SABER, arte y técnica

Minerva. Saber, Arte y Técnica
AÑO IV / VOL. 1 JUNIO DE 2020
ISSN en línea 2545-6245
ISSN impreso 2591-3840

Tensiones entre SEGURIDAD Y PRIVACIDAD en torno al Sistema Federal de Identificación Biométrica (SIBIOS)*

DIEGO EMILIO FRESCURA TOLOZA
Facultad de Ciencias Sociales,
Universidad de Buenos Aires,
Argentina
diego_frescura@yahoo.com.ar

RECIBIDO: 4 de febrero de 2020
ACEPTADO: 10 de junio de 2020

Resumen Este artículo es de carácter exploratorio y se inscribe en un proyecto de investigación para la realización de la tesina de grado en Ciencias de la Comunicación (UBA). El propósito es describir y analizar la creación y puesta en marcha del Sistema Federal de Identificación Biométrica para la Seguridad (SIBIOS), creado mediante el Decreto 1766/11 del Poder Ejecutivo Nacional. Asimismo, busca estudiar cómo fue el debate público en torno a su creación e implementación, con especial atención a las tensiones y riesgos para el ejercicio de los derechos y libertades ciudadanos que puedan plantearse. Para ello, primero se hará un recorrido sobre el desarrollo en materia de identificación biométrica que ha tenido la Argentina desde sus orígenes hasta la actualidad. Además, se relevarán y estudiarán contenidos de la página web www.biometria.gov.ar y los Congresos CIBRA (Congresos Internacionales de Biometría de la República Argentina) desarrollados anualmente desde 2006 hasta 2013. Por último, se analizarán publicaciones e informes de distintas organizaciones sociales (de Derechos Humanos y defensa de los derechos ciudadanos) que se manifestaron en contra de SIBIOS, entre sus críticas se destacan que no se sometió a debate parlamentario ni su creación ni las condiciones bajo las cuales las fuerzas de seguridad acceden a SIBIOS.

Palabras Clave biometría; control; seguridad; privacidad

Abstract

This article has an exploratory character and is part of a research project for the bachelor's degree thesis in Social Communication Sciences (UBA). The purpose of it is to describe and analyze the creation and start-up of the Federal Biometrics Identification System for Security (SIBIOS), which was created in 2011 by the National Executive Power Decree no. 1766/11. Also, seeks to study how was the public debate surrounding its creation and implementation, with special attention to the tensions and risks to the exercise of the rights and citizen freedoms that can be considered. For that purpose, firstly we will explore the development that Argentina has had in the field of biometric identification since its origins until the present time. Besides, we will relieve and study contents of the web page www.biometria.gov.ar and the CIBRA congresses (International Biometric Congresses of the Argentine Republic) that took place annually from 2006 to 2013. Finally, we will analyze publications and reports of different social organizations (of Human Rights and defence of the citizen's rights) that were against SIBIOS, among the criticisms, they stand out that neither its creation nor the conditions under which the security forces have access to SIBIOS was submitted to parliamentary debate.

Keywords

biometrics; control; security; privacy

SIBIOS y el reconocimiento biométrico automatizado

El Sistema Federal de Identificación Biométrica para la Seguridad (SIBIOS) es una plataforma de datos biométricos de todos los ciudadanos argentinos creada en noviembre de 2011 por medio del Decreto del Poder Ejecutivo Nacional N° 1766/11. Este sistema permite el reconocimiento automático de cualquier ciudadano en base a rasgos físicos únicos, como la huella digital y el rostro. Son sus usuarios el Registro Nacional de las Personas (Renaper), la Dirección Nacional de Migraciones, las Fuerzas de Seguridad del Estado Nacional –Policía Federal (PFA), Policía de Seguridad Aeroportuaria (PSA), Gendarmería Nacional (GNA) y Prefectura Naval (PNA)–, todas las policías provinciales y de la Ciudad Autónoma de Buenos Aires (MSNA, 2017) así como todos los organismos que dependen del Poder Ejecutivo o del Poder Judicial tanto nacional como provinciales y de la Ciudad Autónoma de Buenos Aires que quieran adherirse (Decreto 243/17) .

Para comprender de qué se trata SIBIOS, primero es necesario entender qué es la biometría. El diccionario de la Real Academia Española la define como el "estudio mensurativo o estadístico de los fenómenos o procesos biológicos" (RAE, s.f.). El término "biometría" proviene del griego *bios* ("vida") y *metron* ("medida"). En este sentido, al medir características fisiológicas o de comportamiento pertenecientes a un ser humano, la biometría permite identificar o autentificar su identidad. Actualmente, el desarrollo tecnológico ha permitido perfeccionar y automatizar los procesos de reconocimiento biométrico con métodos automatizados matemáticos y estadísticos. Dichos métodos se utilizan principalmente en el campo de los controles de vigilancia, la identificación criminal, el acceso a sistemas informáticos, dispositivos electrónicos e instalaciones tanto en el ámbito estatal como en el sector privado, con fines tan diferentes como el control de presencia de empleados, transacciones comerciales, etc. (Niklas y Barrera, 2017; Pérez San-José *et al.*, 2011; Thill, 2010).

De este modo, de acuerdo con expertos en materia biométrica, como Thill (2010), la precisión es una de sus ventajas, dado que para identificar o autentificar identidades de individuos utiliza características inherentes a estos, y no algo que deban portar (como una tarjeta inteligente[1] o un token[2]) o saber (como una contraseña, un pin o una respuesta a una pregunta de seguridad). El individuo lleva el dato consigo mismo, y resulta casi imposible que otra persona pueda falsearlo

1 Una tarjeta inteligente o smartcard es una tarjeta generalmente de plástico y de tamaño bolsillo, otorgada a un usuario autorizado para ingresar a un sistema o instalación, con un circuito electrónico integrado que contiene información personal y puede ser leído por un lector electrónico de tarjetas.

2 Un token es un pequeño dispositivo electrónico con información encriptada que se le otorga a un usuario autorizado para autentificar su identidad y poder ingresar a un sistema informático.

Minerva AÑO IV VOL 1 JUNIO 2020, pp 82-107

para suplantar su identidad. A su vez, la utilización de la biometría mejoraría la eficiencia y reduciría costos frente a otras técnicas, ya que no se tiene que invertir en dispositivos adicionales, que además pueden ser perdidos u olvidados por sus legítimos portadores.

En el caso de los factores basados en conocimiento y en posesión, el sistema no puede distinguir si el que utiliza el dispositivo o clave es su legítimo poseedor o no. De todos modos, la biometría muchas veces se utiliza en conjunto con este tipo de tecnologías no biométricas para reforzar la identificación y reducir la posibilidad de fraude. En esos casos se trata de sistemas de autenticación de doble factor. Asimismo, cuando se utilizan dos o más técnicas distintas para la captura y autenticación de los rasgos biométricos, se trata de un sistema biométrico multimodal, el cual también posee el objetivo de hacer aún más precisas y seguras las identificaciones (Pérez San-José *et al.*, 2011; Thill, 2010).

Las características humanas utilizadas para identificar o autentificar a los individuos pueden ser rasgos físicos (estáticos) o de comportamiento (dinámicos). Por un lado, los rasgos estáticos son relativamente estables en el tiempo, y entre ellos se encuentran, por ejemplo, las huellas digitales, los patrones faciales, los patrones de las venas de la mano, la geometría de la mano, el olor corporal, el iris y la retina de los ojos, la estructura de la oreja, etc. Por otro lