación del segundo chip e, incluso, no se volvió a plantear el tema del documento electrónico en la agenda pública por las autoridades competentes. “Es muy destacable que el gobierno haya hecho silencio, ha sido prudente y no ha vuelto a mencionar el DNI electrónico, pero tampoco niega que se vaya a aplicar con lo cual el tema sigue latente (...) Creo que ha frenado un poco esta iniciativa”⁸⁴, opina Pérez Esquivel.

5.3-Filtraciones y descargas

Pese a las medidas de seguridad aludidas por el Ejecutivo, existieron en el pasado ciertas situaciones en las que se sorteó la protección referida y se vulneraron datos personales recabados en torno a cuestiones documentarias.

⁸⁴ Entrevista con Andrés Pérez Esquivel realizada en Buenos Aires el 23 de septiembre de 2015.

Un ejemplo de ello fue la descarga y recolección de las fotografías correspondientes al padrón electoral de la base de datos gubernamental. Mediante un simple código y en unas pocas horas, se pudo acceder a una de las carpetas del sitio oficial y generar la descarga automática de las imágenes que se encontraban allí junto a sus correspondientes números de DNI.

Este hecho dejó en evidencia la poca solidez de las barreras digitales para proteger la información personal de los ciudadanos en tutela de un organismo estatal. En relación a lo sucedido, el director Nacional Electoral, Alejandro Tullio, declaró a los medios de comunicación que las fotos se encuentran en los servidores de la Cámara Nacional Electoral (CNE), no bajo su área, y que están protegidos bajo los estándares de la Dirección General de Tecnología del Consejo de la Magistratura. Seguidamente explicó que la transferencia de las imágenes se realiza de manera electrónica, desde el Renaper hasta la CNE⁸⁵.

Previo a este hecho, la Asociación por los Derechos Civiles solicitó a la Justicia el retiro de las imágenes del sistema, al considerar que su presencia viola el derecho a la privacidad de las personas. Fue así que a través de una acción de hábeas data colectiva, la ONG hizo la petición ante el Juzgado Contencioso Administrativo Federal N° 4 de la Ciudad de Buenos Aires, a cargo de la magistrada Rita Ailán, para que se retire de manera inmediata la totalidad de las imágenes fotográficas de los ciudadanos y ciudadanas contenidas y exhibidas en el sitio de consulta oficial <http://padron.gob.ar/>⁸⁶. Por otra parte, representantes de la organización aseguraron que la difusión de las imágenes por Internet podrían ser utilizadas por terceros que las pueden compilar e integrar a bases de datos con fines comerciales e ilícitos.

Una polémica similar se generó al exponer en la red los registros de transacciones de los usuarios de la tarjeta SUBE tras una filtración generada por Anons.ar, un grupo de hackers argentinos que asegura ser miembro de Anonymous. Según esta agrupación, la exposición y publicación de estos movimientos en un sitio web⁸⁷ se realizó con el

⁸⁵ Fernández, Pablo Martín (2013, noviembre 04). Por una falla de seguridad se pueden descargar fotos del padrón electoral. *Infotechnology*. Recuperado el 08 de mayo de 2015, de <http://www.infotechnology.com/internet/Por-una-falla-de-seguridad-se-pueden-descargar-fotos-del-padrón-electoral-20131104-0001.html>

⁸⁶ Asociación por los Derechos Civiles (2013, octubre 22). La ADC pidió a la justicia que se retiren las fotos de los votantes del padrón electoral online. Recuperado el 10 de junio de 2015, de http://www.adc.org.ar/1045_la-adc-pidio-a-la-justicia-que-se-retiren-las-fotos-de-los-votantes-del-padrón-electoral-online/

⁸⁷ Anonymous (s.f). Todo lo que SUBE... tiene que BAJAR... Recuperado el 10 de octubre de 2015, de <http://pastehtml.com/view/bm5wlsazn.html>

objetivo de señalar la falta de medidas de seguridad para mantener a resguardo la información personal de los pasajeros.

Los medios de comunicación se hicieron eco de la cuestión y publicaron un extracto del comunicado que se adjuntó con el listado de las transacciones registradas. A modo de protesta contra el avance estatal en materia identificatoria, éste sostiene que “el gobierno argentino exige una identificación por DNI cuando no es necesaria, y luego rastrea cada uso de esta tarjeta, creando una base de datos del ir y venir de cada ciudadano”⁸⁸. Previo a este episodio, la organización Vía Libre había señalado como abusiva la recolección de datos por parte del Estado de los movimientos de los usuarios del sistema de transporte público.

A raíz de estas innovaciones y consecuentes filtraciones por esta política impulsada por el Estado, diversas organizaciones defensoras de las libertades civiles y los derechos humanos elaboraron y firmaron un documento, en el que manifiestan su disconformidad y preocupación por tales medidas. “El Estado argentino está creando llaves maestras de todos los ciudadanos que permiten su vigilancia y control en tiempo real y que, como si fuera poco, también se han mostrado vulnerables. Sin dudas esto representa un serio perjuicio para la seguridad democrática sea que esté en manos de un gobierno democrático, autoritario, o que sea filtrada por empresas u organizaciones criminales de cualquier tipo”⁸⁹, sostiene.

Paralelamente, un grupo político de jóvenes propuso intercambiar la tarjeta SUBE entre los usuarios para evitar el registro personal de viajes y que el gobierno controle los movimientos de los pasajeros. La iniciativa, planteada por miembros del Partido Liberal Libertario (PLL), consiste en un acto de resistencia al sistema electrónico de transporte que registra las acciones que cada pasajero realiza a través de trenes, colectivos y subtes.

“Nuestra propuesta es un acto de resistencia civil pacífica ante el abuso despótico del gobierno. Llamamos a la gente a que cambie la tarjeta, a que no se quede con la suya. Que se la den a un amigo o a un compañero de trabajo para que no sepan sus

⁸⁸ Exponen en la Red los registros de viajes de la tarjeta SUBE (2012, enero 30). *La Nación*. Recuperado el 08 de julio de 2015, de <http://www.lanacion.com.ar/1444623-exponen-en-la-red-los-registros-de-viajes-de-la-tarjeta-sube>.

⁸⁹ Los DNI electrónicos violan nuestros derechos (2014, octubre 06). Recuperado el 08 de julio de 2015, de <http://www.pensamientopenal.org.ar/dni/>

movimientos”⁹⁰, explicó el vocero de PLL a la prensa. “Si Anonymous tuvo acceso a los datos, también lo puede tener cualquier empresa privada y el Estado. No queremos darle al gobierno el gusto de tener a un clic de distancia la información de cada pasajero”⁹¹, sostuvo en relación a la filtración de los datos de SUBE desarrollada más arriba.

Si bien este tipo de acción no modifica el sistema de boleto electrónico implementado por el Estado y el consecuente registro de movimientos de pasajeros, puede considerarse una táctica -en términos de De Certeau y según el análisis desarrollado en el capítulo 4-; se trata de una práctica de desvío frente a la estrategia del poderoso, que si bien es endeble y no puede acumular fuerza para cambiar el sistema, es la posibilidad que tiene aquel que ocupa la posición más débil. “Lo cotidiano se inventa con mil maneras de cazar furtivamente” (1996:42), apunta el autor.

Otro ejemplo de este tipo de filtraciones fue llevado a cabo en 2009 por un grupo de hackers alemanes, conocidos como The Hacker’s Choice, que descifró la manera de leer la información contenida en el chip RFID de un pasaporte europeo. Una vez logrado descifrar la información del documento, lo clonaron y cambiaron los datos. A modo de burla, utilizaron el nombre Elvis y como apellido Presley, sumándole algunos datos biométricos para utilizarlo en el aeropuerto de Amsterdam, donde la máquina lectora de pasaportes inteligentes leyó normalmente el dispositivo y mostró la imagen del astro del rock, supuesto titular.

Un año antes, el holandés Jeroen van Beek contratado por el diario The Times, en menos de una hora y con una lectora de RFID de 80 dólares, accedió a los datos biométricos contenidos en dos pasaportes entregados por el diario, modificó la información y clonó un chip RFID con los datos de Osama Bin Laden. Algo similar había sucedido en 2006 cuando dos expertos alemanes, contratados por la BBC, llevaron a cabo el mismo procedimiento pero en tan sólo cinco minutos.

Por su parte y a modo de protesta, ciudadanos alemanes preocupados por su privacidad implementaron un curioso método para destruir el chip que contiene la cédula y evitar así una posible vigilancia por parte de la Agencia de Seguridad Nacional de Estados Unidos: lo ‘cocinan’ en el microondas. Esta particular acción, considerada por las

⁹⁰ Caminos, Mauricio (2012, enero 31). Proponen intercambiar entre usuarios la SUBE para evitar el registro personal de viajes. *La Nación*. Recuperado el 08 de julio de 2015, de <http://www.lanacion.com.ar/1444834-proponen-que-los-usuarios-intercambien-sus-tarjetas-sube>.

⁹¹ Id.

autoridades como una modificación ilegal de documentos oficiales, puede entenderse también como una táctica o desvío, en términos de De Certeau.

Si bien estos casos no corresponden a la Argentina, el tipo de tecnología de los documentos adulterados es la misma que se usa en el Nuevo DNI y pasaporte argentino. Estos ejemplos demuestran que la herramienta RFID dista mucho de ser infalible; por el contrario, conlleva importantes riesgos y despierta grandes preocupaciones. Al respecto, el experto en seguridad informática Bruce Schneier expresó: “Los viajeros que llevan pasaporte RFID están emitiendo su identidad. Significa que los titulares del pasaporte están emitiendo continuamente su nombre, nacionalidad, edad, dirección y cualquier otra cosa que esté en el chip RFID. Significa que cualquiera con un lector puede acceder a esa información, sin que su portador lo sepa ni autorice (...) Se trata de una clara amenaza tanto para la privacidad como para la seguridad personal”⁹².

5.4-Principios contra la vigilancia indiscriminada

Luego del pedido de informe realizado al Poder Ejecutivo Nacional sobre la creación de un nuevo DNI electrónico para todos los ciudadanos argentinos, la Asociación Pensamiento Penal elaboró un análisis de las respuestas al respecto⁹³.

En el texto se afirma que el futuro documento dejará de ser un mero certificado de identificación para convertirse en una base de datos portable y digitalizada con datos biológicos, biográficos y de la rutina de transporte y consumo que podrán actualizarse y monitorearse en tiempo real a través de un chip de radio frecuencia y otro criptográfico para conexión online, en consonancia a la idea y categoría de análisis planteada como “panóptico de bolsillo”, elaborada en capítulos anteriores.

Paralelamente, la asociación asegura que dicha medida constituye una restricción del derecho humano a la privacidad que pone en cuestión los límites de recolección, uso y protección de los datos personales y sensibles de toda la ciudadanía por parte del Estado. Para realizar tal afirmación utiliza como fundamento el artículo 12 de la Declaración Universal de los Derechos Humanos y el artículo 11 de la Convención Americana de Derechos Humanos sobre protección de la honra y de la dignidad, así

⁹² Schneier, Bruce (2014, octubre 24). Pasaportes RFID. Recuperado el 08 de mayo de 2015, de <http://blog.segu-info.com.ar/2004/10/pasaportes-rfid.html>

⁹³ APP frente a la respuesta del PEN sobre DNI electrónico (2014, octubre). Recuperado el 20 de septiembre de 2015, de <http://www.pensamientopenal.org.ar/wp-content/uploads/2014/10/APP-frente-a-los-DNI-electr%C3%B3nicos.pdf>

como también el artículo 19 de la Constitución Nacional, analizado en el capítulo anterior.

Más adelante, el artículo de APP examina la información brindada por el PEN respecto al cumplimiento de los Principios Internacionales sobre la aplicación de los Derechos Humanos a la Vigilancia de las Comunicaciones⁹⁴. Estos fueron desarrollados entre 2012 y 2013 por más de cien organizaciones de la sociedad civil a nivel mundial con el objetivo de clarificar cómo se aplica el derecho internacional de los derechos humanos en el actual entorno digital, en particular a la luz del aumento y los cambios implementados en las tecnologías y técnicas de vigilancia de las comunicaciones.

Dichos principios -resultado de una consulta global con grupos de la sociedad civil, la industria y expertos internacionales en legislación sobre vigilancia de las comunicaciones, políticas públicas y tecnología-, proporcionan a las sociedades y a los Estados un marco para evaluar si las leyes y prácticas de vigilancia, actuales o propuestas, están en línea con los derechos humanos. A su vez, intenta proveer a los gobiernos, activistas, abogados y legisladores el vocabulario y las referencias necesarias para repensar y reformar leyes en defensa de la privacidad en un mundo donde las prácticas actuales pueden exponer a ciudadanos inocentes a la vigilancia invasiva.

Por tales motivos y en consonancia al planteo de que la vigilancia gubernamental avanza y resulta necesario restringirla de alguna manera, la Asociación Pensamiento Penal utilizó los principios internacionales mencionados para analizar los cambios tecnológicos implementados en el actual documento de identidad argentino.

El primer principio se refiere a la legalidad y establece que cualquier limitación al derecho a la privacidad debe ser prescripta por ley. Respecto a esto, la organización APP recupera la negativa dada por el poder Ejecutivo respecto a la intención de enviar proyectos de ley al Congreso para aprobar el SUBE para transporte y microconsumo comercial y el DNI electrónico. De esta forma, sostiene que “la restricción de un derecho fundamental debe ser tomada como un acto altamente intrusivo y excepcional que interfiere con el pleno ejercicio democrático (...) Por lo tanto, el gobierno no ha mostrado intenciones de respetar el principio de legalidad al menos hasta el primero de marzo de 2015”⁹⁵.

⁹⁴ Principios Internacionales sobre la Aplicación de los Derechos Humanos a la Vigilancia de las Comunicaciones (2014, mayo 10). Recuperado el 20 de septiembre de 2015, de <https://es.necessaryandproportionate.org/text>

⁹⁵ APP frente a la respuesta del PEN sobre DNI electrónico (2014, octubre). Recuperado el 20 de septiembre de 2015, de <http://www.pensamientopenal.org.ar/wp-content/uploads/2014/10/APP-frente-a-los-DNI-electr%C3%B3nicos.pdf>

El siguiente principio analizado internacionalmente y recuperado por APP refiere al objetivo legítimo, mediante el cual se establece que las leyes sólo pueden autorizar la vigilancia de las comunicaciones a autoridades específicas dentro del Estado y con el fin de alcanzar un objetivo legítimo que se vincule a un importante interés legal que es necesario en una sociedad democrática. A partir de las respuestas brindadas por el Ejecutivo relacionadas sólo con meras comodidades y facilidades en el uso, APP asegura que “no hay interés jurídico preponderante o importante que justifique esta nueva restricción del derecho constitucional y convencional a la privacidad. Sólo se presentan argumentos relacionados con facilidades administrativas y de eficiencia en el uso de recursos públicos. Por lo tanto no tiene un objetivo legítimo”⁹⁶.

Otro de los principios internacionales sobre la aplicación de los Derechos Humanos a la vigilancia en las comunicaciones redactado en un documento conjunto es el de necesidad, sobre el que se describe que las leyes que autoricen la vigilancia de las comunicaciones por parte del Estado deben limitar esa vigilancia a aquella que sea la mínima indispensable y necesaria para alcanzar el objetivo legítimo. Sobre este punto, el Estado argentino refirió en el informe que el cambio previsto en el DNI no guarda relación con posibles deficiencias en las medidas de seguridad sino que forma parte de una lógica incremental relacionada a avances de la ciencia y la técnica, tendencias seguidas por la mayoría de los países. A partir de esto, APP destaca que documentaciones de otras naciones (ver apartado Panorama internacional) son motivo de fuertes debates a nivel mundial y que varias de éstas al igual que sus bases de datos biométricos fueron anuladas y/o declaradas inconstitucionales. “Es importante recordar que ninguna tecnología es infalible (...) Por lo tanto, además de innecesario el DNIE puede resultar un retroceso respecto a la seguridad del actual”⁹⁷, se afirma en el documento de APP.

El cuarto principio es idoneidad y refiere a que cualquier caso de vigilancia de las comunicaciones autorizado por la ley debe ser apropiado para cumplir con el fin legítimo que se haya identificado. Al respecto, APP analiza que “nada garantiza que los DNI electrónicos efectivamente simplifiquen y mejoren los trámites de la ciudadanía con el Estado, ni ahorren recursos al mismo (...) Resulta alarmante la falta de planificación en materia de documentación teniendo en cuenta que se modificó tres veces el DNI en 4 años y cada una implicó la movilización y gasto de nuevos

⁹⁶ Id.

⁹⁷ Id.

recursos”⁹⁸, tal como se desarrolló extensamente en el capítulo 2. Por lo tanto, el informe concluye sobre este punto que “el DNLe no resulta idóneo en ninguno de los objetivos explicitados por el gobierno”⁹⁹.

El siguiente ítem se refiere a la proporcionalidad y da cuenta que las decisiones sobre la vigilancia de las comunicaciones deben hacerse ponderando el beneficio que se busca lograr frente al daño que se causaría a los derechos de los usuarios y a otros intereses que puedan estar en competencia. En relación a este principio, resulta necesario destacar que la propuesta del Estado nacional de incorporar información proveniente de otras bases y/o registros al Nuevo DNI sin la opción de que la ciudadanía pueda elegir u objetar esta decisión (incluso puede llegar a desconocer los datos que porte su documentación), vulnera el principio de autodeterminación informativa, tal como se explicó en el capítulo 4, el cual implica que sin la información necesaria el titular está vedado de ejercer su derecho de rectificación o supresión y resulta menoscabado en su derecho a la autonomía individual.

Al respecto, APP en su escrito explica y propone que “si hay una restricción de derechos, el Estado debe demostrar que la técnica usada es la menos invasiva en la práctica porque otras instancia ya han sido agotadas. Y que la medida estará limitada a lo estrictamente relevante conforme los objetivos legítimos, en los plazos establecidos, sin retener información excedente que pueda menoscabar las libertades individuales. Si los objetivos son solamente las facilidades administrativas para el ahorro de tiempo y la posibilidad de la firma digital, el gobierno debería proponer hacerlo permanentemente optativo y a través de una tarjeta separada a la del DNI. Sin embargo omite responder la pregunta sobre si han evaluado otras opciones de firma electrónica y digital en vez de hacerlo a través del DNI. A esto se debe sumar que deja la puerta abierta a incorporar futuros datos sin límites claros. Por lo tanto, el DNLe no respeta el principio de proporcionalidad”¹⁰⁰.

Por último, cabe destacar los principios de transparencia y supervisión pública. El primero refiere a que los Estados deben ser transparentes sobre el uso y alcance de las técnicas y facultades de vigilancia; mientras que el segundo alude a que éstos deben contar con mecanismos independientes de control y revisión para garantizar la transparencia de las actividades de vigilancia de las comunicaciones.

⁹⁸ Id.

⁹⁹ Id.

¹⁰⁰ Id.

Al respecto, el Estado argentino explicó en los informes respondidos que en lo referente al resguardo de información se tomarán las mismas medidas de seguridad que existen para el almacenamiento de los datos de identificación de los ciudadanos existentes en los archivos y bases de datos del Renaper, y recibirán igual tratamiento, restricción en su acceso y protección de datos personales que rige en la actualidad. Teniendo en cuenta los casos de filtraciones y sistemas vulnerados descriptos más arriba, cabe suponer que las medidas de seguridad aludidas resultan insuficientes. Sobre estos principios, APP sostiene que el Estado “omite responder si habrá nuevos controles ciudadanos de acuerdo a esta tecnología. Lo que remite al actual régimen de protección de datos personales cuya autoridad de aplicación es una dirección general que no es autónoma ni autárquica (...) y que no ha auditado organismos públicos desde que fuera creada”¹⁰¹. Por otra parte, y en consonancia con algunas de las situaciones de permeabilidad informática mencionadas, afirma que “la supervisión pública y ciudadana actual en pos de la protección de nuestros datos personales es, cuando no escasa, nula”¹⁰².

Vale aclarar que existen otros principios contra la vigilancia indiscriminada, ya que el documento elaborado enumera una cantidad de 13 en total, que son la autoridad judicial competente, debido proceso, notificación al usuario, integridad de las comunicaciones y de los sistemas, garantías para la cooperación internacional y garantías en contra del acceso ilegítimo. Sin embargo, los analizados tienen competencia respecto al futuro DNI electrónico.

A modo de cierre del análisis de las respuestas del Poder Ejecutivo, APP sostiene que “se puede afirmar con sus propias palabras que la iniciativa de implementar en forma compulsiva un DNI electrónico para todos los argentinos es una medida ilegal, ilegítima, innecesaria, inapropiada y desproporcionada, la cual además carecería de la necesaria supervisión pública y ciudadana sobre la protección de nuestros datos personales y sensibles; pudiendo resultar contraproducente para la seguridad de la población”¹⁰³.

5.5-Panorama internacional

El análisis de lo que acontece en la República Argentina respecto al dispositivo documentario y las innovaciones tecnológicas en el Nuevo DNI planteado hasta aquí, no

¹⁰¹ Id.

¹⁰² Id.

¹⁰³ Id.

puede desconocer ni estudiarse de manera completa al margen del contexto mundial y el tratamiento brindado por otros países a dichas cuestiones.

El acontecimiento que trajo importantes modificaciones en el tema de la seguridad a nivel planetario, y que repercutió en el control poblacional en cuanto a los dispositivos documentarios, fue el atentado terrorista perpetrado a las Torres Gemelas en Estados Unidos.

Haciéndose eco de este episodio, el departamento de Análisis Documental de la Dirección de Información Migratoria correspondiente a la Dirección Nacional de Migraciones, elaboró un informe que se utiliza de manera interna para capacitar y formar a los futuros inspectores en el control migratorio del país. En este se afirma que “a partir de los trágicos acontecimientos del 11 de septiembre del año 2001 llamado 9/11, los Estados Unidos solicitaron adoptar urgentemente medidas destinadas a reforzar la seguridad documental. Se introdujeron así elementos biométricos en los pasaportes. Estos indicadores consisten en impedir la utilización de identidades falsas. A través de una fotografía digitalizada e impresiones dactilares y otros elementos, se ha aumentado la fiabilidad en los controles migratorios que verifican personas con documentos de viaje alrededor de todo el mundo”.¹⁰⁴

En consonancia a este suceso de repercusión mundial, en la introducción de *Un mundo vigilado* Mattelart sostiene que “la multiplicación de las medidas de excepción en el marco de la ‘guerra global’ contra el terrorismo se ha conjugado en los países democráticos a raíz del 11 de septiembre de 2001 con la creciente injerencia de los dispositivos de vigilancia en la vida cotidiana de los ciudadanos. A más seguridad, más tecnología: la gestión de la seguridad del riesgo se va convirtiendo en una cuestión de técnicas” (2009:11).

Esto coincide con “un principio facilitador eficientista”¹⁰⁵, expresión utilizada por Andrés Pérez Esquivel en el marco de una entrevista personal, respecto a que si la tecnología posibilita implementar un determinado cambio es necesario y efectivo realizarlo. Se debe a una concepción extendida que “supone que la tecnología siempre viene a solucionar problemas”¹⁰⁶, explicó la politóloga y periodista Natalia Zuazo en la Jornada *Te estamos vigilando*. En concordancia, la Asociación por los Derechos Civiles

¹⁰⁴ Normativas sobre ingreso y egreso de personas. (2015, marzo). Dirección Nacional de Migraciones.

¹⁰⁵ Entrevista con Andrés Pérez Esquivel realizada en Buenos Aires el 23 de septiembre de 2015.

¹⁰⁶ *Te estamos vigilando* (2015, diciembre 2). Jornada organizada por la Asociación por los Derechos Civiles, Argentina.

y la Fundación Vía Libre expresaron una idea similar: “La visión que parece imponerse en el Estado argentino es que cualquier ‘avance’ tecnológico es deseable en sí mismo”¹⁰⁷.

Siguiendo esta premisa y tal “como ocurre en los países más desarrollados”¹⁰⁸ -según las palabras del titular de la cartera del Interior y Transporte-, fue que el Estado implementó numerosas innovaciones tecnológicas en materia identificatoria, como se desarrolló a lo largo del trabajo.

Pese a estos argumentos, varias de las naciones que impulsaron políticas masivas de identificación debieron retroceder en esa decisión y dismantelaron los sistemas de control. Un ejemplo es el de Francia en donde, en 2012, el Consejo Constitucional declaró inconstitucional la creación de una base nacional de datos biométricos y el chip electrónico en el DNI, por no brindar garantías de seguridad ni de éxito en la lucha contra el delito de robo de identidades. Además dicha medida fue considerada un avance desproporcionado sobre el derecho a la privacidad de las personas¹⁰⁹.

Una situación similar se produjo en Inglaterra, país que revirtió la implementación del carnet de identificación electrónico, creado en 2006 y dejado sin efecto en 2010 por la presión ciudadana tras fuertes críticas y fallas de seguridad¹¹⁰.

Por su parte, España -nación con la que la República Argentina firmó el acuerdo para la incorporación de tecnología en el Nuevo DNI- cuenta con documento electrónico desde 2006. Sin bien esta identificación también recibió críticas, el chip no contiene información relativa a datos personales distintos a los que aparecen impresos en la superficie de la tarjeta, como sí está previsto para el caso argentino¹¹¹.

En consonancia a estas decisiones, Mattelart sostiene que “durante más de un siglo las democracias de los países industrializados han rechazado los proyectos de

¹⁰⁷ Nuevos DNI: No se trata sólo de avances tecnológicos (2014, junio 27). Asociación por los Derechos Civiles. Recuperado el 20 de septiembre de 2015, de <http://www.adc.org.ar/nuevos-dni-no-se-trata-solo-de-avances-tecnologicos/>

¹⁰⁸ El nuevo DNI tendrá un chip que incluirá la historia clínica de las personas y los datos de su SUBE (2014, junio 27). Infobae. Recuperado el 20 de septiembre de 2015, de <http://www.infobae.com/2014/06/27/1576438-el-nuevo-dni-tendra-un-chip-que-incluire-la-historia-clinica-las-personas-y-los-datos-su-sube>.

¹⁰⁹ Crettaz, José (2013, diciembre, 15). DNI: la privacidad, en riesgo por la identificación biométrica. *La Nación*. Recuperado el 15 de octubre de 2015, de <http://www.lanacion.com.ar/1647826-dni-la-privacidad-en-riesgo-por-la-identificacion-biometrica>.

¹¹⁰ El nuevo DNI de Florencio Randazzo es un arma para espiar (2014, octubre 09). *La izquierda diario*. Recuperado el 15 de octubre de 2015, de <http://www.laizquierdadiario.com/El-nuevo-DNI-de-Florencio-Randazzo-es-un-arma-para-espiar>.

¹¹¹ Desde 2015, el DNI tendrá un chip para guardar más datos (2014, junio 28). *La Voz*. Recuperado el 15 de octubre de 2015, de <http://www.lavoz.com.ar/ciudadanos/desde-2015-el-dni-tendra-un-chip-para-guardar-mas-datos>.

generalización de la identificación biométrica por temor a atentar contra la vida privada y los derechos de los ciudadanos. Y muchas llegarán a plantear objeciones al principio mismo del carné de identidad” (2009:31-32).

En dirección contraria a estas restringidas iniciativas europeas, India creó una tarjeta de identificación con chip integrado que almacena una enorme cantidad de información a la que se accede digitalmente y está interconectada con todas las instituciones tanto privadas como públicas. Se la conoce como Aadhaar (que significa ‘plataforma’ en 22 lenguas indias) y permite acceder a servicios sociales básicos, becas estudiantiles, medicinas o promociones de viviendas municipales. Esta política de identificación incluyó un censo previo con datos personales y biométricos de todos los habitantes, lo que posibilitó la centralización de información sensible y la vinculación a un número particular. Además, este plan prevé que cada persona nueva que se inscribe primero es comparada biométricamente con todos los ciudadanos ya inscritos para detectar si hay identidades duplicadas, con el fin de evitar el acceso fraudulento a varias prestaciones.

“Este ambicioso programa no fue aprobado por ley en el Congreso Nacional pero está avanzando y a punto de terminar con el objetivo de empadronar a 1.300 millones de personas. Por primera vez en la historia, de la mano de empresas europeas, se centralizan los datos biográficos y biológicos digitalizados de un 15% de la humanidad”¹¹², explicó Pérez Esquivel sobre este caso en la jornada *Tecnología, vigilancia y derechos personalísimos*. Al respecto, resulta pertinente mencionar el caso de dos ciudades indias que anunciaron la pérdida de sus bases, por lo que tuvieron que volver a convocar e inscribir a todos sus habitantes. Desconocer el destino de esa información, con los posibles riesgos que esta situación conlleva, resulta por demás sugestivo y alarmante.

En el plano latinoamericano, a mediados de 2015 el DNI electrónico peruano fue reconocido como el mejor documento de identidad de la región por sus características y funciones. La distinción se debió a que el carnet, lanzado en 2013 y emitido por el Registro Nacional de Identificación y Estado Civil, posee 15 mecanismos de seguridad y contiene dos certificados digitales, uno de los cuales permite firmar digitalmente documentos electrónicos¹¹³.

¹¹² Tecnología, vigilancia y derechos personalísimos (2015, agosto19). Jornada organizada por la Carrera de Especialización en la Facultad de Derecho de la Universidad de Buenos Aires, Argentina.

¹¹³ DNI electrónico ganó premio como mejor documento de la región (2015, junio 25). *El Comercio*. Recuperado el 15 de octubre de 2015, de <http://www.elcomercio.pe/lima/ciudad/dni-electronico-gano-premio-como-mejor-documento-region-noticia-1821484>.

Por último, cabe mencionar un caso paradigmático y por demás llamativo. En 2013 Nigeria firmó un acuerdo con la empresa MasterCard para que su ciudadanía disponga de un documento de identidad que también funciona como tarjeta de crédito. Este carnet con sistema de pago electrónico integrado, cuenta con datos demográficos y biométricos de la persona y se encuentra ligado a una cuenta de banco que habilita a depositar fondos, realizar transacciones, pagar sus servicios y retirar dinero en efectivo en comercios y cajeros automáticos¹¹⁴.

Ciertos países con posiciones hegemónicas a nivel mundial no imponen este tipo de políticas de identificación ni crean bases nacionales biométricas por considerarlas un riesgo para sus poblaciones, como se describió anteriormente, resguardando así los principios de privacidad e intimidad y regulando la recolección de datos personales. Sin embargo, varias de esas naciones invierten esta postura al impulsar, participar y promover invasivas medidas a otros países, habitualmente de zonas periféricas, para múltiples usos -social, comercial, policial o militar- y de modo experimental. “Argentina es un país de laboratorio en la materia. Esto se observa en múltiples cuestiones culturales y coyunturales: esta nación fue sede de encuentros internacionales de biometría, Interpol tiene la sede más antigua en el país, lo que refuerza y profundiza el vínculo con la policía internacional. Por otra parte, en Argentina existe una amplia tradición de sesión de datos en materia de identificación a partir del invento de Vucetich, además de contar una construcción hegemonía discursiva muy fuerte respecto del tópico de la seguridad, entre otras cuestiones”¹¹⁵.

5.6-Políticas de exclusión

Entre los diferentes riesgos que se vislumbran a raíz del fenómeno de empadronamiento biológico masivo de la humanidad se destacan determinadas políticas o medidas de exclusión impulsadas por ciertos países, a partir de un uso arbitrario y discriminador de sus bases de datos.

Según diversos autores, las bases de datos se definen como un “conjunto de programas de computación (software) que provee eficientes métodos de acceso a los datos institucionalizados pero no sólo a este tipo de datos. Cuando las bases de datos están organizadas o se implementa un sistema de manejo de las mismas se forma un banco de

¹¹⁴ Pérez, Miguel (2013, mayo 24). Nigeria como modelo emergente: DNI's electrónicos con sistema de pagos integrado. Recuperado el 15 de octubre de 2015, de <http://www.blogthinkbig.com/nigeria-modelo-emergente-dnis-electronicos-sistema-de-pagos/>

¹¹⁵ Entrevista con Andrés Pérez Esquivel realizada en Buenos Aires el 23 de septiembre de 2015.

datos”¹¹⁶. Por su parte, el sociólogo James Rule subraya que una vez que estos sistemas de recopilación de datos son puestos en marcha “tienden a crecer y difícilmente pueden ser desmantelados. Conforme se perfeccionan los medios para conocer más sobre las personas, más eficaz se vuelve para las instituciones que las emplean para recopilar más datos”¹¹⁷.

A partir de esta definición es pertinente mencionar el concepto de banóptico, acuñado por Didier Bigo, que se vincula con la utilización de la biometría y las bases de datos interconectadas como instrumentos para expulsar a los individuos pertenecientes a ciertos grupos sociales o a marginales globales, como ser los inmigrantes, los sospechosos de terrorismo y demás sujetos transformados en ‘blanco’ de innovadores sistemas de seguridad.

El prefijo ‘ban’ del término banóptico remite a la palabra en inglés exclusión y sirve como un modo de pensar la vigilancia y las tecnologías de elaboración de perfiles utilizadas para determinar quién debe ser objeto de un control estricto. Tal como explican Bauman y Lyon en *Vigilancia líquida* (2013), el banóptico es una forma de practicar la vigilancia mediante instrumentos que se dedican a “mantener lejos” en vez de “mantener adentro”, como hacía el panóptico, que crece y se nutre del imparable aumento de las preocupaciones securitarias y no de la necesidad de disciplinar, como era el caso del diseño panóptico.

Este planteo coincide con el desarrollo de Agamben sobre el estado de excepción, como fue desarrollado en el capítulo 1, en el que la ley se aplica desaplicándose y funciona un dispositivo biopolítico que permite al soberano enfrentarse con la vida biológica de sus súbditos al producirse la suspensión de la validez del ordenamiento jurídico. Por otra parte, el autor define a esta exposición de la vida al estado de excepción como una situación de bando. Aquel que se encuentra en esta situación está por fuera de la ley, pero, simultáneamente, dado que ésta sólo es pensable bajo el poder soberano, se remite a ella. El filósofo italiano recupera el concepto de exclusión de Jean Luc Nancy y sostiene: “La relación de excepción es una relación de bando. El que ha sido puesto en bando no queda sencillamente fuera de la ley ni es indiferente a ésta, sino que es abandonado por ella, es decir que queda expuesto y en peligro en el umbral en que vida y derecho, interior y exterior se confunden (...) No hay afuera de la ley. La relación

¹¹⁶ Lucena Cid, Isabel (2012). La protección de la intimidad en la era tecnológica: hacia una reconceptualización. *Revista Internacional de Pensamiento Político*, I Época, (7), p.134.

¹¹⁷ Id.

originaria de la ley con la vida no es la aplicación sino el abandono” (Agamben, 1998:44-45).

La combinación del concepto de exclusión, en el sentido desarrollado por Agamben, con la idea de óptico de Foucault, da como resultado el dispositivo denominado banóptico que, en un contexto en que se rastrea y controla la movilidad poblacional, muestra “quién es aceptado y quién no, creando categorías de personas excluidas no sólo por un determinado Estado-nación, sino por un conglomerado amorfo y no unificado de poderes globales. Y ese conjunto opera virtualmente, utilizando bases de datos interconectadas, para canalizar los flujos de datos, especialmente datos sobre lo que todavía no ha pasado”, explican Bauman y Lyon (2013:70).

Según los autores, la función principal del diagrama banóptico se basa en determinar una minoría como excluida; de impedir el acceso a aquellos individuos que no cuentan con los dispositivos individualizados de control que les permita practicar la propia vigilancia. Por otra parte, destacan que “tres elementos constituyen un poder excepcional en el seno de las sociedades liberales (el estado de emergencia que se convierte en la regla), la selección (que excluye a ciertos grupos, o a categorías enteras de personas excluidas, por su comportamiento social futuro) y la normalización de los grupos no excluidos (mediante la creencia en la libre circulación de bienes, capital, información y personas). El banóptico actúa en los espacios globalizados que superan el Estado-nación, por lo que los efectos del poder y la resistencia ya no se dan sólo entre el Estado y la sociedad” (Id.:70-71).

Un claro ejemplo de este tipo de dispositivo es el sistema Eurodac que permite a los países de la Unión Europea (UE) identificar a los solicitantes de asilo y a las personas interceptadas en relación con el cruce irregular de las fronteras exteriores. Basado en la comparación de las impresiones dactilares, los países del bloque pueden comprobar si el solicitante de asilo o el extranjero presente en su territorio ya solicitó refugio en otro país de la UE o entró irregularmente.

Este sistema se compone de una unidad central gestionada por la Comisión Europea, una base central informatizada de datos dactiloscópicos y medios electrónicos de transmisión entre los países miembros y la base central. De este modo, a toda persona mayor de 14 años se le toman las huellas dactilares, datos particulares (sexo, país de la UE de origen, lugar y fecha de solicitud de asilo o intercepción de la persona, fecha de toma de impresiones y de transmisión de datos a la unidad central) y se le asigna un número de referencia. Este último, que se compone de una o varias letras y de un

código, permite atribuir las huellas a una persona específica y determinar el país del bloque que transmitió los datos. Toda esa información se envía a la unidad central a través de los puntos de acceso nacionales y se conserva durante diez años, con excepción de los casos de obtención de permiso de residencia, abandono del territorio del bloque o adquisición de ciudadanía de un país de la UE.

Además de la política de exclusión que pone en juego este sistema banóptico, es importante destacar que en ciertas situaciones de vigilancia como la descrita, los cuerpos son reducidos a meros números -tal como se expresó en el capítulo 3-. El sistema Eurodac resulta un caso paradigmático de la utilización de datos biométricos en las fronteras, cuyo objetivo es controlar la identidad de los cuerpos y luego permitir o denegar la posibilidad de cruzar los límites territoriales.

Bajo estos sistemas, la información sobre el cuerpo es tratada como concluyente para determinar la identidad de las personas, ignorando la integridad corporal. Así, la propia información descorporizada y su lectura mediante software y técnicas estadísticas determinan el destino y las oportunidades de cientos de seres humanos, cuyas humanidades quedan reducidas a simples categorías.

Probablemente, estos ejemplos del uso de biometría en materia de identificación constituyan los rasgos más negativos y las formas de muerte asumidos por el biopoder; modos en que el poder soberano puede ejercer positivamente su derecho de muerte en sociedades cuya principal técnica de gobierno se basa en la intervención y el desarrollo de la vida.

Conclusiones

En la presente tesina nos propusimos estudiar, desde una perspectiva biopolítica, el proceso documentario como mecanismo de control estatal y el Documento Nacional de Identidad, específicamente, como ensamble entre el período disciplinario y la era de la vigilancia.

Para lograrlo, reconstruimos la genealogía del dispositivo documentario argentino como una eficaz herramienta para el reconocimiento, fichaje e identificación de los individuos. A su vez, analizamos las innovaciones técnicas incorporadas en la materia que apuntan a profundizar los objetivos planteados. Estas transformaciones se caracterizan por el uso de tecnología biométrica en el nuevo Documento Nacional de Identidad (DNI), sumada a la potencialidad de convertirlo en un documento electrónico con la incorporación de dos chips y la conformación de una base estatal de datos a partir de la puesta en marcha del Sistema Federal de Identificación Biométrica para la Seguridad (SIBIOS), que tiene por objeto prestar un servicio centralizado de información respecto de los registros personales, a fin de identificar y monitorear a los ciudadanos.

Por otra parte, exploramos la normativa legal vigente sobre la que se sostiene el proceso de identificación en la República Argentina junto a las modificaciones y complementaciones realizadas. Paralelamente, hicimos foco en la incidencia sobre la privacidad e intimidad, las libertades civiles y la autodeterminación informativa, amparadas en la Constitución Nacional y en tratados internacionales. También describimos las vulnerabilidades informáticas sufridas por los sistemas estatales encargados de resguardar la información de la ciudadanía, lo que evidencia la debilidad en la seguridad y los riesgos que esto conlleva. Asimismo, destacamos los casos documentarios más emblemáticos a nivel internacional.

De igual manera, analizamos los pedidos de informes elevados al Poder Ejecutivo Nacional sobre el Nuevo DNI por parte de distintos actores sociales, asistimos a congresos y jornadas sobre la temática organizadas por entidades que se oponen o cuestionan la política identificatoria/documentaria argentina como la Asociación por los Derechos Civiles, la Fundación Vía libre y la Asociación Pensamiento Penal, y entrevistamos al sociólogo y especialista en la materia Andrés Pérez Esquivel, para poder abordar la temática más acabadamente.

Por último, examinamos la relación asimétrica que se establece entre el Estado en su rol de recolector de datos y los individuos como proveedores de información, en la que el primero cuenta con una posición dominante capaz de quebrantar o avasallar el lugar más débil de este vínculo, posibilitando múltiples formas de discriminación y políticas de exclusión.

A modo de conclusiones o puntos relevantes que surgen como resultado del recorrido elaborado en el presente trabajo de investigación, destacamos que:

- € El sistema documentario argentino se sustenta en la Ley N° 17.671 de Identificación, Registro y Clasificación del Potencial Humano Nacional, la cual fue sancionada en 1966 durante el gobierno de facto comandado por Juan Carlos Onganía. Los múltiples cambios y modernas innovaciones tecnológicas que se hicieron desde ese momento mantienen la matriz autoritaria correspondiente a dicha normativa, ya que no se efectuaron cambios legislativos que implicaran la discusión y aprobación de una nueva ley en la materia por lo que se puede cuestionar el carácter democrático de tales modificaciones. La legislación vigente caracteriza a la población como potencial humano, en detrimento a una nominación y/o perspectiva basada en los derechos humanos. A su vez, define a los ciudadanos como meros datos a ser clasificados, por lo que quedan subsumidos como capital del Estado.
- € Existe una extendida aceptación y naturalización del proceso documentario por parte de la ciudadanía argentina así como también de la tramitación, portación y renovación del documento, con la correspondiente entrega de datos personas y huellas digitales. Posiblemente esto se deba a que los argentinos cuentan con una larga tradición en la materia y están acostumbrados a poseer un carnet identificador que lo habilita a ejercer sus derechos, acceder a beneficios y realizar todo tipo de trámites. De esta manera, se puede afirmar que el proceso documentario como mecanismo disciplinario es un verdadero éxito en la Argentina, debido a que sus nacionales lo incorporaron a su *habitus*, en términos de Pierre Bourdieu (1994).
- € Tanto el doble chip en el Nuevo DNI (datos biométricos + información que puede interactuar con otros sistemas, lo que potencialmente lo convierte en un documento electrónico) como la conformación de una base estatal de datos a partir del funcionamiento del Sistema Federal de Identificación Biométrica para

la Seguridad, que apunta a centralizar la información de los registros patronímicos y biológicos a fin de identificar y monitorear a los ciudadanos mediante referencias cruzadas por parte de las agencias de seguridad, fueron medidas tomadas por resoluciones administrativas sin el correspondiente paso y discusión en el Congreso Nacional así como tampoco fueron temas instalados en la agenda pública, salvo aislados intentos de debate sin grandes repercusiones.

- € La incorporación de tecnología biométrica en el Nuevo DNI así como la creación del SIBIOS fueron presentadas por las autoridades y recepcionadas por la ciudadanía en términos positivos, bajo la premisa que cualquier incorporación o avance tecnológico es deseable y efectivo por sí mismo. De esta manera los dispositivos en cuestión se *cajanegrizan*, en términos de Bruno Latour (2001), es decir, se evita problematizar sobre sus contenidos y se invisibilizan los posibles riesgos y amenazas debido al éxito en cuanto a sus beneficios. Advertimos, entonces, la necesidad de un debate y tratamiento respecto a la falta de seguridad, la vulnerabilidad y los peligros a los que está sometida la información de la ciudadanía en manos del Estado a raíz de los casos de filtraciones y descargas en distintos sistemas públicos.
- € Las innovaciones tecnológicas implementadas en la política documentaria argentina contribuyen a la conformación de un Estado con amplitud de poder en materia identificatoria, ya que reúne numerosa información y datos personales que posibilita el monitoreo, la vigilancia y el control de la población, poniendo en riesgo o vulnerando la privacidad, la intimidad y las libertades civiles de los individuos, derechos garantizados por la Constitución Nacional y por tratados internacionales. Por ello, consideramos la necesidad de la puesta en ejercicio de la cultura cívica y de prácticas tendientes a una mayor resistencia por parte de la ciudadanía.
- € La tecnología biométrica incorporada en el dispositivo documentario implica la identificación del individuo no por lo que posee, sabe o hace sino con lo que el sujeto es, con lo más íntimo de su ser, aquello que constituye su propia biología. La tendencia que se vislumbra respecto a este modo de identificación supone el mismo recorrido que con otros tipos: en un comienzo se utiliza en los sospechosos o clases peligrosas y luego se extiende al conjunto de la población, impidiendo o dificultando ciertos desvíos para escapar del control ya que este actúa sobre el cuerpo y puede implementarse sin consentimiento. Aisladas voces

disidentes a nivel mundial expresaron su negativa a someterse a tal invasivo procedimiento.

- € El potencial DNI electrónico con la incorporación de dos chips, uno de los cuales se basa en tecnología de identificación por radiofrecuencia (RFID) -al igual que la tarjeta SUBE y el pasaporte- habilita la trazabilidad de las personas y el control absoluto de sus movimientos e interacciones, transformándose así en un *panóptico de bolsillo*. A su vez, los titulares de estos documentos emiten continuamente su identidad al igual que aquellos datos contenidos en el chip, al que se accedió y logró vulnerar y adulterar fácilmente en diferentes oportunidades sin el consentimiento o con el desconocimiento de sus portadores, por lo que representa una gran amenaza para la privacidad y la seguridad personal.
- € La potencialidad de convertir el DNI en un carnet inteligente multipropósito que contenga e interactúe con múltiples informaciones como la historia clínica, los datos previsionales y jubilatorios así como las referencias de recorridos en transporte y microconsumo comercial provenientes de la tarjeta del SUBE, significa una representación metonímica de los sujetos debido a que cada documento se puede transformar en una involuntaria biografía individual, la cual puede sustituir a la propia persona, figura real y portadora de sus datos. Además, estos documentos pueden considerarse como *extensiones protésicas*, en términos de Carmen Romero Bachiller (2008), ya que se convierten en habilitadores y garantes de la verdad humana de los sujetos que los ostentan quienes, a su vez, quedan reducidos a dichas extensiones.
- € La situación de un Estado con abundante información a su disposición a partir de la conformación y administración de esta base de datos genera una relación asimétrica y desigual con su ciudadanía, lo cual pueda dar lugar a diversas irregularidades y políticas de exclusión. Es necesario generar las estrategias suficientes para que la población, el actor social más perjudicado de este vínculo, disponga de los medios y herramientas para evitar posibles abusos o avances sobre sus derechos. A su vez, consideramos la urgencia de indagar y hallar mecanismos de fiscalización para con el Estado o hacia aquellos que encarnan su figura, planteo que se puede sintetizar con el interrogante: ¿Quién controla a los que controlan?

- € La extracción de datos biométricos de forma masiva y compulsiva puede dar lugar a la conformación de las sociedades predelictivas o *sociedades del hipercontrol*, en términos de William Bogard (2006), que coincide con el *imperativo de la providencia* planteado por Gérard Wajcman (2011). Este tipo de sociedades se caracterizan por operar en términos predictivos y de actuación previa al hecho, y apuntan a estrategias reguladoras preventivas. Bajo estas premisas, los Estados reúnen la información disponible de la mayor cantidad de personas a fin de combatir la delincuencia y abordar más fácilmente al sujeto que decida delinquir a futuro. Así se produce el pasaje de la prevención a la anticipación, que afecta la presunción de inocencia al revertir la carga de la prueba: todos somos culpables hasta que la identificación demuestre lo contrario.
- € Diversos países europeos que tiempo atrás desarrollaron una política identificatoria basada en la incorporación de tecnología biométrica como es el caso de la República Argentina, decidieron dar marcha atrás a tales iniciativas por considerarlas invasivas, inconstitucionales o violatorias de derechos y libertades civiles, priorizando así la privacidad y autonomía de sus ciudadanos. Pese a esto, varias de esas mismas naciones impulsan e incentivan la adquisición de tales sistemas de seguridad a países periféricos o en vías de desarrollo a través de la venta de tecnología o de alianzas estratégicas relacionadas a metodologías rechazadas para sus propias poblaciones.

A modo de recuperar el punto de partida, creemos que demostramos que el Documento Nacional de Identidad constituye un ensamble entre el período disciplinario y la era del control, el cual permite comprender la matriz técnico-social que define a cada momento histórico, así como sus formas y prácticas características.

Partiendo de la noción de biopoder que caracteriza un poder cuya función más alta es la administración de los cuerpos y la gestión calculadora de la vida, analizamos el proceso documentario como una gran tecnología biopolítica mediante la cual el individuo se transforma en ciudadano, y exploramos el DNI particularmente como el principal dispositivo de identificación de la sociedad disciplinaria argentina, que fue reconfigurado en la era de la vigilancia y el control con la incorporación de tecnología biométrica y la potencialidad de convertirse en un carnet electrónico multipropósito.

Durante el período disciplinario, las sociedades definidas como máquinas extractoras de energía, contaban con instituciones de encierro que moldeaban y formaban cuerpos dóciles y útiles. En este contexto, el proceso documentario sirvió para registrar, clasificar e identificar a cada ciudadano y, a su vez, mediante un conjunto de procesos biopolíticos, convertir al pueblo en población.

Por su parte, en el período caracterizado por las sociedades postdisciplinarias o de control, definidas como extractoras de información, aparecen nuevos dispositivos y algunos otros consiguen reconfigurarse, como es el caso de nuestro objeto de estudio, conformando entre todos ellos una amplia red de vigilancia que apunta a la trazabilidad y el control, y opera no sobre individuos encerrados en instituciones sino que circulan libres y anónimos en espacios abiertos.

Hasta aquí, nuestro trabajo exploratorio. Concluimos esta tesina pero consideramos que esta investigación puede ser retomada a futuro pues la política documentaria argentina no está completamente instrumentada y el Nuevo DNI posee grandes potencialidades aún no efectivizadas. Además, resulta un interrogante la decisión política que se tomará en la materia así como los próximos lineamientos tendientes a la continuidad o a la modificación de la tarea identificatoria llevada a cabo hasta el momento, a partir de la asunción de las nuevas autoridades correspondiente a la alternancia en la administración que supone el sistema democrático.

Bibliografía

Libros:

About, Ilse & Denis, Vincent (2011). *Historia de la identificación de las personas*. Barcelona: Editorial Ariel.

Agamben, Giorgio (1998). *Homo Sacer I*, Valencia: Pre-textos.

Agamben, Giorgio (2004). *Estado de excepción. Homo Sacer II, I*. Buenos Aires: Adriana Hidalgo editora.

Anitua, 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.

Bauman, Zygmunt (2001). *En busca de la política*. Buenos Aires: Fondo de Cultura Económica.

Bauman, Zygmunt (2002). *Modernidad Líquida*. México: Fondo de Cultura Económica.

Bauman, Zygmunt & Lyon, David (2013). *Vigilancia líquida*. Argentina: Paidós.

Bogard, William (2006). Welcome to the Society of Control: The Simulation of Surveillance Revisited. *The New Politics of Surveillance and Visibility*, editado por K. Haggerty y R. Erickson. Toronto: University of Toronto Press.

Bourdieu, Pierre (1994). *El sentido práctico*. Madrid: Taurus.

Bourdieu, Pierre (1999). *Razones prácticas. Sobre la teoría de la acción*. Barcelona: Anagrama.

De Certeau, Michel (1996). *La invención de lo cotidiano I. Artes de hacer*. México: Universidad Iberoamericana.

Deleuze, Gilles (1999). “Posdata sobre las sociedades de control”, en Christian Ferrer (comp.). *El lenguaje libertario. Antología del pensamiento anarquista contemporáneo*. Buenos Aires: Altamira.

Díaz, Esther (2010). *Las grietas del control. Vida vigilancia y caos*. Buenos Aires: Editorial Biblos.

Esposito, Roberto (2006). *Biopolítica y filosofía*. Buenos Aires: Editorial Grama.

Foucault, Michel (1992). *Historia de la sexualidad I. La voluntad de saber*. Buenos Aires: Siglo XXI Editores.

Foucault, Michel (1996a). *Genealogía del racismo*. Argentina: Altamira.

- Foucault, Michel (1996b). *La verdad y las formas jurídicas*. Barcelona: Gedisa.
- Foucault, Michel (2000). *Defender la sociedad. Curso en el Collège de France (1975-1976)*. Buenos Aires: Fondo de Cultura Económica.
- Foucault, Michel (2005). *El poder psiquiátrico. Curso en el Collège de France (1973-1974)*. Buenos Aires: Fondo de Cultura Económica.
- Foucault, Michel (2006). *Seguridad, territorio, población*. Buenos Aires: Fondo de Cultura Económica.
- Foucault, Michel (2007). *Nacimiento de la biopolítica*. Buenos Aires: Fondo de Cultura Económica.
- Foucault, Michel (2008). *Vigilar y castigar*. Buenos Aires: Siglo XXI Editores.
- Hardt, Michael & Negri, Antonio (2002). *Imperio*. Argentina: Paidós.
- Latour, Bruno (2001). *La esperanza de Pandora. Ensayos sobre la realidad de los estudios de la ciencia*. Barcelona: Gedisa.
- Lazzarato, Maurizio (2006). *Políticas del acontecimiento*. Buenos Aires: Editorial Tinta Limón.
- Lyon, David (1995). *El ojo electrónico. El auge de la sociedad de la vigilancia*. Madrid: Alianza.
- Lyon, David (2009). *Identifying citizens: ID cards as surveillance*. Cambridge, UK; Malden, MA: Polity Press.
- Marx, Gary (1988). *Undercover. Police Surveillance in America*. Berkeley: University of California Press.
- Mattelart, Armand (2009). *Un mundo vigilado*. Barcelona: Paidós.
- Nissenbaum, Helen (2011). *Privacidad amenazada. Tecnología, política y la integridad de la vida social*. México: Océano.
- Pato, Joseph & Millet, Lynette (Eds.) (2010). *Biometric recognition: Challenges and opportunities*. National Academies Press.
- Piccirilli, María Eugenia (s.f). Principios Nacionales e Internacionales en el marco de la Protección de Datos Personales. Deficiencias. Recomendaciones. Tensiones que genera la aplicación de las Tecnologías de la Información y las Comunicaciones (TICs) y los derechos a la protección de datos personales, intimidad e imagen. Proyecto de Investigación UBACYT. Programación científica 2014-2016.
- Siri, Laura (2009). Todos somos vigilados o la sociedad de las identidades formalizadas en Aníbal Ford (ed.). En *La marca de la bestia. Identificación, desigualdades e infoentretenimiento en la sociedad contemporánea*. Buenos Aires: Norma.

Sloterdijk, Peter (2002). El desprecio de las masas. *Ensayo sobre las luchas culturales de la sociedad moderna*. Valencia: Pre-textos.

Villarruel, Darío (2011). *DNI. Hacia una identidad sin trampas*. Buenos Aires: Ediciones B.

Wajcman, Gerard (2011). *El ojo absoluto*. Buenos Aires: Manantial.

Publicaciones impresas (Revistas y Diarios):

Agamben, Giorgio (2004, enero 11). No al tatuaje bio-político. *Le Monde*.

Bañuelos, Jacob (2003, febrero-marzo). Videovigilancia en la sociedad panóptica contemporánea. *Razón y Palabra*, 31.

Colección Cuadernos Caras y Caretas (2011) Historia de la identidad de los argentinos. Buenos Aires: Fundación Octubre -Trabajadores de Edificios.

Castro Orellana, Rodrigo (2009). La ciudad apestada. Neoliberalismo y postpanoptismo. *Revista de Ciencia Política*, 1 (29).

Febbro, Eduardo (2010, noviembre 20). Siempre se infunde miedo en nombre del bien. Diálogo con el intelectual francés Paul Virilio. *Página 12*.

García Fanlo, Luis (2011, marzo). ¿Qué es un dispositivo?: Foucault, Deleuze, Agamben. *Parte Rei Revista de Filosofía*, 74.

Godina Herrera, Célida (2006, julio). El panóptico moderno. *A Parte Rei Revista de Filosofía*, 46.

Lucena Cid, Isabel (2012). La protección de la intimidad en la era tecnológica: hacia una reconceptualización. *Revista Internacional de Pensamiento Político*, I Época, (7).

Navia, Javier (2013, diciembre 15). Sibios. El polémico sistema de identificación del nuevo DNI. *La Nación*.

Romero Bachiller, Carmen (2008). Documentos y otras extensiones protésicas, o como apuntalar la 'identidad'. *Política y Sociedad*, 45 (3).

Torres, Ariel (2013, noviembre 09). En busca de las armas de vigilancia masiva. *La Nación*.

Vásquez Roca, Liliana (2007). Fenomenología de la intimidad; aproximación jurídica y ontológica a los conceptos de intimidad y privacidad. *Psikeba: Revista de Psicoanálisis y Estudios Culturales*, 5.

Publicaciones Electrónicas:

APP frente a la respuesta del PEN sobre DNI electrónico (2014, octubre). Recuperado el 20 de septiembre de 2015, de <http://www.pensamientopenal.org.ar/wp-content/uploads/2014/10/APP-frente-a-los-DNI-electr%C3%B3nicos.pdf>

Asociación por los Derechos Civiles (2013, octubre 22). La ADC pidió a la justicia que se retiren las fotos de los votantes del padrón electoral online. Recuperado el 10 de junio de 2015, de <http://www.adc.org.ar/1045-la-adc-pidio-a-la-justicia-que-se-retiren-las-fotos-de-los-votantes-del-padron-electoral-online/>

Asociación por los Derechos Civiles (2015, mayo 19). Si nos conocemos más, nos cuidamos mejor. Recuperado el 10 de junio, de <http://www.adc.org.ar/publicaciones/download-info/si-nos-conocemos-mas-nos-cuidamos-mejor-informe-sobre-politicas-de-biometria-en-la-argentina/>

Asociación por los Derechos Civiles (2015, enero 18). Si nos conocemos más, nos cuidamos mejor. Recuperado el 10 de junio, de <http://www.adc.org.ar/publicaciones/download-info/el-des-control-democratico-de-los-organismos-de-inteligencia-en-argentina/>

Congreso Internacional de Biometría de la República Argentina [CIBRA] (2011, noviembre 14). Apertura Dr. Aníbal Fernández. Recuperado de 4 de junio de 2015, de <http://www.biometria.gov.ar/congresos/cibra-2011/videos.aspx#.U8cX7DtSZrs.twitter>.

Conozca SIBIOS: La masiva y Orwelliana base de datos biométrica de Argentina (2013, octubre 28). El Nuevo despertar. Recuperado el 10 de diciembre de 2014, de <https://elnuevodespertar.wordpress.com/2013/10/28/conozca-sibios-la-masiva-y-orwelliana-base-de-datos-biometrica-de-argentina/>

Haciendo (el panóptico genético de) Buenos Aires (s.f.). Recuperado el 10 diciembre de 2014, de <http://derechoaleer.org/blog/2011/01/haciendo-el-panoptico-genetico-de-buenos-aires.html>

Janices, Pedro (2012, julio 03). Mitos y Realidades de la Biometría en Argentina. Biometría. Recuperado el 25 de junio de 2015, de <http://www.biometria.gov.ar/editoriales/2012/07/03/mitos-y-realidades-de-la-biometria-en-argentina.aspx>.

Los DNI electrónicos violan nuestros derechos (2014, octubre 06). Recuperado el 08 de julio de 2015, de <http://www.pensamientopenal.org.ar/dni/>

Nuevos DNI: No se trata sólo de avances tecnológicos (2014, junio 27). Asociación por los Derechos Civiles. Recuperado el 20 de septiembre de 2015, de <http://www.adc.org.ar/nuevos-dni-no-se-trata-solo-de-avances-tecnologicos/>

Pérez, Miguel (2013, mayo 24). Nigeria como modelo emergente: DNI's electrónicos con sistema de pagos integrado. Recuperado el 15 de octubre de 2015, de <http://www.blogthinkbig.com/nigeria-modelo-emergente-dnis-electronicos-sistema-de-pagos/>

Presentación del Programa Identificación Biométrica: Palabras de la Presidenta de la Nación (2011, noviembre 7). Casa Rosada. Recuperado el 10 de octubre, de <http://www.casarosada.gob.ar/informacion/discursos/25505-presentacion-del-programa-de-identificacion-biometrica-palabras-de-la-presidenta-de-la-nacion>.

Principios Internacionales sobre la Aplicación de los Derechos Humanos a la Vigilancia de las Comunicaciones (2014, mayo 10). Recuperado el 20 de septiembre de 2015, de <https://es.necessaryandproportionate.org/text>

Quina Carta Compromiso con los Ciudadanos (2012). Registro Nacional de las Personas. Recuperado el 25 de noviembre de 2014, de http://www.sgp.gov.ar/contenidos/onig/carta_compromiso/docs/RENAPER-Quinta_Carta.pdf.

Randazzo presentó las puertas biométricas en Ezeiza (2015, agosto 27). Dirección Nacional de Migraciones. Recuperado el 27 de agosto de 2015, de http://www.migraciones.gov.ar/accesible/indexN.php?mostrar_novedad=2867

Rodríguez, Pablo Esteban (s.f.). ¿Qué son las sociedades de control? Recuperado el 27 de agosto de 2014, de <http://www.sociales.uba.ar/wp-content/uploads/21.-Qu%C3%A9-son-las-sociedades-de-control.pdf>.

Schneier, Bruce (2014, octubre 24). Pasaportes RFID. Recuperado el 08 de mayo de 2015, de <http://blog.segu-info.com.ar/2004/10/pasaportes-rfid.html>.

Serratos, Francesc (s.f.). La biometría para la identificación de las personas. Recuperado el 10 de mayo de 2015, de [https://www.exabyteinformatica.com/uoc/Biometria/Biometria_ES/Biometria_ES_\(Modulo_1\).pdf](https://www.exabyteinformatica.com/uoc/Biometria/Biometria_ES/Biometria_ES_(Modulo_1).pdf).

Stallman, Richard (2012, 7 de junio). Mi última visita a la Argentina. Fundación Vía Libre. Recuperado del 27 de agosto de 2015, de <http://www.vialibre.org.ar/2012/06/07/mi-ultima-visita-a-argentina/>

Un nuevo Estado, un nuevo DNI (s.f.). Ministerio del Interior y Transporte. Recuperado el 20 de septiembre de 2015, de <http://www.mininterior.gov.ar/asuntospoliticos/pdf/nuevo-estado-nuevo-DNI.pdf>.

Revistas y Diarios:

Agamben, Giorgio (2005, diciembre 5). No a la biometría. *Le Monde*. Recuperado el 16 de agosto, de <https:// analisismadrid.wordpress.com/2011/09/05/no-a-la-biometria-giorgio-agamben/>

Anonymous (s.f.). Todo lo que SUBE... tiene que BAJAR... Recuperado el 10 de octubre de 2015, de <http://pastehtml.com/view/bm5wlsazn.html>.

Assange: “Argentina tiene la vigilancia más agresiva de América Latina” (2013, junio 27). *Infobae*. Recuperado el 27 de agosto de 2015, de <http://www.infobae.com/2013/06/27/717385-assange-argentina-tiene-la-vigilancia-mas-agresiva-america-latina>.

Busaniche, Beatriz (2012, agosto 14). El fin del derecho a la intimidad. *La Nación*. Recuperado el 08 de junio de 2015, de <http://www.lanacion.com.ar/1499039-el-fin-del-derecho-a-la-intimidad>

Caminos, Mauricio (2012, enero 31). Proponen intercambiar entre usuarios la SUBE para evitar el registro personal de viajes. *La Nación*. Recuperado el 08 de julio de 2015, de <http://www.lanacion.com.ar/1444834-proponen-que-los-usuarios-intercambien-sus-tarjetas-sube>.

Crettaz, José (2013, diciembre, 15). DNI: la privacidad, en riesgo por la identificación biométrica. *La Nación*. Recuperado el 15 de octubre de 2015, de <http://www.lanacion.com.ar/1647826-dni-la-privacidad-en-riesgo-por-la-identificacion-biometrica>.

Desde 2015, el DNI tendrá un chip para guardar más datos (2014, junio 28). *La Voz*. Recuperado el 15 de octubre de 2015, de <http://www.lavoz.com.ar/ciudadanos/desde-2015-el-dni-tendra-un-chip-para-guardar-mas-datos>.

DNI electrónico ganó premio como mejor documento de la región (2015, junio 25). *El Comercio*. Recuperado el 15 de octubre de 2015, de <http://www.elcomercio.pe/lima/ciudad/dni-electronico-gano-premio-como-mejor-documento-region-noticia-1821484>

García Fanlo, Luis (2013, marzo 06). Vigilar e identificar. Formas actuales de la sociedad de vigilancia en Argentina. *Revistas Trazos*. Recuperado el 16 de noviembre de 2014, de http://revistatrazos.ucse.edu.ar/13o_000.htm.

García Fanlo, Luis (2014). Gestión de la identidad y procesos de subjetivación en la Argentina actual (2001-2013). *Revista Trazos universitarios*. Recuperado el 16 de noviembre de 2014, de http://www.revistatrazos.ucse.edu.ar/articulos_con_referato/id_fanlo.htm.

El DNI y el pasaporte argentinos obtuvieron la norma de calidad ISO 9001 (2015, diciembre 7). *Télam*. Recuperado el 10 de diciembre de 2015, de <http://www.telam.com.ar/notas/201512/129377-dni-pasaporte-norma-de-calidad-iso-9001.html>

El nuevo DNI de Florencio Randazzo es un arma para espiar (2014, octubre 09). *La izquierda diario*. Recuperado el 15 de octubre de 2015, de <http://www.laizquierdadiario.com/El-nuevo-DNI-de-Florencio-Randazzo-es-un-arma-para-espiar>

El nuevo DNI tendrá un chip que incluirá la historia clínica de las personas y los datos de su SUBE (2014, junio 27). *Infobae*. Recuperado el 20 de septiembre de 2015, de <http://www.infobae.com/2014/06/27/1576438-el-nuevo-dni-tendra-un-chip-que-incluire-la-historia-clinica-las-personas-y-los-datos-su-sube>

Exponen en la Red los registros de viajes de la tarjeta SUBE (2012, enero 30). *La Nación*. Recuperado el 08 de julio de 2015, de <http://www.lanacion.com.ar/1444623-exponen-en-la-red-los-registros-de-viajes-de-la-tarjeta-sube>.

Fernández, Pablo Martín (2013, noviembre 04). Por una falla de seguridad se pueden descargar fotos del padrón electoral. *Infotechnology*. Recuperado el 08 de mayo de 2015, de <http://www.infotechnology.com/internet/Por-una-falla-de-seguridad-se-pueden-descargar-fotos-del-padron-electoral-20131104-0001.html>.

Randazzo anunció que “Argentina incorporará tecnología biométrica que permitirá ayudar a la justicia a identificar identidades desde imágenes” (2015, octubre 13). Ministerio del Interior y Transporte. Recuperado el 30 de noviembre de 2015, de <http://www.mininterior.gov.ar/prensa/prensa.php?i=4594>.

Randazzo promete DNI inteligente (2014, junio 27). *Clarín*. Recuperado el 10 de abril de 2015, de http://www.clarin.com/sociedad/Randazzo-promete-DNI-inteligente-viene_0_1164483877.html.

Rodríguez, Esteban (s.f). Galpones y patrones de estancia. *Revista Lote*, 94. Recuperado el 12 de junio de 2015, de <http://www.revistalote.com.ar/nro094/patrones.htm>.

Tomoyose, Guillermo (2013, noviembre 07). ¿Qué es Sibios, el sistema que tiene bajo la lupa a 40 millones de argentinos? *La Nación*. Recuperado el 08 de junio de 2015, de <http://www.lanacion.com.ar/1635928-que-es-sibios-el-sistema-que-tiene-bajo-la-lupa-a-40-millones-de-argentinos>.

Organismos Oficiales (Páginas web):

Administración Nacional de la Seguridad Social (ANSES). Recuperado de <http://www.anses.gob.ar/>.

Biometría. Recuperado de <http://www.biometria.gov.ar/>

Dirección Nacional de Migraciones. Recuperado de <http://www.migraciones.gov.ar/>

Normas 9000. Recuperado el 10 de diciembre de 2015, de <http://www.normas9000.com/que-es-iso-9000.html>

Registro Nacional de las Personas. Recuperado de <http://www.mininterior.gov.ar/renaper/renaper.php>

Real Academia Española. Recuperado de <http://lema.rae.es>.

Jornadas y Entrevistas:

El impacto de la recolección obligatoria de información biométrica por parte del Estado, en los Derechos Humanos (2014, noviembre 20). Jornada organizada por El Observatorio de Género y Derechos Humanos de los Bloques Legislativos Nacionales de la UCR y la Fundación Vía Libre, Argentina.

Te estamos vigilando (2015, diciembre 2). Jornada organizada por la Asociación por los Derechos Civiles, Argentina.

Tecnología, vigilancia y derechos personalísimos (2015, agosto19). Jornada organizada por la Carrera de Especialización en la Facultad de Derecho de la Universidad de Buenos Aires, Argentina.

Entrevista con Andrés Pérez Esquivel realizada en Buenos Aires el 23 de septiembre de 2015.

Normativas:

Constitución de la Nación Argentina (1994).

Organización de las Naciones Unidas (2008). Declaración Universal de los Derechos Humanos.

Convención Americana de Derechos Humanos (1978).

Ley N° 1.565 de Creación de Registro Civil de la Capital de la República Argentina y Territorios Nacionales, 1886.

Ley N° 4.144 de Residencia, 1902.

Ley N° 8.129 de Enrolamiento General, 1911.

Ley N° 8.871 de General de Elecciones, B.O. del 10/02/1912.

Ley N° 11.386 de Enrolamiento de Ciudadanos, B.O. del 25/10/1926.

Ley N° 13.010 del Voto Femenino, B.O. del 09/09/1947.

Ley N° 13.482 de Creación del Registro Nacional de las Personas, B.O. del 20/10/1948.

Ley N° 17.671 de Identificación, Registro y Clasificación del Potencial Humano nacional, B.O. del 29/02/1968.

Ley N° 25.326 de Protección de Datos Personales, B.O. del 30/10/2000.

Ley N° 26.413 de Registro del Estado Civil y Capacidad de las Personas del 10/09/2008.

Decreto N° 1.740 de Normas de Inscripción de los habitantes, 1857.

Decreto N° 1.172 de Acceso a la Información Pública, B.O. del 3/12/2003

Decreto N° 90/2009 de Necesidad y Urgencia, B.O. del 27/02/2009.

Decreto N° 1.501/2011 de Autorización la utilización de tecnologías digitales en la identificación de los ciudadanos nacionales y extranjeros como así también en la emisión del Documento Nacional de Identidad, B.O. del 20/10/2009.

Decreto N° 261/2011 de Reglamento para la Emisión de Pasaportes. B.O. del 02/03/2011.

Decreto 1.766/2011 de Creación el Sistema Federal de Identificación Biométrica para la Seguridad, B.O. del 07/11/2011.

Resolución RENAPER N° 169/2011 de Establece requisitos para la imagen fotográfica, B.O. del 25/01/2011.

Resolución RENAPER N° 585/2012 de Aprobación de las nuevas características de diseño del Documento Nacional de Identidad, B.O. del 19/03/2012.

Resolución RENAPER N° 797/2012 se Establece el DNI tarjeta, B.O. del 20/04/2012.

Resolución RENAPER N° 2.566/2014 de Incorporación del número CUIL como dato en el reverso del Documento Nacional de Identidad, B.O. del 12/09/2014.

Resolución RENAPER N° 2.030/2015 de Prórroga de la Resolución N° 3.117/2014 (Canje obligatorio del DNI). B.O. del 12/06/2015.

Anexo

Entrevistado: *Andrés Pérez Esquivel - Sociólogo (UBA). Asesor en seguridad y DDHH en la Legislatura Porteña. Miembro de Asociación Pensamiento Penal y la Red Latinoamericana LAVITS.*

Fecha: 23 de septiembre de 2015

-En referencia a los pedidos de informes que se realizaron al ejecutivo nos cuenta:

- Es un precedente muy importante que los organismos históricos: APDH, Madres, Liga, Fundación Vía Libre, ADC, Comisión Provincial y APP hayamos hecho este texto en torno a las tecnologías de vigilancias porque es un momento de transición. En cuanto a disputa de derechos humanos ya existen los riesgos y la infraestructura (se interrumpe por un llamado telefónico)

El tema del DNI es un debate a nivel internacional, personalmente estoy de acuerdo con el chip criptográfico y el tema de la firma digital. Esto se utiliza principalmente para acelerar trámites con el Estado, para hacer las cosas más dinámicas, más fáciles a nivel interno y el Estado está al servicio del usuario. En este sentido es bueno, pero el debate surge cuando se quiere extender a toda la población porque, básicamente, los que necesitan una firma digital o los que la pueden usar con frecuencia son pocos en la población por eso no se justifica que este dentro del DNI. Si uno quiere la firma digital porque es una empresa, por ejemplo, el Estado te puede dar una tarjeta pero no que te obligue a tenerla y menos en el DNI.

La firma digital realmente es beneficiosa, hay mucho robo de identidad en internet y esto es un mecanismo seguro. El problema es con el otro chip (con el RFID) que permite la trazabilidad, como la tarjeta SUBE, y como la normativa nacional nos obliga a tener DNI en todo momento con nosotros tenemos un problema. Uno tiene la tarjeta SUBE porque le da más beneficios, porque es más barato que usar moneda, aunque no sabemos porque no se mantiene el mismo precio con tarjeta que con moneda pero la intención es que se utilice la tarjeta SUBE. En la misma línea va el tema del DNI que se convertía en una base de datos personal portable y actualizable incluso. ¿Cuál es el otro riesgo de los DNI electrónicos para el uso de internet? Que implica un hardware especial para conectar a la computadora y esto implica muchas empresas intermediarias. Incluso Windows de España ya generó un software preparado para el uso del DNI electrónico. Está por un lado lo del hardware y por el otro lo del software, mientras que el hardware requiere instalación, gestión de generar su cuenta, tener una clave (que no se sabe quien la tiene), cuando te la dan, no hay información que pasa con todo ese uso y es difícil saber dónde está el principio y el final. Hay intermediarios e incluso se va de las manos del Estado. Es difícil usarlo por más que se haga no se va a usar, tal es el caso español que 2006 la fundación Orange publicó que solo el 0.5% de personas lo han usado, no se justifica si es cuestión de eficiencia.

En el DNI se juntan muchas cosas, varios proyectos: esta la base de datos nacional, centralizada y digitalizada de datos biométricos y el tema de la trazabilidad. Es cuestión de que avance un poco la tecnología para que uno este viajando, use la tarjeta SUBE y que al mismo tiempo, si hay una comunicación directa en tiempo real, directamente puede surgir una alerta porque ya está marcada la tarjeta (identificada con el nombre) y se empieza a realizar el seguimiento con la cámara. En cuanto a la cámara, hay que esperar que avance un poco más la tecnología para un reconocimiento facial.

- ¿Ese sistema ya está aplicado?

- Si, efectivamente. De hecho la empresa Morfo, la empresa principal, tiene diseñado un programa que se está usando en aeropuerto, porque implica cierta cuestión controlada, y es el sistema face on the fly: la persona va caminando por el aeropuerto cruzan cámaras y ya sale la identificación. Estados Unidos lo vende mucho en la ficción, ellos tienen una base pero con los que ya cometieron delitos pero se presupone (pero en realidad no es así) que tienen una base de todo el mundo. Eso es una gran diferencia con los falsos positivos y los falsos negativos. El uso de reconocimiento facial porque a nivel nacional tenés a todos los habitantes por lo tanto hay más chances. Está bien, puedes tardar más tiempo, puedes tardar más horas pero lo encontrás, al fin de cuentas descartas entre cinco y uno va a ser.

- O alguno tiene que ser...

-Sí, o alguno tiene que ser y es así.

- El método tampoco es infalible.

-El hecho de tener una base completa hace que algunos debates que se están dando en otros países sobre los riesgos de la biometría directamente se cierran por el peor lado que son los falsos positivos y los falsos negativos que puedan haber es cuestión de tiempo.

En ese sentido estaríamos siendo en país de laboratorio. Hubo tres encuentros internacionales de Biometría en Argentina en donde estaba Aníbal Fernández, también participaron gente de muchísimas empresas, vino también gente de Interpol, había mucho interés en el tema para que se aplique y también la normativa permite que se aplique. De este tema hablo muy bien Valeria Milanés (en el informe de ADC) explica toda la tradición de sesión de datos y de identificación. Hay que estar atento porque después vienen los otros proyectos que tienen que ver con lo genético.

La trazabilidad y la biometría es lo que se viene, una antesala. El principio posibilitador de todo esto es la cultura que hay en general que es “si la tecnología me lo permite, entonces lo hago” porque antes no lo podíamos hacer lamentablemente pero ahora la tecnología actúa como si fuese un posibilitador muy bueno. Por ejemplo en medicina, para algunas cosas pero no en otras cuestiones, pero no vale para todo.

- ¿Por qué pensás que Argentina vendría a ser un país laboratorio?

- Estos DNI electrónicos también son proyectos en otros países latinoamericanos con mucha fuerza. Más en la zona iberoamericana, esto tiene que ver con la región. Nosotros tenemos una vieja y larga tradición en este tema a partir del invento de Vucetich y es una condición de posibilidad que en otros países no surgió.

No se si hay algo especial con Argentina, tal vez una mezcla de cosas culturales pero también coyunturales. Interpol tiene una de las sedes más antigua en la Argentina, ahora Buenos Aires es una de las 6 sedes regionales de Interpol en el mundo (van cambiando de acuerdo al uso horario) Todo este vínculo y liderazgo argentino ante la policía internacional puede ser bien visto. También hay actores y decisiones políticas puntuales porque si hay voces en contra esto podría no suceder, no es una cuestión determinista podría ser peor de lo que es ahora, aun puede serlo, puede mejorar. No es que es Argentina porque es Argentina. Se están dando las condiciones que se llevó a esto y la idea es seguir avanzando.

-¿Por qué es un tema que no se debate?

- En general estas cuestiones vienen de la mano de políticas de seguridad. Hay una hegemonía discursiva del tópico “seguridad”, la construcción del discurso social hay un tópico hegemónico claro que es el tema de seguridad y desde ahí se jerarquiza el resto de los discursos por lo cual a veces surgen estos tipos de diálogos “sordos” no ingenuos que si alguno plantea algún reparo en

alguna de las iniciativas en donde hay un lobby fuerte genera un dialogo sordo en el cual estar de acuerdo con la seguridad y no importa lo racional, los argumentos, los fines sino lo importante es quien tiene la razón y empieza una lógica de retórica fuerte.

No hay búsqueda de consenso, no es la idea de buscar consenso en estos temas sino en imponer una cosa e ir a fondo. Por eso la única forma de frenar es anticiparse un poco o de dar un planteo más holístico, por un lado el planteo de los derechos afectados civiles por el uso de nueva tecnología y por otro lado del mismo eficientísimo que generalmente plantean estas tecnologías. Si realmente son tan eficientes como dicen ser, que pruebas se tiene que sean más eficientes y después los nuevos riesgos que trae generalmente las nuevas tecnologías incluso en materia de seguridad. Está bien, plantean que vienen a resolver los temas de seguridad pero ¿qué nuevos riesgos, problemas básicos traen? ¿Cuál es el problema por el cual se vuelve necesario crear el DNI electrónico? ¿Cuál es el serio problema sobre el robo de identidad para justificar esta medida? Eso es lo que preguntamos en el pedido de informe y nos dicen...bueno, esto tiene que ver con las tendencias internacionales, para mejorar y hacer las cosas más eficientes, mejores para todos. Hay muchas variables: legalidad, legitimidad, necesidad, idoneidad, proporcionalidad, transparencia, etc. que no se están contemplando.

-Nosotras observamos que las respuestas del ejecutivo efectivamente se respaldan diciendo que se aplican en Argentina por una tendencia internacional ¿por qué consideras que es así?

-Bueno, eso es en cuanto al DNI pero también está la base de datos que plantea otro debate porque el DNI hizo confluir varias cosas: SUBE, SIBIOS y los mecanismos de seguridad para el uso de internet. Es muy destacable que el gobierno haya hecho silencio porque en muchas cosas han avanzado igual y no les importo nada, han sido prudentes y no han vuelto a mencionar el tema del DNI electrónico pero tampoco niegan que se vaya a aplicar, con lo cual el tema está latente.

-¿Consideras que a futuro se puede dar vuelta atrás a esta iniciativa?

-El gran debate es que estas cosas se tienen que empezar a tratar en el Congreso. Puede generar debates políticos, por eso creo que han frenado un poco esta iniciativa pero también están extendiendo SUBE a todo el país. La lógica es si hay resistencia por acá, voy por otro lado, con lo que ya está aceptado.

Son muchas las variables y variantes de las cosas, son muchas las empresas y los lobby. También están los software para video vigilancia que son más automatizadas, también pueden incluir muchas de estas variables y que las normativas regulan, cuando hay normativa de video vigilancia que están totalmente desactualizadas en ese terreno.

También hay otras cuestiones riesgosas: el programa Mi Huella y AFA Plus, que es un proyecto que quedó trunco, costo mucha plata y Telecom tiene en sus servidores toda una base de datos de 40.000 personas que obtuvieron más datos que el RENAPER : sacaban la foto de perfil, de frente, llenabas una planillas con un montón de datos personales y está todo en una base de datos privada y, lo peor, es que está boyando porque el programa cerró y telecom le hizo una denuncia a Afa para que le dé una indemnización. Mientras tanto telecom tiene los datos de 40.000 personas que lo puede vender.

Mientras no haya voluntad de debatir políticamente estas cosas en el Congreso, implica repensar la Dirección de Protección de Datos personales que tiene muy poco personal y una cantidad de facultades enormes pero no tienen presupuesto y no es autónomo y problemas en la Ley de Datos Personales que si no se empiezan a corregir todo esto va a terminar en un terreno judicial y ahí los que van a decidir son los jueces y la jurisprudencia y todo el tiempo que esto genera mientras tanto siguen avanzando.

- ¿Y en el plano internacional, más allá de lo explicado del caso de Argentina?

- Estas cosas son tendencias, se están dando en el plano internacional. Los europeos tienen una tradición más fuerte en cuanto a la protección de datos personales y en ese sentido hay que mirarlos un poco a ellos.

Por ejemplo en Francia están de acuerdo con las bases biométricas pero para certificación de identidad para que no haya robo de identidad pero no para uso de seguridad pero en Argentina este tema está más complicado. Otro caso es la India que se creó la base pero cuando la quiso usar la policía se lo prohibieron. Acá, en cambio, empezó para el uso policial.

Por otro lado está la Protección de Datos en general, Francia que es anti biometría, está muy preocupada por el termino soberanía porque les están absorbiendo datos sobre su población desde EEUU y otros países, entonces están preocupados por ver cómo controlar y poner frenos. Los debates que se están dando allá son importantes para plantearlos acá porque siempre esta este doble estándar para nosotros una cosa y para los otros otra. Hay que estar atentos a los cambios que se estén dando allá para hacerlos repercutir acá, incluso en EEUU tienen debates en cuanto a este tema, hay mucha teorización sobre el tema de seguridad de esta tecnología, se está creando mucha doctrina pero con límites para dejar tranquila a la población. (Explicación de análisis del delito – triangulo de actividad) A diferencia de EEUU acá se podría hacer directamente un listado de sospechoso (con nombre y apellido) y monitorearlos con las cámaras, estas son condiciones que pueden ser posibles pero que hoy no se está haciendo, esa doctrina que se está haciendo allá de policiamiento predictivo se podría empezar a aplicar acá con un nivel de detalle que será más útil para ellos.

Lo importante es que las cosas se planifiquen y no solo por el hecho de hacer negocios, es importante que se piensen las cosas porque los riesgos pueden ser muy grandes y hay que pensar esta tecnología en las manos del peor gobierno posible y no del que más nos gusta.

En Brasil por ejemplo cuando fue el conflicto en las calles, por ejemplo, hubo bastante secuestros “preventivos”, hubo un caso que se metieron en la casa de un chico de 14 años a las 3 am por manejar una página de Facebook que llamaba a las calles y se lo llevaron frente a los padres con el argumento que incitaba a la violencia. Se buscan patrones de movilidad poblacional y no ir por todos, con las nuevas comunicaciones se puede sortear mucha censura.

En China tienen una política solida del control de su población, una tradición e incluso una política internacional

En cuanto a Argentina hay que estar a atentos a los distintos modelos, porque va a empezar a surgir modelos y la tecnología va a hacer un poco el indicador.

-Cuando la identificación es el propio cuerpo y el Estado tiene esa información es muy difícil escapar de eso (si el Estado se vuelve en contra)

-Existe el facilitador eficientita de decir “si la tecnología me lo permite lo hago” y por el otro lado. Está la idea complementaria de tratar de transmitir esa sensación de decir “no importa lo que hagas, ya estas rodeado”. Para que haya poder tiene que haber resistencia cuando hay resistencia es cuando se empieza a notar ese poder.

-Pero existe una demanda de la sociedad de estas medidas de seguridad, existe una aceptación de este tipo de medidas

-Si, ahí está el debate fundamental que tiene que ver con el tema de seguridad, ahí están los grandes proyectos por eso es tan importante aprender sobre las medidas de seguridad y hacer propuestas y no solo criticar. Racionalizar las demandas y generar propuestas en medida de

seguridad, es un tema muy importante pero cuando se convierte en un negocio o genera más inseguridad es un problema. Una cosa es el proyecto y otra es como se termina aplicando.

Evento: “Nuevo DNI: ¿qué datos son necesarios para identificarnos?”

Organización: Manuel Garrido (diputado nacional UCR-Capital) organiza, junto con el Observatorio de Derechos Humanos y Género de los Bloques Legislativos Nacionales de la UCR

Fecha: 7 de agosto 2014

Participantes: *Beatriz Busaniche – Representante de la Fundación Vía Libre.*

Eleonora Rabinovich – Representante de Asociación por los Derechos Civiles.

Luisa Storani - Titular Observatorio de Derechos Humanos y Género.

Manuel Garrido - Diputado Nacional UCR-Capital

Katarzyna Szymielewicz - Presidenta de la Fundación Panóptico

Presentación: Beatriz Busaniche (Fundación Vía Libre)

Impacto en los DDHH de estas políticas estatales que se están implementando. Por un lado el avance de la tecnología y, como este avance, es utilizado por el Estado de mayor manera en la recopilación de datos biométricos, cámaras, cuestiones novedosas pero que impactan en los derechos humanos.

Varias organizaciones que siguen con preocupación el avance de identificación de ciudadanos, el avance de incorporación de tecnología para la vigilancia que consideramos que no están teniendo el debate público que merece. Consideramos que todas estas medidas deben pasar por el Congreso Nacional pero lamentablemente las decisiones se toman por resoluciones administrativas y hoy nos convoca un tema que nos genera preocupación, que ha puesto al país a la vanguardia de estos temas a nivel internacional por la incorporación del sistema biométrico y la ampliación de los datos que se utilizan para la identificación de los ciudadanos. La incorporación de SIBIOS que es el sistema integrado de identificación biométrica que se implementa en Argentina a partir de un decreto anunciado por la presidenta Fernández de Kirchner en noviembre 2011 por cadena nacional, en la cual hizo una descripción muy detallada. Ese sistema que seguramente varios ya han pasado en la renovación del DNI y también en el momento de ingreso y salida del país en los aeropuertos.

Es un momento en que cada vez se están incorporando más tecnología y no sabemos cuáles son los objetivos, no sabemos cuáles son los alcances, Manuel (Garrido) hizo un pedido de informe al RENAPER sobre el nuevo DNI y la respuesta fue muy pobre, contribuyo muy poco para entender cuál es el proceso de este nuevo DNI. Y cuando decía que Argentina está a la vanguardia de estos temas, lo decía porque esto no es lo común. Primera cuestión: no todos los países tienen tarjeta de identificación, el DNI está muy naturalizado aquí pero no es así en el mundo y eso se debe a una matriz autoritaria (Ley 17.671 vigente desde la revolución Argentina 1968), alcanza con ver la ley para ver la matriz autoritaria. Es necesario un cambio de esa ley y ponerla en términos de DDHH y no en términos de “capital humano nacional”, la actual ley dejar en claro que los ciudadanos están subsumidos como capital del estado.

Lo que llama la atención es que se presenta como que está a nivel del primer mundo. Cuando uno lo escucha a Florencio Randazzo que anuncia que vamos a tener un DNI con chip, con base de datos de salud, con la base de datos de seguridad social, base impositiva dentro del mismo DNI y se lo promociona como a la vanguardia, al nivel de los países europeos. Podemos conocer y debatir con Katarzyna Szymielewicz el estado de los niveles de identificación en los países europeos, discusión de la incorporación de sistemas biométricos que además alcanza o pretenden alcanzar la identificación del ciudadano en el espacio público todavía no se hace pero temeriza escuchar a la presidenta cuando hace el anuncio de SIBIOS decir que se van a poder

cruzar los datos de las cámaras de vigilancia del espacio público con la base de datos de reconocimiento facial que tiene SIBIOS y saber quién es quién al instante en el espacio público “para conocernos mejor” (slogan de la campaña).

¿Qué nivel de avance hay en estas tecnologías? Sabemos que Argentina está comprando tecnología de vigilancia e interceptación de comunicaciones, sabemos porque legisladores del partido verde han solicitado un informe para saber que está exportando Alemania en el informe de las exportaciones da que Argentina ha estado comprando por miles de euros tecnologías de vigilancia a este país. Desde Vía Libre estamos solicitando a los legisladores una ampliación para saber qué es lo que compra argentina. Estas son cuestiones que no afectan solo a un país sino que debe ser abordado a nivel global porque son grandes empresas que proveen estas tecnologías, muchas radicadas en Europa o en EEUU.

Hay que poner la mirada en los tratados internacionales que regulan las exportaciones de estas tecnologías como el Convenio de Wassenaar¹ hay que poner la mirada en quienes compran y venden, es por eso que nosotros entendemos que la cooperación de las organizaciones internacionales es clave. Nos enteramos que Argentina está comprando tecnología porque hay un grupo en Alemania interesado en esto que pide explicaciones a su gobierno. Entonces la cooperación internacional en este tema es clave porque es la única forma de cruzar información y articular estrategias de defensa conjunta. Cuando viene Bandazo y dice “esto se incorpora en Europa”, al menos desde nuestro punto de vista, los países que más han avanzado con los sistemas de datos de identificación son aquellos que han tenido una trayectoria autoritaria más larga: Portugal tuvo la dictadura más larga en Europa en el siglo XX y es el primero, España, Estonia. Por su parte Inglaterra en 2010 derogo el sistema biométrico por exigencia del congreso, se mandó eliminar la base de datos que se estaba conformando.

El tema que hoy nos convoca es muy complejo, requiere abordaje técnico, abordaje jurídico, abordaje de DDHH, requiere un abordaje interdisciplinario.

Katarzyna Szymielewicz: Puedo contribuir en traer la discusión que se da en Polonia, país de origen, y en la Unión Europea sobre este tema.

Cuando escuche por primera vez hablar de SIBIOS retrotrajo lo que también el gobierno polaco esta también tratando de remodelar.

Beatriz: Está avanzando sistemáticamente a nivel mundial.

Katarzyna Szymielewicz: La perspectiva es que los gobiernos se están dando cuenta que tienen una gran cantidad de bases de datos y las planean unificar. Acá hay otro actor fundamental que son las grandes corporaciones que producen estas tecnologías y está empujando porque es un gran negocio entonces hacen presión en los gobiernos para que compren estas tecnologías.

Además de los gobiernos y las personas que lo venden hay un tercer actor es la Unión Europea que tiene una gran cantidad de fondo para invertir en proyectos de este tipo y financiar este tipo de iniciativas y del otro lado tenemos organizaciones de ciudadanos preocupados por la privacidad, hay una asimetría enorme en las condiciones de la discusión.

La estrategia que estamos tratando de hacer desmantelar este discurso de la modernización, porque lo que viene es un sistema más profundo de vigilancia.

Nuestra estrategia es plantear que si el gobierno quiere crear una nueva base de datos o darle un uso distinto a la base de datos que ya tienen entonces nos tiene que explicar ¿qué quiere hacer y por qué? No tiene que dar por hecho de la cual no tiene que dar explicaciones.

Es nuestra visión de la privacidad que cada base de datos debe ser considerada, cada nuevo uso de base de dato debe estar prohibido y debe ser justificado bajo los principios de necesidad.

Lo que escucho sobre SIBIOS, que el gobierno avanza sin explicaciones como si tuviera el derecho de hacerlo y es exactamente lo contrario tiene prohibido hacerlo y si lo quiere hacer tiene que hacerlo con autorización y el debido debate parlamentario y las explicaciones del caso.

No tengo los detalles de esta base de datos pero el punto de inicio es poder definir ¿cuál es el propósito? Si el gobierno pone alguna razón como por ejemplo: vamos a combatir el terrorismo o queremos ahorrar fondos en el sistema de Salud público, optimizar algún plan social, para utilizar mejor el gasto, etc. Lo primero que tiene que hacer es evaluar si eso son medios legítimos para la sociedad.

Podemos imaginar que manejar mejor el gasto social o administrar mejor el gasto público podría ser una meta deseable en Argentina. Segunda mirada es ver si esta nueva tecnología que se quiere implementar es el método apropiado para alcanzar ese objetivo.

Después de hacer investigaciones en Polonia vimos que los mismos objetivos se podrían lograr con los datos que ya tienen o con un mejor uso de esos datos pero no con medidas de este tipo.

Si el objetivo y la medida a tomar coinciden, lo que hay que evaluar cuál es el costo que va a pagar la sociedad por esa medida. El gobierno puede argumentar que teniendo todos estos datos el Estado puede mejorar por ejemplo en salud pero si el costo es tener toda la base de datos biométricos de la población, incluso hacia futuro puede que este momento no haya tal riesgo pero no sabemos si en 10 años puede cambiar la perspectiva y puede haber un gobierno que decida discriminar, excluir o incluso eliminar a un grupo de la sociedad por distintas razones.

Tenemos que poner este tema dentro de la discusión y advertir los potenciales riesgos que existen porque aunque no parece posible ahora, nunca se sabe cuándo una dictadura o gobierno opresivo puede repetirse.

Los datos son un recurso extraordinario, es una herramienta muy poderosa y una vez que nos desprendemos de esos datos es muy difícil recuperar. Una vez que estos datos están en manos de las corporaciones o del gobierno es muy difícil saber que va a pasar con ello, hemos perdido el lazo con estos datos y es muy difícil recuperar. Los datos son una parte fundamental del ser humano.

Hay otros aspectos cuando entramos en los aspectos de biometría. Cuando el estado comienza a obtener datos biométricos la relación con el ciudadano cambia. El origen del estado (teoría contractualista) es un ciudadano, sujeto libre que concuerda en la conformación del Estado. Es bastante abstracto lo que estoy diciendo pero hay que entender que no llegamos a esta cuestión social como cuerpos sino como sujetos sociales. Por ejemplo personas que no son ciudadanos de este país no tiene derecho a elegir gobernantes, puedo cambiar mi identidad puedo cambiar mi nombre (ejemplo: en Alemania nazi los ciudadanos tuvieron que cambiar su identidad porque el estado los perseguía) si cambiamos la simple identificación del ciudadano a los datos corporales cerramos la salida de emergencia de poder cambiar cuando la identificaron es tu propio cuerpo. Quizás estoy planteando una apología de engañar al Estado pero no siempre el Estado es bueno y hay épocas que engañarlo es legítimo.

Esto es difícil decirle a los políticos porque les estamos diciendo que nosotros no le estamos dando confianza ilimitada sino que es una confianza LIMITADA.

A mi parecer esta es la diferencia entre un Estado democrático y uno totalitario. Si veo que el acuerdo que dio origen a mi Estado se me está volviendo en contra tengo la posibilidad como ciudadano de salirme de ese acuerdo e irme. A lo largo de la historia el registro biométrico se realizaba en los grupos marginados: esclavos, los presos, los grupos que de alguna manera la sociedad ha castigado o marginado.

El mayor cambio que estamos viendo que incluso ciudadanos libres que tienen una buena relación con el Estado que no son sujetos de ningún tipo de sospechas son objeto de recolección de datos biométricos.

Los estados modernos deben darles a los ciudadanos la opción de elegir. Si el Estado dice que si das todos los datos te voy a ofrecer el mejor sistema educativo o salud entonces puede realizar un intercambio libre pero el ciudadano siempre tiene que tener la opción de no entregar esos datos. Si tengo el Estado detrás de mí unificando todas las bases de datos, las cuales les he ido entregado a lo largo de la vida por diferentes razones entonces no tengo esa libertad.

FIN DE INTRODUCCION

Manuel Garrido: ¿Qué debates se plantearon en Europa sobre este tema?? (pregunta a Katarzyna Szymielewicz)

Katarzyna Szymielewicz: No estoy al tanto de ningún fallo Europeo. Aparentemente no hay ninguna ley porque las competencias de los Estados son diferentes al interior de cada país de la unión Europea. Estos casos mayormente lo discuten los tribunales nacionales porque los reclamos se realizan en el tribunal constitucional nacional no al europeo. Sé que hubo discusión fuerte en Holanda sobre la incorporación de biometría y fue ganada por los ciudadanos que rechazaron este tipo de registros. Austria impulsó una división de datos, entre el número de identificación y el resto de las distintas bases de datos. En Polonia no hay regulación estricta en el registro de datos. Hubo un proyecto de unificar la base de datos de educación y salud pero se solicitó la intervención del Defensor del pueblo para que explique que alcance tendría esta unificación.

Manuel Garrido: En Argentina no hay designado Defensor del Pueblo

Katarzyna Szymielewicz: No estamos discutiendo si debe o no haber base de datos, lo que se está discutiendo es la magnitud de esas bases de datos y quienes tienen acceso. Estamos viendo que algunos casos tienen acceso de datos la policía o los médicos pero siempre debe existir una forma de saber quién ha tenido acceso a esos datos y un sistema de control de acceso a esas bases de datos. Estos sirven para evitar el control total por parte de un cuerpo político o una parte del gobierno.

Sería inconcebible en Polonia que un funcionario político decidiera obtener toda la información de un ciudadano y poder obtenerla sin ningún control. (Sea el jefe de policía o primer ministro) nunca hay un interés legítimo que justifique el acceso completa a la base de datos de un ciudadano.

Eleonora Rabinovich (Asociación por los Derechos Civiles) Creo que la situación en la Argentina en general de la población frente a las políticas de registro de los datos es bastante permisible sobre todo en los últimos años con el discurso de seguridad y combate sobre el crimen. Hay una aceptación e incluso un pedido que haya mayor cantidad de políticas que tenga que ver con cámaras de vigilancia, registro de datos personales (demanda social) Llegamos al tema de SIBIOS en donde se está implementado una política con muy poca información a la sociedad. Desde ADC se hizo una investigación en donde se demostró la falta de seguridad de muchas bases de datos estatales. La pregunta es ¿cuál es la experiencia de inseguridad en las base de datos en Polonia o Unión Europea, filtrado de información?

Cuando queremos advertir sobre estas cuestiones parece un daño hipotético frente a un beneficio (necesidad) concreto.

Beatriz Busanечи: Por ejemplo: La base de datos fue transferida sin ningún control a la autoridad electoral de votación y se puso directamente en Internet (dirección, foto y todos los

datos) Además esa misma base de datos fue descargada y se presentó un amparo sobre eso y la autoridad responsable se negó a dar una explicación sobre los controles de seguridad.

Katarzyna Szymielewicz: Hay que tener en claro que una vez que existe la base de datos las filtraciones van a ocurrir, las grietas de inseguridad. Hay un proyecto en Polonia de hacer perfiles de personas desempleadas para ajustar mejor la clase de apoyo que pueden recibir, en principio tiene sentido pero cuando ves la implementación, tienen datos de salud, el cuestionario es muy intrusivo, hay una pérdida grande en los individuos. En esta transacción el ciudadano pierde, es asimétrica.

Estuvimos trabajando en capturar estas historias tenemos varios casos de gente que no recibe ningún beneficio de todo esto porque han sido catalogados en una categoría equivocados y ni siquiera pudieron enterarse como los habían catalogado.

Encontramos personal encargado de confeccionar estas bases que nos han filtrado las preguntas correctas que deberían responder. Porque muchos funcionarios estaban en de acuerdo con la implementación de esto y con la colaboración tuvimos en condiciones de demostrar como fracasa este sistema y como genera condiciones de discriminación y exclusión. Esta es la mejor forma porque los ciudadanos se ven afectados, es una nueva forma de discriminación y exclusión.

Beatriz Busaniche: Por ejemplo: Datos AFIP.- Ver protección de datos

Eleonora Rabinovich: Ley Base de datos personales.

Penalmente se busca, por ejemplo, armar un registro de delincuentes, de violadores ¿cómo entienden ustedes esta cuestión?

Katarzyna Szymielewicz Se está discutiendo, entienden que esta idea de armar bases de datos es una forma de abordar el tema. Porque es estigmatizante y genera otro tipo de castigo también. Los criminales deben ser castigados de acuerdo a lo que hayan hecho y se debe incluir mucho trabajo para reinsertarlo. Incluso después que dejan la prisión se le puede hacer algún tipo de seguimiento, de trabajo posterior. Pero eso es una relación entre ellos y el Estado punitivo y no en relación con el resto de la sociedad. Si terminas en la base de datos de los violadores nunca vas a reinsertarte en la sociedad, y antes de hacer esto deberíamos considerar que hay gente que debe ser excluida por siempre y eso es un castigo de por vida. No podemos pretender que han vuelto a la sociedad pero a su vez que se los mantenga excluidos por esta base de datos.

Manuel Garrido: Hace dos años este tema se discutió y me lleva a enlazar con algo que mencionaste y porque se hace tan difícil debatir este tema en la Argentina. Todos los documentos desde siempre tiene la huellas digitales de cualquier ciudadano e inclusive, uno de los mitos en la Argentina que uno de los inventores de las huellas digitales es argentino. Tenemos instalado y naturalizado que el Estado recopila datos biométricos para identificar a todos los ciudadanos y mi reflexión es en cuanto al registro de violadores (de ADN) y yo me opuse...se me cuestiona porque no se puede hacer un registro de ADN cuando el Estado ya tienen las huellas digitales de todos los ciudadanos. Con estos precedentes se sigue avanzando en la recopilación de datos biométricos. Desde hace muchos años recopila datos biométricos, es "Orgullo Nacional" y eso se utiliza para justificar otra base de datos más complicada como esta que mencionamos de ADN para los que cometieron delito contra la integridad sexual.

Participante: ¿cuál es la reacción de la sociedad en tu país? como decían acá hay una inercia ante esto e incluso un orgullo. La gente no es consciente, incluso se sienten más protegidos con las cámaras ¿no te parece que esto le deja el camino libre al Estado para seguir avanzando en estas políticas?

Katarzyna Szymielewicz: La sociedad polaca ha atravesado por una transformación muy dinámica (de una sociedad comunista a Capitalista). La sociedad se ha movido no solo de ciudades sino de clase sociales. Hemos reconstruido las sociedades, por ejemplo, ahora soy una ciudadana de 40 años, viviendo en capital con mi familia pero mis padres fueron agricultores en las áreas rurales. En estas cuestiones es muy normal que la gente intente diferenciarse con aquellos que están peor. Muchas veces se incorporan técnicas de vigilancias (video) por esa razón para diferenciarse del otro.

Tenemos muchos territorios marcados y vigilados que es de la gente rica. No son solo cuestión de seguridad sino cuestión simbólica para demostrar una diferencia. Nosotros hacemos un planteo de cómo debería ser una sociedad si esta gente que está detrás de los muros no debería integrarse con el resto y sería una sociedad más feliz.

Hay investigaciones que demuestran que esta dinámica hace incrementar la inseguridad porque aquel que va a robar se ve más motivado a violar la defensa de aquella persona que está viviendo ahí.

Incluso hay investigaciones psicológicas que dicen que las personas que viven en estos Getxo cerrados terminan con una sensación mucho mayor porque vive en prisión. Siente que necesita más y más seguridad permanentemente. Estamos usando muchas investigaciones que surgen de estos trabajos empíricos porque hay mucha gente que cuando sale de esa situación quiere irse a vivir a África porque extraña el lazo con la comunidad, en contexto de aislamiento.

Esto no es que se vaya a poder cambiar en un año pero estas experiencias pueden ser utilizadas para transformar porque hay gente que realmente está mostrando un cambio muy negativo en su vida a partir de esta dinámica. En Varsovia y el resto de Europa hay muchos grupos emergentes que están dando esta discusión, la disputa por el espacio público, lugares para compartir algunos con una mirada más divertida, más crítica pero todos en la disputa por el espacio público y la reintegración. Quizás en 20 años seremos como Berlín ahora en donde la gente no simula ser lo que no es y vive el espacio público de una mejor Manera.

Luisa Storani: Las cámaras en el espacio público porque ahora todos vivimos como en un gran "espacio cerrado". En CABA todos somos filmados, todo el día, todo el tiempo. Esto también es una idea de encierro, sos libre pero estas siendo filmado y nadie tiene una conciencia de que esto está pasando las 24 hrs. ¿Esto sucede en Europa? ¿Utilizan las filmaciones en las calles?

Katarzyna Szymielewicz: esto es otra gran parte de la discusión. Es otra lucha dentro de la organización Panóptico porque las cámaras de vigilancia no están reguladas. Estamos casi convenciendo al gobierno que las cámaras deben ser reguladas. Hay borrador de Ley que va a ser puesto en consulta pública para los ciudadanos. Sé que va a establecer reglas claras y firmes de cuando las cámaras podrán ser colocadas en espacios públicos y ser justificados de alguna manera y deben ser sujetas al órgano que controla la protección de datos. Tiene que haber un registro de la base de datos y una explicación a los ciudadanos, que la cámara pertenece al Congreso, los datos ara saber con quién se debe contactar si uno quiere saber más sobre los datos de esa cámara. Una regla estricta de cuanto puede durar el registro que quien puede usar ese registro.

Nosotros creemos que con la ley va a cambiar la mentalidad sobre el tema pero actualmente en Polonia está pasando algo similar que en Argentina, las autoridades locales están enamoradas de las cámaras y gastan fortunas.

Manuel Garrido: no hay reglamentación que regule el foco de la cámara, hacia donde está dirigida puede tomar la puerta o la ventana de tu casa.

Eleonora Rabinovich: hay un acuerdo entre el gobierno de la ciudad que deben ceder a los medios de comunicación las filmaciones

La Ley 25.886, Ley Blumberg del 2004, obliga a crear el registro público de usuarios de telefonía móvil (nunca se reglamentó) incluye datos filiatorios.



El Impacto de la recolección obligatoria de información biométrica por parte del Estado, en los derechos humanos

**20 de noviembre de 2014 a las 10, Salón Perito del Edificio Alfredo Palacios
Hipólito Yrigoyen 1708, 5ºPiso**

El Observatorio de Género y Derechos Humanos de los Bloques Legislativos Nacionales de la UCR junto con la Fundación Vía Libre y el Diputado Manuel Garrido tienen el agrado de invitarlos a la continuación del desayuno de trabajo "Nuevo DNI: ¿Qué datos son necesarios para identificarnos?". Esta vez exploraremos el impacto en los derechos humanos de la recolección obligatoria de información biométrica por parte del Estado.

Los Presidentes de los Bloques Nacionales de la UCR, Senador Gerardo Morales y Diputado Mario Negri, abrirán el encuentro en el que contaremos con la presencia de **Katarzyna Szymielewicz (Fundación Panoptikon) y con Katitza Rodríguez (Electronic Frontier Foundation).**

Las invitadas expondrán sobre los riesgos que implican la expansión de las tecnologías de reconocimiento facial, en conjunto con la identificación biométrica y con la implementación de cámaras de seguridad en la vía pública, para el resguardo de la privacidad, el derecho a la libertad de expresión, la participación en la vida pública y política, y el ejercicio de nuestros derechos ciudadanos.

Katarzyna Szymielewicz es abogada y activista. Graduada en Derecho y Administración por la Universidad de Varsovia, y en el programa de estudios sobre desarrollo de la Universidad de Londres, en la Escuela de Estudios Orientales y Africanos. Es co-fundadora y presidente de la fundación polaca Panoptikon (<http://panoptikon.org/>), y vicepresidenta de la coalición "European Digital Rights" (EDRI: <https://edri.org/>).

Katitza Rodríguez es graduada en Derecho por la Universidad de Lima, Perú, y actualmente es la directora internacional de derechos de la EFF (Electronic Frontier Foundation: <https://www.eff.org>). Katitza se especializa en políticas comparadas de privacidad a nivel internacional, concentrándose sobre todo en la aplicación de las leyes, la vigilancia gubernamental, y el intercambio de datos personales entre países.

Evento: “Tecnología, Vigilancia y Derechos Personalísimos”

Organización: Carrera de Especialización de Derecho Informático – Facultad de Derecho de la Universidad de Buenos Aires.

Fecha: 19 de agosto de 2015

Expositores: *Andrés Pérez Esquivel - Asesor en seguridad y DDHH en la Legislatura Porteña. Miembro de Asociación Pensamiento Penal y la Red Latinoamericana –LAVIT*

Eduardo Petudo - Director del Centro de Protección de Datos Personales de la Defensoría del Pueblo de la Ciudad Autónoma de Buenos Aires.

Valeria Milanés – Integrante de la Asociación por los Derechos Civiles –ADC-

Eugenia Carrasco - Investigadora del Instituto Latinoamericano de Seguridad y Democracia –ILSED-

Presentación a cargo del Dr. Eduardo Quiroga (Director de la Carrera de Especialización de Derecho Informático)

Video vigilancia, Biometría, drones y protección de datos personales

Licenciado Andrés Pérez Esquivel -Sociólogo (UBA). Asesor en seguridad y DDHH en la Legislatura Porteña. Miembro de Asociación Pensamiento Penal y la Red Latinoamericana LAVITS.

Analizar las bases biométricas que se están construyendo a nivel nacional e internacional como un paso a las sociedades predilectiva o como plataforma que permite habilitar el paradigma de policiamiento predictivo, entre otras cosas.

En primer lugar es importante tener en cuenta que la autodeterminación informativa general, la protección de datos personales y en general los datos biométricos se están convirtiendo, cada vez más, en un derecho que debe ser abordado desde una óptica colectiva como un derecho de los pueblos. Los certificados de identificación que el Estado otorga a las ciudadanos deben usar algunos datos biométricos sin embargo esto no significa que es necesario crear una base de datos nacional, centralizada y digitalizada que copie y reúna los datos biológicos de toda la población. Es una copia fiel de nosotros mismos en una base de datos centralizada. Esto otorga mucho poder a quien la administra y a quien la crea. Estas bases definen ¿Quiénes somos? ¿Qué somos? Algo que hasta unos años no sucedía.

Estas técnicas convierten a las individuos en individuos porque se toman rasgos únicos e irremplazables, este tipo de almacenamiento que siempre estuvo para quienes realizaban crímenes dilectivos aumenta la escala de sospecha a toda la población en post de crear perfilados sociales. Hoy aproximadamente un 20 % de la población mundial forma parte de una base biométrica nacional, siendo la India un caso paradigmático.

La utilidad de estos perfilados sociales puede tener fines de carácter social, comercial, policial e incluso militar. Los principales interesados son las potencias militares, las agencias internacionales de seguridad (INTERPOL) entidades financieras (Banco Mundial) que estas promoviendo estas bases y estos programas de identificación nacional en África y en distintos países periféricos para usos múltiples y de modo experimental. En cuanto a los usos de aplicaciones militares podemos mencionar a EEUU que considera estos datos de valor estratégicos en materia de defensa, combate al terrorismo. De hecho han realizado un programa en Irak para registrar a la población de manera de anticiparse a un posible ingreso a su propio territorio, el visado para entrar a EEUU incluye la extracción de los datos biométricos, las diez huellas digitales, entre otras cosas. Varios países centrales, en este sentido, no aceptan este tipo de bases para sus propias poblaciones como es el caso de Francia, Inglaterra y el mismo EEUU

pero si las promueven para otros países u otras regiones como es el caso de India, África, Latinoamérica o se lo aplican a poblaciones de otros países cuando quieren emigrar o piden refugios en sus áreas. Ahí cabe destacar el caso de la base de Eurodac (Zygmunt Bauman hace un buen análisis del concepto del Banóptico, la biométrica como un instrumento para poder expulsar) reúne datos biométricos de 2 millones de personas y permite que si una persona pide refugio en un país y es rechazada, puede pedir en otro país y también va a hacer rechazada porque hay una base centralizada. Podemos mencionar el caso de Israel y Palestina: Israel ha creado bases no reguladas tanto para refugiados como para los palestinos (se extraen las huellas, el iris entre otras cosas) y es la única manera en que los palestinos pueden tener un permiso temporal para cruzar los puestos de control israelíes. En los últimos años Israel promovió la creación de una base nacional de datos biométricos y el DNI electrónico, esto ha generado bastante debate, se sancionó una ley con periodo de prueba, se iba a aprobar en mayo y finalmente se extendió nuevamente el periodo porque se denunciaron muchas irregularidades, muchos problemas en la base de datos e incluso la Corte Suprema tuvo que fallar diciéndole al gobierno que aclare que no era obligatorio la inscripción en esa base porque estaba en periodo de prueba, ya el gobierno estaba promoviendo otra cosa.

En cuanto a los servicios sociales es importante prestar atención a los programas con transferencias condicionadas que promueven el Banco Mundial (nosotros ya conocemos) el caso más significativo en Argentina es la AUH (Asignación Universal por hijo) en cuanto a lo condicional dice que el subsidio está pero uno tiene que mostrar que el carnet de salud y el escolar que están completos, estas son las condicionalidades. Algunos son más punitivos o menos punitivos, el de la AUH es poco, por suerte, y mostro buenos resultados. En cambio en otros países dentro de estas condicionalidades esta la entrega de datos biométricos porque va de la mano de la construcción de las tarjetas, de estos DNI de identificaciones, en países que nunca tuvieron.

Hay muchas empresas participando, si bien Inglaterra, Francia no están de acuerdo con esto, sus empresas si participan en estos programas por ejemplo en la India y ahí es importante destacar el proyecto “Aadhaar” que es el programa más ambicioso en materia de biometría, no fue aprobado por ley en el Congreso Nacional pero está avanzando y está a punto de terminar con el objetivo de empadronar a 1300 millones de personas, hasta el momento hay más de 1000 millones y estaría terminando a fin de este año. Por primera vez en la historia de la humanidad se centralizan los datos biográficos y biológicos digitalizados de un 15 % de la humanidad en un disco rígido (dos o tres discos). Estamos hablando de huellas, iris, rostro, datos clínicos, domicilio, teléfonos, familiares, etc. También hay que mencionar casos de dos ciudades que anunciaron que perdieron las bases, tuvieron un problema y convocaron a todo de vuelta a inscribirse. Esta tarjeta se está convirtiendo casi en una condición para acceder a muchos servicios (muestra un folleto de la India que dice: base biométrica más grande del mundo y describe los servicios sociales que se puede acceder como gas, servicio social, transporte, etc.) La importancia de esto ha llevado a que en muchos casos las empresas concesionarias decían que no prestaban el servicio hasta que no tuviesen la tarjeta Aadhaar, al punto que la Corte Suprema tuvo que fallar diciendo que no se puede negar un servicio básico por no tener la tarjeta por no estar inscripto, en especial porque no hay ley sancionada.

Por otro lado hay un fallo importante de la Corte Suprema de la India que cuando la policía quiso empezar a pedir información de esas bases (una vez que están creadas. ¿Por qué no?) La Corte Suprema le negó la información y argumentó que sólo se puede usar para servicios sociales e identificación pero no para uso policial.

En Argentina, en cuanto a transferencias condicionadas tenemos al ANSES con el programa “Mi Huella”, todos los jubilados deberán identificarse con sus huellas en cajeros automáticos para poder cobrar su jubilación, la AFIP también ha creado su base biométrica para que se

pueda acceder a un registro impositivo en la obtención de un empleo. Para acceder al derecho del Transporte, también está la cuestión de tipo electrónico no biométrico que es la tarjeta SUBE, ya no es tan condicionante pero en principio si era condición, incluso hay incentivos como que cueste más barato el boleto o que se pueda reintegrar el dinero en el caso que se pierda la tarjeta.

¿Por qué es importante el fallo de la India? Porque refiere a la extensión del uso, en estos litigios legales se debate si la policía trabaja con otras instituciones o no a la hora de pensar este esquema de policiamiento predictivo y utilizar todas estas bases biométricas. Hay tres escenarios: que no trabaje, que si trabaje o que trabaje a través de otras instituciones, tomando a estas, instituciones, como una extensión de la institución policial al servicio de las investigaciones e incluso en el paradigma de policiamiento predictivo que es algo concreto.

Este principio de policiamiento predictivo se basa en que para combatir la delincuencia los Estado deben reunir toda la información disponible de la mayor cantidad de gente posibles para poder abordarla fácilmente cuando decida volverse mala o incluso antes. De la prevención se pasa a la anticipación, no solo poder seguir a los que ya cometieron delito sino a las personas de su entorno para monitorear en el caso que suceda una reiteración y también de las personas que se sospecha y ,en este caso es importante, tener en cuenta todas las variantes tecnológicas como SIBIOS porque estamos hablando de una base que pueden acceder todas las policías (El registro era de la policía, se pasó a manos civiles y a través de SIBIOS fue devuelto a la policía y sin restricciones) es una base distinta, una base digitalizada, más sólida y extendida a toda la población. Tenemos la India que no deja usar la base a la policía y en Francia está prohibido, fue declarado anticonstitucional dos casos paradigmáticos importantes para pensarnos también a nosotros. No es menor tener en cuenta que Argentina desde el 2014 es el primer país en participar en Comunidad de Policías de América (AMERIPOL) con todo el ministerio de Seguridad y no con toda la fuerza como lo hacen otros países y que Buenos Aires se ha constituido en una de las 6 sedes regionales de INTERPOL en el mundo y que el actual Secretario de Seguridad Nacional, Sergio Berni, se convirtió en un representante de las américas (Comité ejecutivo de INTERPOL) que es un organismo muy activo en este terreno.

Uno de los derechos que se ve afectado es que la Biometría se está convirtiendo en un requisito obligatorio para tener derecho a tener derechos, incluso para elegir representantes. Por otro lado afecta el principio de inocencia al invertir la carga a la prueba “todos somos culpables hasta que nuestro cuerpo demuestre la contrario”, también el derecho a no autoincriminarse: el silencio es considerado una garantía ante cualquier presión pero los datos biométricos pueden extraerse compulsivamente y la expansión de necesidad de identificarse frente al Estado y los privados obligados a la suspensión de derechos por breves lapsos que caracterizan regímenes o patrones autoritarios.

¿Qué medidas se pueden tomar en el plano internacional? La primer pregunta que hay que hacer es ¿qué problema grave de suplantación de identidad existe para crear estas bases? ¿Qué problemas vendrían a resolver estas bases? (la funcionalidad parece múltiple) y si no se pueden responder estas preguntas pensar en la posibilidad de no crear estas bases como ha sucedido en algunos países. Discutir los principios de legalidad, legitimidad, finalidad, necesidad, proporcionalidad, idoneidad y transparencia y control público son fundamentales, una base de consenso que deberíamos tener. No se pueden negociar, estas cosas deben cumplir con estos principios. En el caso de Argentina, quieren crear en el DNI una pequeña base de datos portable para usos múltiples. Junto a 8 organizaciones se ha presentado una solicitada en que propusimos: existe SIBIOS, existe Sube, quieren hacer el DNI electrónico, es todo valido pero esto no puede no pasar por el Congreso, estos principios tienen que discutirse en el Congreso y tiene que ser con una ley como está sucediendo en la mayoría de los países y además restringen el uso policial mientras que en este país no tenemos ni ley y habilitamos el uso policial. Es

importante tener en cuenta los riesgos que esto tiene, no naturalizar estos avances y que estas cuestiones, estos debates deben pasar por el Congreso.

Licenciado Eduardo Petudo - Director del Centro de Protección de Datos Personales de la Defensoría del Pueblo de la Ciudad Autónoma de Buenos Aires.

Privacidad e intimidad quiero hacer referencia al salto conceptual constitucional entre la Constitución Nacional (que pese a la reforma no se ha modificado el art 19) y la Constitución de la Ciudad de Buenos Aires que pone el centro en una de las cuestiones que estamos abordando cuando detalla en su artículo 12 inciso 3 que el derecho a la privacidad, intimidad y confidencialidad la Ciudad garantiza como parte inviolable a la dignidad humana, esto nos acerca a lo que hoy estamos tratando de abordar. El conjunto de problemas que tenemos que encarar es de múltiple abordaje, por un lado esta lo institucional, por otro lado esta lo normativo pero hay un sustrato o una sobre determinación (según el marco conceptual) que es la **cuestión cultural**, en este último eje se encuentra uno de los principales componentes de aquello que tenemos que abordar desde no solamente enfoques multidisciplinarios o transdisciplinarios sino que atraviesen a la sociedad civil. Hago una mera referencia (comparación entre los dispositivos de los años 60 y la actualidad) hay una presión social que los transforma en descartable.

Datos biométrico y el poder, no me refiero al poder formal al poder de los estados sino al poder concentrado y a la circulación de esta conformación en esos canales del poder concentrado que a veces no conocemos ni su rostro ni sus nombres.

Hay una falta absoluta de proporcionalidad y responsabilidad en la utilización de muchos instrumentos. Pensaba ¿cuál es el valor, en términos axiológicos, que hoy ocupa en nuestra sociedad la privacidad del individuo? ¿Cuál es en realidad ese conjunto de valores en oposición a la exposición? ¿Cuándo exposición en muchas circunstancias y en muchos casos es sinónimo de éxito? ¿Cómo hacemos para contrarrestar una cultura cuyo uno de los aspectos dominantes es la división de la sociedad entre “ganadores” y “Perdedores”? Son abordajes estructurales y profundos que debemos encarar.

Cuenta la experiencia de una encuesta – Relación entre los jóvenes y nuevas tecnologías: Conocimiento tecnológico avanzado: 25 % tenía en cuenta la privacidad, 25 % imagen como parte integral de los datos personales y 2 % conocía la existencia de marco normativo.

Para terminar, en la cultura contemporánea hay fenómenos de transculturación que de manera inconsciente incorporamos a nuestro lenguaje, por ejemplo el concepto de red social, como construcción histórica, una red social era un grupo constituido por sujetos de carne y hueso, de identidad conocida que se unían en torno o en pos de un objetivo común. Las actuales llamadas redes sociales no constituyen una red social y eso sin considerar que muchos de los participantes tienen identidades falsas.

Para concluir considero que inexorablemente en algún momento y a partir de una dificultosa construcción vamos a tener que llegar a una convención internacional donde el tema de manejo de internet y el manejo de redes tengan el mismo sentido, el mismo cuidado, la misma protección y el mismo contenido normativo que lo que son las redes sociales materiales.

Doctora Valeria Milanés - Directora de la Asociación por los Derechos Civiles (ADC), áreas de Libertad de Expresión Acceso a la Información y Privacidad

Informe “Si nos conocemos más, nos cuidamos mejor”

Toma el nombre del slogan que uso la presidenta para presentar SIBIO. Resulta llamativo como, de un tiempo a esta parte, el estado argentino ha empezado a implementar mayores políticas de

recolección, almacenamiento y procesamiento de datos biométricos. Sin embargo los riesgos que la adopción de estas tecnologías, que implican un salto exponencial desde de los viejos sistemas a estos nuevos, no han sido merituados acabadamente. Este tipo de adopción de políticas en nuestro país se hace sustancialmente en base a decretos y a reglamentaciones de reparticiones estatales no pasa por el Parlamento, no se le da ese tipo de discusión.

Explica el informe de ADC



Facultad
de Derecho | UBA

Miércoles 19 de agosto de 2015 a las 18 hs. en el Salón Rojo, Facultad de Derecho (UBA)

Carrera de Especialización en Derecho Informático
Director: Daniel R. Altmark y Eduardo Molina Quiroga | Coordinadora: Paula Rómulo

Tecnología, Vigilancia y Derechos Personalísimos



thilo_m
<https://flic.kr/p/9hr8hH>
<https://creativecommons.org/licenses/by-nc-nd/2.0/>

Expositores:

- Ab. **Valeria Milanes**, directora de la Asociación por los Derechos Civiles (ADC), áreas de Libertad de Expresión, Acceso a la Información y Privacidad.
- Lic. **Eduardo Peduto**, director del Centro de Protección de Datos Personales de la Defensoría del Pueblo de la Ciudad Autónoma de Buenos Aires
- Ab. **Eugenia Carrasco**, investigadora del Instituto Latinoamericano de Seguridad y Democracia (ILSED)
- Lic. **Andrés Pérez Esquivel**, sociólogo, Asesor en Seguridad en la Legislatura CABA, miembro de la Asociación Pensamiento Penal y de Latin American Network of Surveillance Technology and Society Studies (LAVITS)
- Dr. **Eduardo Molina Quiroga**, director del proyecto de investigación UBACyT “*Tensiones que genera la aplicación de TICs y los derechos a la protección de datos personales, intimidad e imagen*”.

Entrada libre y gratuita.



Informes e inscripción:
Departamento de Posgrado
4809-5606/7 | E-Mail: cedi@derecho.uba.ar
Twitter: [@posgradosderuba](https://twitter.com/posgradosderuba)

Departamento de Posgrado

Evento: “Te estamos vigilando”

Organización: ADC- Asociación por los Derechos Civiles

Fecha: 1 de diciembre 2015

Expositores: Valeria Milanés - Integrante de la Asociación por los Derechos Civiles-ADC

Natalia Zuazo – Periodista /Autora: “Guerras de Internet”

Horacio Azzolin – Fiscal a cargo de UFECI

Vladimir Chorny – Abogado / Investigador R3D (México)

Presentación:

Leandro Ucciferri – Miembro de la Asociación por los Derechos Civiles (ADC)

Desde el área de Privacidad de ADC venimos trabajando hace algunos años con temas como: biometría, protección de datos personales, sistema de vigilancia y recientemente big data. Tanto éste área, como las áreas de libertad de expresión y acceso de la información, trabajamos con la misma matriz, con una mirada digital, de nuevas tecnologías.

La propuesta de hoy es charlar sobre vigilancia estatal desde distintos aspectos.

Valeria Milanés – Directora del Área Privacidad de la Asociación por los Derechos Civiles (ADC)

Voy a hablar de los 13 Principios Internacionales sobre la aplicación de los Derechos Humanos a la Vigilancia de las Comunicaciones.

ADC fue parte de la génesis de estos principios, es un proyecto mundial que tardó aproximadamente un año, en donde se relevó la opinión de gente técnica, sociedad civil e industrial. Hoy hay más de 300 organizaciones que adhieren a estos principios.

Los principios devinieron importantes y necesario en su elaboración por la irrupción de la tecnología, abaratamiento en el almacenamiento de la información que se va recolectando, las prácticas estatales de la vigilancia y el cambio de paradigma de los datos, aquellos que sabemos que entregamos, los que generan nuestros dispositivos, los metadatos, datos en tránsito, datos almacenados, distinta tipología de datos que requieren una atención especial. Todo este escenario y las prácticas detectadas post Snowden generaron la iniciativa en elaborar principios que pudieran aplicarse a cada legislación o que cada país pudiera considerar para elaborar su propia legislación, pero están ausente en la mayoría de los países.

Volviendo al tema de los datos, no solamente es contenido en general. El contenido tiene un estándar de protección alto en detrimento de los metadatos que suelen ser datos que se consideran de registro (datos puntuales que hacen a las personas que utilizan las tecnologías), suelen tener un estándar de protección menor pero que es en el análisis de esos datos junto a otros, que dan más información sobre la persona que una base de contenido y tiene un estándar de protección mucho menor (en los principios está detallado la protección de metadatos).

Los principios se pueden leer en: <https://es.necessaryandproportionate.org/text>.

NECESIDAD y PROPORCIONALIDAD son dos de los estándares principales que se piden siempre que haya que regular algo referido a DDHH. Necesario y proporcionado: resumen o ponen en evidencia dos características que son, hasta de sentido común, y tiene que ser la guía en este tipo de cuestiones.

Los principios se tienen que entender en forma holística, tomar uno por separado no se entiende el concepto, se tienen que tomar como un todo. Están focalizados en el accionar del Estado pero también aplican a empresas privadas que tienen que ver con tecnología e interceptación.

Sabemos, más allá del discurso de seguridad, el Estado comparte, elige o usa un discurso legítimo. También hay un negocio muy grande en cuanto a la compra de tecnología, más allá de la participación de empresas como las Telco o empresas de internet y demás, que tienen mucha información, sobretodo de metadatos que utilizan para sus propios fines pero los principios están dirigidos al accionar estatal.

No solo cuando hablamos de tecnología de interceptaciones de comunicaciones, hablamos de privación de la privacidad sino que también sabemos o es conveniente reflexionar que la privacidad y la intimidad nos permiten la elaboración de pensamientos, formación de opinión, vinculada a la expresión de libertad.

Los principios tienen dos o tres definiciones, "Información Protegida" es toda información que incluye, refleja, surge de, o se refiere a las comunicaciones de una persona y que no está fácilmente disponible y accesible para el público en general.

Es una definición muy amplia y bajo esa definición capta casi todo, o todo lo posible, hay que tener presente que son principios generales que después deberán ser trabajados localmente para adecuar a las legislaciones que se sancionen y que van a estar limitados por cuestiones como pautas culturales o las pautas de políticas públicas que el Estado pueda llegar a elaborar.

LEGALIDAD: ninguna medida, ninguna interceptación de nueva tecnología puede ser utilizada si no hay una ley en el sentido formal y material que lo avale. No basta un decreto, tiene que ser una ley sancionada, cumpliendo el procedimiento que cada constitución establece. En nuestro caso tiene que pasar por el Congreso de la Nación y seguir el trámite ante el poder legislativo. Debe tener un lenguaje claro y preciso. La mayoría de las veces se utiliza un lenguaje ambiguo, poco preciso o se utiliza formulas generales, que cuando hay que bajarlas a terreno abarcan un espectro amplio que están desvirtuando el fin protectorio que tienen. En este caso sabemos que es una dificultad y que los términos pueden ser interpretados de distinta manera, por lo tanto es necesario un lenguaje claro, preciso y lo más acotado posible. También es necesario un punto de revisión periódica que no es un tema menor, porque es sabido que las leyes tiene un ciclo de revisión muy largo, si es que lo tienen, y en el caso de las tecnologías la revisión debe ser permanente porque las tecnologías se desarrollan a una velocidad que deja atrás los métodos normales de actualización de datos.

OBJETIVO LEGÍTIMO: no alcanza decir seguridad, tiene que ser establecido por autoridades estatales. Tiene que respetar y corresponder a un interés público, preponderante e importante. Tiene que evitar formas que tengan que ver con discriminación, o que tengan como objetivo religión, raza, intereses o partidos políticos. Todo lo que tenga que ver con interceptación de comunicaciones debe ser con un objetivo claro, tiene que estar establecido con la menor ambigüedad y aplicarse a la población en general, no a un sector específico.

No nos olvidemos que estos principios son globales y hay países muy sensibles en cuanto a estas diferencias.

NECESIDAD - PROPORCIONALIDAD e IDONEIDAD: cuando se pide la interceptación de una comunicación (porque se tiene que pedir ante un juez) debe acreditarse un alto grado de probabilidad de que se esté por cometer un delito grave o se haya cometido un delito grave para un fin legítimo. Tiene que haber un alto grado de probabilidad de las evidencias pertinentes o materia que van a hacer adquiridas de la información protegida de la que se quiere acceder. Además debe probarse y acreditarse que otras formas menos invasivas ya han sido utilizadas o no tendrían sentido. Esto tiene que ver con educación de los pueblos, de los fiscales, de los que tienen a su cargo la petición y el otorgamiento de estas medidas. La ley sola nos puede servir pero también requiere un ejercicio de educación y de entendimiento de las personas que están involucradas en este esquema y en estas medidas.

La información a la que se accederá tiene que ser solamente en cuanto a lo relevante, es decir al objetivo específico, la idea es que sea lo más pormenorizado y acotado posible. La información excedente, lo que no se use, todo el material que no se utiliza no puede quedar por las dudas, tiene que ser destruido o debe ser devuelto. Tener grabaciones que hace 15 años se realizaron es la información altamente vulnerable de la privacidad e intimidad de las personas, en este sentido no tiene ninguna utilidad.

AUTORIDAD JUDICIAL COMPETENTE: tiene que ser autoridad judicial imparcial y competente. Tiene que estar separada y ser independiente de las autoridades encargadas de la vigilancia. En el esquema de un juez que ordene y un órgano gestor (que tenga que llevar adelante la medida) pero no puede ser el mismo órgano el que lleve la medida y decida hacerla. La mayoría de los jueces no comprende o no termina de entender, lo esperable es que los jueces o las autoridades que tienen a su cargo la autorización de este tipo de tecnologías comprendan que se trata, lo esperable es que tengan los recursos adecuados para poder hacerlo.

DEBIDO PROCESO: el proceso tiene que estar establecido por ley, el procedimiento mediante el cual se lleva adelante la interceptación tienen que ser consistente y disponible al público en general es decir, cualquier persona puede y debe conocer de antemano los procedimientos que se llevan a cabo en este sentido. Lo esperable es que haya una audiencia pública y justa dentro de un plazo razonable para el sujeto que está siendo vigilado cuyas comunicaciones están siendo interceptada, excepto que haya un peligro de vida y la autorización del juez puede venir a posteriori y debe ser en tiempos razonables (lo más rápido posible)

NOTIFICACIÓN DEL USUARIO: acá no pasa pero en algunas legislaciones sucede y en los principios se contemplan. Es dar a la persona que fue vigilada poder, con tiempo e información suficiente, para que pueda impugnar la posición adoptada u ofrecer otra solución, darle a esta persona acceso a los materiales que sustentaron la petición. El Estado tiene la obligación de notificar y los proveedores mediante los cuales se suele realizar la interceptación tienen la facultad de notificar. El Estado no tendría que intervenir en esta facultad para notificar. Claramente hay excepciones, el principio es claro: hay que notificar al usuario y la excepción es salvo que se corra riesgo con la finalidad por la cual la interceptación se ordenó. Hay otras cuestiones más pero no las voy a desarrollar.

TRANSPARENCIA: las leyes que establezcan interceptación de comunicaciones, los reglamentos o las actividades que llevan a cabo los organismos encargados tienen que ser públicos, ser accesibles al público, compartidos en un idioma, de tal forma que lo pueda entender la ciudadanía en general.

Publicar la información de las interceptaciones y solicitudes que se realizaron: detalladas o separadas, identificadas por proveedor, por autoridad que ordene la investigación, el tipo de propósito que tiene esto, el número de las personas afectadas. La idea es siempre dar un principio de máxima transparencia.

Insisto, son principios generales que deberán bajarse a terreno en cada país y responder a las características de los sistemas procesales y a las garantías que cada país ya tenga.

SUPERVISIÓN PÚBLICA: tiene que ver con la existencia de mecanismos independientes de supervisión o de control.

INTEGRIDAD DE LAS COMUNICACIONES Y SISTEMAS: que el Estado tenga la facultad de ordenar medidas de interceptación no debe alterar el funcionamiento de los prestadores de

servicios, ni de rastreo, ni de generar tecnología que sirva para la interceptación de las comunicaciones. Si lo hacen por una cuestión empresarial, es otro tema, pero que el Estado obligue a generar a la prestadora tecnología para interceptar no sería parte a lo que los principios alientan.

GARANTÍAS PARA LA COOPERACIÓN INTERNACIONAL: la forma en que las comunicaciones digitales se producen. Cuestiones de jurisdicción es uno de los grandes problemas que tiene que ver con todo el circuito digital. Las legislaciones son jurisdiccionales, el sistema penal es jurisdiccional, los sistemas de seguridad son jurisdiccionales, internet y las comunicaciones digitales no son jurisdiccionales. Ahí hay un salto cuántico que requiere en principio acuerdos de cooperación, ágiles y diálogo permanente.

GARANTÍAS CONTRA EL ACCESO ILEGÍTIMO Y DERECHO A RECURSO EFECTIVO: este principio alienta que haya sanciones civiles y penales para aquellos agentes públicos o privados que realizan interceptaciones ilegítimas a las comunicaciones. Ahora también la protección a los “whistle blowers”, aquellos que han denunciado irregularidades, por ejemplo caso Snowden, lo mismo que el uso de herramientas de anonimato y cifrado. En este sentido, es un tema sensible, sabemos que EEUU y Europa por el atentado, están yendo en contra de herramientas de cifrado. Los principios invitan a reflexionar sobre los aspectos positivos de las herramientas de cifrado y anonimato. Es una manera de expresarse libremente.

Los principios lo que intentan es poner luz sobre estos aspectos que son muy sensibles y que si no se tienen en cuenta pueden generar legislaciones, en el mejor de los casos legislaciones, o como está pasando en nuestro país, prácticas que si no se tienen en cuenta principios de privacidad y otros derechos pueden resultar abusivas y contrarias a lo que se intenta proteger.

Natalia Zuazo – **Presentación del Capítulo** Vigilar y entretener, un modelo de negocio feliz **del libro “Guerras de internet: Un viaje al centro de la red para entender cómo afecta tu vida”**

Explicación de vigilancia estatal a través de las videocámaras

Me interesaba saber que datos tenemos entre seguridad e inseguridad, que dicen las estadísticas, quien las provee para adoptar los sistemas de vigilancia, que tipos de cámaras, que tipos de equipos, que evaluación previa y posterior se realiza para tomar una decisión que viene siendo masiva, siempre: comprar más sistemas de seguridad, En este caso específico en cámaras de vigilancias, pueden ser otros sistemas, pero siempre la respuesta ante el supuesto aumento de inseguridad (pero tampoco hay estadísticas homogéneas) es la misma, incrementar los sistemas de videovigilancias. No tenemos estadísticas previas ni posteriores pero siempre se toma la misma decisión.

- Cámaras para uso político sin importar la privacidad de los ciudadanos(...)

- Hipótesis: como estamos ofreciendo el control de nuestras datos, no solo de las imágenes sino también de otro tipo de datos, algoritmos dominados por un puñado de empresas que cooperan y hacen negocios entre sí con la política y como se ven influenciados nuestros derechos porque siempre la tecnología se supone que viene a solucionar los problemas.

Vladimir Chorny -Seguridad y Privacidad

Mi planteo se basa en pensar: sucede muchas veces la mal planteada dicotomía entre seguridad y privacidad, pareciera que en un polo tenemos la única opción, como pensado en blanco y negro, de tener a ese Estado hiperpoderoso, con todas las facultades de ir a fondo, sin ninguna limitación, como una especie de Leviatán que debe tener todas las facultades de conocernos a todos y observarnos todo el tiempo o, del otro lado, tener un "mundo rosa" en que generalmente

se ridiculiza o se pone en un discurso bobo a las personas que creemos en los DDHH, que pareciéramos que no entendemos que si buscamos el respeto a la privacidad van a llegar los terroristas a bombardearnos y a matarnos a todos.

Hace más de 44 años Daniel Ellsberg filtró los papeles del pentágono en los cuales se mostraba lo que pasaba en Vietnam y muchas de las atrocidades y las políticas que se tomaban en ese momento. Es uno de los buenos antecedentes que muestra lo que puede hacer un gobierno fuerte, sin límites, sin controles y opacos, es algo parecido a lo que pudimos ver con Snowden cuando sucedieron las distintas filtraciones y también nos hicieron reflexionar sobre cuál es el rol de tener a ese Estado todopoderoso, sin controles, ilimitado que muchas veces parecía estar en todas partes y ser al mismo tiempo invisible, lo que es bastante paradójico.

¿Qué tipo de Estado queremos tener? o ¿en qué tipo de Estado queremos vivir y que tipo de sociedades queremos tener?

Si nosotros rendimos el discurso a los DDHH, el discurso a la privacidad que no solo tiene que ver con la privacidad sino también con la articulación de un montón de derechos más: libertad de expresión pero también, en algunos casos, salud y desde luego otras acciones que tienen que ver con el desarrollo de la personalidad de las personas. Si nosotros rendimos eso bajo el discurso de la seguridad que devora todo en un estado policial entonces hay muchas cosas a las que estamos renunciando que no se reducen a la mera idea de la privacidad.

Pero eso es solo una parte, la segunda parte es que si nosotros aceptamos esto, si nosotros aceptamos un estado policial de esta forma o un Leviatán desencadenado, nosotros también estamos aceptando un poder de invisibilidad a esas estructuras, a esas autoridades para que hagan prácticamente lo que sea, porque muchas veces ante amplias facultades de vigilancia (masivas) no existen posibilidades de salvaguardas que te permitan saber cómo se está utilizando esa información, que tantas intervenciones están haciendo, cuantas personas están siendo geolocalizadas, que uso se está dando a la retención de datos. Como uno no tiene acceso a esta información tampoco se puede combatir, uno no sabe que está haciendo el gobierno porque el discurso del gobierno, en parte, es que esa información no puede ser revelada porque eso afectaría su trabajo de persecución al crimen y de combate ante el terrorismo.

Te estamos vigilando

Una conversación sobre las capacidades de
vigilancia del Estado y el derecho a la privacidad
de las personas

Horacio Azzolín Fiscal a cargo de UFECI

Vladimir Chorny Abogado / Investigador R3D
(México)

Natalia Zuazo Periodista / Autora: "Guerras de
Internet"

Valeria Milanes Directora Áreas Libertad de
Expresión, Privacidad y Acceso a la
Información (ADC)

Capacidad limitada
Confirmar asistencia: adc@adc.org.ar



 Hotel NH 9 de Julio
Av. Cerrito 156
Miércoles 2
de diciembre



18:00 a
20:00 hs

Video: “Si nos conocemos mejor, nos cuidamos más”

Fecha: 06 de agosto de 2015

Recuperado de: <https://elnuevodespertar.wordpress.com/2013/10/28/conozca-sibios-la-masiva-y-orwelliana-base-de-datos-biometrica-de-argentina/>

Locutor: Por decisión política de CFK la integración de los Ministerios del Interior y de Seguridad se pone en marcha el nuevo sistema de identificación de los ciudadanos, el Sistema Federal de Identificación Biométrica. La identidad de una persona está formada por un conjunto de rasgos del individuo que los caracteriza frente a los demás entre ellos el rostro y las huellas digitales. La tecnología digital junto al aporte del equipo humano nos permite implementar un sistema de avanzada de nivel internacional que asegura la identidad insustituible de las personas. Ahora vos, sos vos (aparecen personas haciendo el gesto “ok” es decir que muestran el pulgar con sus huellas digitales)

Especialista: Nuestra firma, nuestros ojos, la manera que tenemos al caminar son características que nos diferencian y nos hacen únicos: el rostro, las huellas digitales. Un AFIS es un sistema de identificación de estas características, estamos hablando de tecnología de identificar características físicas y de comportamiento humano. Para poder aplicar esta tecnología es muy importante la etapa de recolección de datos es la base con lo que trabaja este sistema.

Locutor: A través del RENAPER la toma de huellas digitales y la fotografía para el pasaporte y el Nuevo DNI son incorporados una base de datos inteligente, el sistema verifica que esas imágenes no existan asociadas a otro ciudadano

Especialista: En el momento de la identificación el sistema debe responder a dos preguntas:

- Si la persona es quien dice ser.
- ¿Quién es esa persona?

Locutor: El sistema realiza el proceso de identificación en forma totalmente automática y en pocos segundos ejecuta la búsqueda en una base de datos de millones de huellas y rostros previamente registrados asociados a un número de DNI.

Especialista: Más de 10 millones del Nuevo DNI y 1 millón de Pasaportes fueron transferidos a la base de datos de la Fuerza de Seguridad. Estos datos forman un soporte que optimizan los tiempos de control. Este sistema puede ser utilizado para diferentes aplicaciones por ejemplo en un accidente podemos identificar a una persona sin documentación

Locutor: Es una herramienta indispensable en prevención de delitos de suplantación de identidad tanto de tipo económico como de trata de personas

Especialista: Para el fortalecimiento de controles migratorios, para que cada persona que ingresa al país sea la misma que sale y para que esa persona sea quien dice ser

Locutor: Además el sistema multiplica la posibilidad de esclarecimiento y resolución en caso post delito otorgando un soporte científico para los casos criminales. El reconocimiento fisionómico del nuevo del nuevo sistema permite proyectar el rostro de una persona a través del tiempo, aumentando así las posibilidades de encontrarla. De esta manera las fuerzas de seguridad de todo el país quedan integradas en una misma base de datos pudiendo efectuar un mayor control de los ciudadanos con prontuario y protegiendo la identidad del resto de la ciudadanía.

Especialista: si se realiza un chequeo en vivo con el AFIS (Sistema Automatizado de Huellas Digitales) un menor con pedido de paradero podría ser detectado en el acto más allá si presenta un DNI adulterado o falso

Locutor: La alta tecnología del sistema permitirá en el futuro integrar datos de voz, iris ocular e incluso del ADN

Especialista: es importante destacar que este sistema se desarrolló con la colaboración y el intercambio tecnológico con Cuba, con lo cual logramos un sistema de avanzada a muy bajo costo.

Locutor: la implementación del nuevo sistema es parte del programa de modernización de la investigación científica del delito generando una arquitectura integrada de tecnología para las fuerzas policiales y de seguridad nacional y provinciales. Seguimos trabajando para fortalecer nuestra identidad, incorporando tecnología al servicio de una mejor calidad de vida.

Con el Sistema Federal de Identificación Biométrica el Estado incorpora soluciones de identidad para hacer de nuestro un país más seguro. Seguridad de saber quiénes somos y a dónde vamos. Si nos conocemos mejor, nos cuidamos más. *Argentina, un país con buena gente.*

Al Sr. Ministro del Interior
Cdr. Aníbal Florencio Randazzo

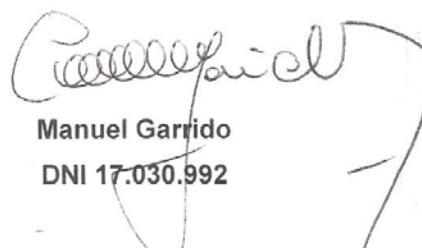
S/D

Manuel Garrido, con domicilio en Riobamba 25 de la Ciudad Autónoma de Buenos Aires, me dirijo a usted para solicitarle, según lo establecido por el Decreto 1172/03, información referida al nuevo documento nacional de identidad con chip.

En particular, le solicito que me informe:

- Qué datos contendrá el nuevo documento nacional de identidad con chip que no contiene ya el actual documento nacional de identidad conforme al decreto 1501/2009;
- Si es obligatorio cambiar de tarjeta y en qué plazo;
- Si no fuera obligatorio, cómo coexistirían ambos sistemas;
- Qué diferencia implica el soporte chip respecto a la tecnología digital actualmente utilizada en el documento nacional de identidad;
- Con qué finalidad se incorporan esos nuevos datos a la tarjeta de identificación;
- Cuáles son los motivos por los cuales se decidió incorporar esos nuevos datos;
- En qué se beneficiarán las personas por la incorporación de nuevos datos personales;
- En qué se beneficiará el Estado con la incorporación de los nuevos datos personales y qué uso pretende darle a dicha información;
- Qué organismo u organismos tendrá/n a su cargo la recolección, conservación, ordenación, almacenamiento, modificación, relacionamiento, evaluación, bloqueo, destrucción y procesamiento de los datos que contendrá el nuevo documento nacional de identidad;
- Qué medidas de seguridad se tomarán para el adecuado almacenamiento de los datos y la protección de los datos personales;
- Qué costo tendrá para el ciudadano la nueva tarjeta;
- En qué consiste el Convenio con la Real Casa de la Moneda de España y en qué colaborará el gobierno español con el Ministerio del Interior. Remita copia del texto del Convenio.

Sin otro particular, lo saluda atentamente,



Manuel Garrido
DNI 17.030.992

mgarrido@diputados.gov.ar Tel. (54.11) 4127-7660/7675



Ministerio del Interior y Transporte

Ref.: Exp-S02:0087461/2014.

Nota N° 2678

BUENOS AIRES, 05 de agosto de 2014.-

Señor

Manuel GARRIDO

Riobamba 25, 7° Piso, Of. 760

(C.P. 1033) Ciudad Autónoma de Buenos Aires.

Me dirijo a Usted en relación a la presentación que diera origen a las actuaciones citadas en la referencia, mediante la cual solicitó información en el marco de lo dispuesto en el Reglamento General del Acceso a la Información Pública para el Poder Ejecutivo Nacional, aprobado por Decreto N° 1172/2003.

Sobre el particular, le adjunto a la presente copia fiel del informe elaborado por la Dirección Nacional del Registro Nacional de las Personas, a fin de dar respuesta a su requisitoria.

Sin otro particular, lo saludo atentamente.-

Dr. Esteban Zannini
Enlace Unidad Ministro

Acceso a la Información Pública - Decreto N° 1172/2003
Ministerio del Interior y Transporte



Ministerio del Interior y Transporte
Registro Nacional de las Personas
Ley N° 17.671



NOTA N° 163 /2014
BUENOS AIRES,

0. 660 2014

Al Dr. Esteban J. Zannini
Enlace Unidad Ministro – Decreto N° 1172/2003
MINISTERIO DEL INTERIOR Y TRANSPORTE
S / D

Me dirijo a Ud. en respuesta a la nota de fecha 28 de julio del corriente, mediante la cual solicita elabore Informe referente a la solicitud formulada por el Diputado Manuel Garrido en el marco del Decreto de Acceso a la Información Pública. A continuación se enumeran las respuestas a cada una de las consultas efectuadas, dejando constancia de que la solicitud manifestada en el punto nro 12 del Informe en cuestión, sobre la remisión de copia de texto del Convenio con la Real Casa de la Moneda de España, deberá ser aportada por esa Unidad Ministro, en vistas de no contar este Organismo con copia del referido convenio Marco, por cuanto se trata de Acuerdo suscripto entre el entonces Ministerio del Interior y la Real Casa de Moneda y Timbre del Gobierno de España.

1. Qué datos contendrá el Nuevo DNI con chip que no contiene ya el actual DNI conforme al decreto 1501/2009

El DNI electrónico contendrá los mismos datos de identificación que el DNI vigente. Se trata de una innovación tecnológica que consiste en dotar de mayores medidas de seguridad al DNI y de la incorporación de un circuito integrado o chip que contendrá los datos de identificación del ciudadano exclusivamente, y otro que podrá contener otros datos y/o información complementaria del titular existente en distintas bases de datos y/o soportes físicos, la que podrá ser de utilidad para el ciudadano en su interacción con el Estado o en el uso de bienes y servicios públicos, como es el caso del transporte y la tarjeta SUBE. Este chip, asimismo, contendrá un certificado de firma digital que permitirá confirmar la identidad digital en internet de un ciudadano. De esta forma, el poseedor del DNI podrá autenticar su identidad en forma automática al momento de realizar ciertos trámites o transacciones en línea. Por cuanto el DNI electrónico se podrá transformar en una llave de acceso del ciudadano usuario a distintos servicios en línea.

2. Si es obligatorio cambiar de tarjeta y en qué plazo



Ministerio del Interior y Transporte
Registro Nacional de las Personas
Ley N° 17.671



No es obligatorio cambiar de tarjeta. Todas las personas que cuenten con el Nuevo DNI, sea este la libreta de tapa celeste, o las diferentes versiones de tarjeta plástica, no tienen ninguna obligación de cambiarlo.

3. Si no fuera obligatorio, cómo coexistirían ambos sistemas

No se trata de dos sistemas diferentes. Se trata de una innovación tecnológica que se incorporará a la producción corriente del DNI. Así como el DNI y el Pasaporte en el resto de los países del mundo se actualizan periódicamente en su formato, diseño e interoperabilidad en función de los avances de la ciencia y la técnica; este cambio no implica modificaciones en la validez ni la convivencia con los DNI en circulación.

4. Qué diferencia implica el soporte chip respecto a la tecnología digital actualmente utilizada en el DNI

El soporte DNI continuará siendo una tarjeta plástica con la diferencia de la incorporación en su interior de dos dispositivos de almacenamiento de datos con propósitos diferentes. La tecnología digital, es decir el software utilizado, se trata del mismo que se utiliza actualmente y fuera desarrollado para la tramitación, verificación digital y emisión del DNI.

5. Con qué finalidad se incorporan estos datos en la tarjeta de identificación

Como se indicó en la primera respuesta, no se pretende incorporar más datos que los actuales previstos en la ley; sino que en el futuro, la tecnología del nuevo DNI electrónico hará que el ciudadano pueda incorporar datos o información que le pudiera resultar de utilidad. El DNI electrónico permitirá que en el futuro un ciudadano cuente en un mismo soporte plástico con datos que pueden darle mayor practicidad a su interacción con servicios públicos.

6. Cuáles son los motivos por los cuales se decidió incorporar esos nuevos datos

Se reitera que no se incorporan nuevos datos. Sino que será el ciudadano el que en un futuro podrá incorporar en su DNI datos que estén disponibles en diversas bases y/o



Ministerio del Interior y Transporte
Registro Nacional de las Personas
Ley N° 17.671



registros para facilitar el acceso de las personas a servicios esenciales. Esto es, simplificar trámites y ahorrar tiempo para los ciudadanos.

7. En qué se beneficiarán las personas por la incorporación de nuevos datos personales

Las personas que en un futuro cuenten con el DNI en su versión electrónica contarán principalmente con la facilidad de portar un único soporte plástico con información a la que podrán acceder servicios públicos autorizados únicamente, sin la necesidad de hacer otras gestiones para obtenerla. Además, el DNI electrónico será un DNI más eficiente en términos de seguridad por cuanto la incorporación de un chip consiste en un nuevo elemento de seguridad que reduce las posibilidades de falsificación o adulteración de documentos.

8. En qué se beneficiará el Estado con la incorporación de los nuevos datos personales y qué uso pretende darle a dicha información

El Estado se beneficiará en cuanto al uso más eficiente y el acceso seguro a información y datos que hoy se encuentran dispersos. Al mismo tiempo, se ahorran los recursos públicos que conlleva la unificación en un único soporte de credenciales y/o comprobantes emitidos a nombre los ciudadanos en su roles de usuarios de distintos servicios.

9. Qué organismo u organismos tendrán a su cargo la recolección, conservación, ordenación, almacenamiento, modificación, relacionamiento, evaluación, bloqueo, destrucción y procesamiento de los datos que contendrá el nuevo DNI

El Ministerio del Interior y Transporte, a través del Registro Nacional de las Personas, organismo autárquico dentro de su órbita, tendrá a cargo la recolección, conservación, ordenación, almacenamiento, relacionamiento, evaluación, bloqueo, destrucción y procesamiento de los datos que contendrá el Nuevo DNI. Cabe aclarar que la modificación de datos que no sean de identificación, será responsabilidad del organismo o la entidad responsable de su generación.



Ministerio del Interior y Transporte
Registro Nacional de las Personas
Ley N° 17.671



10. Qué medidas de seguridad se tomarán para el adecuado almacenamiento de los datos y la protección de los datos personales

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 en el accionar del Registro Nacional de las Personas.

11. Qué costo tendrá para el ciudadano la nueva tarjeta

El costo vigente del DNI es de \$35 y no está prevista una modificación de la tasa en la actualidad.

12. En qué consiste el Convenio con la Real Casa de la Moneda de España y en qué colaborara el gobierno español con el Ministerio del Interior. Remita copia del texto del Convenio

El Convenio de Colaboración y Asistencia Técnica suscripto con la Casa de Moneda y Timbre del Gobierno de España data del año 2009. Durante el transcurso de los últimos 5 años se ha trabajado en forma continua en coordinación con el organismo español, de probada experiencia en la emisión de DNI electrónicos y Pasaportes para España y otros países de Europa y América Latina. El asesoramiento y la asistencia de los técnicos y profesionales de la Casa de la Moneda de España han acompañado los distintos procesos que atravesó la modernización del sistema documentario argentino, así como también la implementación y mejora del pasaporte electrónico argentino, vigente desde el año 2012.

Sin otro particular, saludo a Ud. muy atentamente.


Lic. Mora Arqueta
Directora Nacional
Registro Nacional de las Personas



Ministerio del Interior y Transporte

Ref.: Exp-S02:0103428/2014.

Nota N° 3120

BUENOS AIRES, 16 de septiembre de 2014

Señores
ASOCIACIÓN PENSAMIENTO PENAL
Bartolomé Mitre 4483 - 3° "C"
(C.P. 1201) Ciudad Autónoma de Buenos Aires.

Me dirijo a Ustedes en relación a la solicitud que diera origen a las actuaciones citadas en la referencia, mediante la cual se requirió información en el marco de lo dispuesto en el Reglamento General del Acceso a la Información Pública para el Poder Ejecutivo Nacional, aprobado por Decreto N° 1172/2003.

Sobre el particular, adjunto a la presente copia fiel de la Nota N° 198 de fecha 16 de septiembre de 2014, de la Dirección Nacional del Registro Nacional de las Personas, en respuesta a su consulta.

Sin otro particular, los saludo
atentamente.

Dr. Esteban Zannini
Responsable del Acceso a la Información Pública
Ministerio del Interior y Transporte



Ministerio del Interior y Transporte
Registro Nacional de las Personas
Ley N° 17.671



NOTA N° 198 /2014

BUENOS AIRES, 16 SEP 2014

AL DR. ESTEBAN J. ZANNINI
ENLACE ACCESO A LA INFORMACIÓN PÚBLICA
DECRETO N° 1172/2003
MINISTERIO DEL INTERIOR Y TRANSPORTE
3 / 0

Me dirijo a Ud. en respuesta a la nota de fecha 26 de agosto del corriente, mediante la cual solicita informe sobre las siguientes cuestiones, referidas a la incorporación de tecnología electrónica en los Documentos Nacionales de Identidad:

1. Si el PEN tiene intenciones de enviar un Proyecto de Ley al Congreso para aprobar el SUBE para transporte y microconsumo comercial creado por el Decreto 84/2009 y su complementario Decreto N° 1580/2013, y el futuro DNI electrónico anunciado oficialmente. Así como las razones de la decisión.

No está previsto que integren la agenda de proyectos impulsados por el Poder Ejecutivo Nacional durante el transcurso del presente año legislativo.

2. Detalle los motivos por los cuales resulta imprescindible modificar nuevamente los DNI, remitiendo los estudios que demuestren que los actuales DNI no tienen suficientes medidas de seguridad

Como todo proceso de cambio y mejora continua en la provisión de un servicio público como es la identificación de personas y la emisión de documentación personal, éste forma parte de una lógica incremental de mejora. La modificación del DNI consiste en una innovación tecnológica que, como los DNI y Pasaportes en el resto de los países del mundo, se actualizan periódicamente en su formato, diseño e interoperabilidad en función de los avances de la ciencia y la técnica.

El cambio previsto no guarda relación con posibles deficiencias en las medidas de seguridad que contiene el actual DNI. Consiste en una actualización tecnológica que sigue las tendencias de la mayoría de los países que cuentan con un sistema de identificación nacional y de documentación de sus ciudadanos.

3. Explique por qué se eligió hacerlo a través de la Casa de la Moneda de España y por qué no hubo licitación

El proyecto de DNI electrónico no se hará a través de la Casa de la Moneda de España, sino que dicha institución brindará colaboración técnica y asesoramiento en la implementación del DNI electrónico, que estará a cargo del Registro Nacional de las Personas en forma directa e intransferible.

El Convenio de Colaboración y Asistencia Técnica suscripto entre el entonces Ministerio del Interior y la Fábrica de Moneda y Timbre del Gobierno de España data del año 2009. Durante el transcurso de los últimos 5 años se ha trabajado en forma continua en coordinación con el organismo español, de probada experiencia en la emisión de DNI electrónicos y Pasaportes para España y otros países de Europa y América Latina. El asesoramiento y la asistencia de los técnicos y profesionales de la Casa de la Moneda de España han acompañado los distintos procesos que atravesó la modernización del sistema documentario argentino, así como también la implementación y mejora del pasaporte electrónico argentino, vigente desde el año 2012.

4. Especifique los alcances de la medida con relación a los datos que incorporará el nuevo DNI electrónico, y sus potencialidades de uso por parte de los ciudadanos y por parte del Estado

El DNI electrónico se trata de una innovación tecnológica que consiste en dotar de nueva seguridad al DNI, al tiempo que incorpora un circuito integrado o chip que contendrá los datos de identificación del ciudadano, y otro que podrá contener otros datos y/o información complementaria del titular, la que podrá ser de utilidad para el ciudadano en su interacción con el Estado o en el uso de bienes y servicios públicos, como es el caso del transporte y la tarjeta SUBE. El primer chip, asimismo, contendrá un certificado de firma digital que permitirá confirmar la identidad digital en Internet de un ciudadano. De esta forma, el poseedor del DNI podrá autenticar su identidad en forma automática al momento de realizar ciertos trámites o transacciones en línea. Por cuanto el DNI electrónico se podrá transformar en una llave de acceso del ciudadano usuario a distintos servicios en línea.

En un futuro también se podrán incorporar en el DNI datos que estén disponibles en diversas bases y/o registros para facilitar el acceso de las personas a servicios esenciales. Esto es, simplificar trámites y ahorrar tiempo para los ciudadanos. La determinación de los datos que podrá incorporar el DNI electrónico está sujeta a la definición por parte del Poder Ejecutivo.

El Estado se beneficiará en cuanto al uso más eficiente y el acceso seguro a información y datos que hoy se encuentran dispersos. Al mismo tiempo, se ahorran los recursos públicos que conlleva la unificación en un único soporte de credenciales y/o comprobantes emitidos a nombre los ciudadanos en su roles de usuarios de distintos servicios.

5. Informe si el nuevo DNI electrónico tendrá carácter optativo permanente o es intención del Gobierno Nacional convertirlo en el definitivo gradualmente



No se trata de dos sistemas documentarios diferentes con segmentación de público. El Nuevo DNI electrónico será una innovación tecnológica que se incorporará a la producción corriente del DNI. A partir de su fecha de inicio de emisión, el soporte DNI continuará siendo una tarjeta plástica con la diferencia de la incorporación en su interior de dos dispositivos de almacenamiento de datos con propósitos diferentes.

Cabe aclarar igualmente que todas las personas que cuenten con el Nuevo DNI, sea esto la libreta de tapa celeste, o las diferentes versiones de tarjeta plástica, no tendrán ninguna obligación de cambiarlo.

6. Indique si se han evaluado otras alternativas para facilitar a la ciudadanía el servicio de firma electrónica, que no incluyan datos biométricos, los cuales no están estipulados en la Ley Nacional 25.506 de firma digital

El chip criptográfico a incluir en el DNI electrónico, que podrá ser utilizado por el ciudadano a efectos de emplearlo para firma digital (distinta de la firma electrónica) utilizará a tales efectos un certificado que no incluye dato biométrico alguno.

7. Informe si los Nuevos DNI tendrán chips de radio frecuencia (RFID) y detalle las características técnicas que garantizan la seguridad de los datos y los mecanismos de control y seguimiento que disponen los ciudadanos y los organismos de control estatales.

Como se describió anteriormente, el DNI electrónico tendrá dos chips, uno de los cuales está previsto que sea un chip RFID. Este chip tendrá la única función de interactuar con el Sistema Único de Boleto Electrónico (SUBE), y tendrá exactamente los mismos datos y recibirá idéntico tratamiento que los más de 12 millones de tarjetas actualmente en uso.

8. Especifique si toda la información contenida en los DNI electrónicos será reunida en una misma base de datos y, de ser así, cuál será la autoridad de aplicación y resguardo de la información, y cuáles los mecanismos de control y seguimiento institucional y ciudadano

El Ministerio del Interior y Transporte, a través del Registro Nacional de las Personas, organismo autárquico dentro de su órbita, tendrá a cargo la administración de los datos de identificación que contenga el Nuevo DNI, de idéntica forma que en la actualidad, y de eventuales datos cuya administración sea propiedad del Ministerio del Interior y Transporte, como los del sistema SUBE, por ejemplo. Cabe aclarar que la administración de datos que no sean generados por el Ministerio del Interior y Transporte, será responsabilidad de la autoridad de aplicación de dichos datos y/o información, o del organismo o la entidad responsable de su generación.

En lo referente al resguardo de la información, 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.

9. Detalle qué información de los nuevos DNI electrónicos formará parte de la Base Nacional de Datos Biométricos (SIBIOS)

Exactamente la misma información que hasta hoy. El DNI electrónico no representa 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.

10. Informe si habrá empresas privadas intermediarias en el proceso de implementación y gestión del nuevo DNI, y de ser así, cuáles son

Así como se ha definido desde el inicio de la presente gestión, desarrollar y administrar en forma directa y 100% estatal el sistema de Nuevo DNI implementado desde el año 2009; el Nuevo DNI electrónico será implementado y gestionado 100% por el Ministerio del Interior y Transporte, a través del Registro Nacional de las Personas.

11. Remítanos copia del acta firmada con la Casa de la Moneda de España

Se adjunta copia del Acuerdo de Cooperación celebrado entre el entonces Ministerio del Interior de la República Argentina y la Casa de Moneda y Timbre del Gobierno de España en el año 2009.

Sin otro particular, lo saludo atentamente.


E. de la Riva
Director Nacional
Registro Nacional de las Personas
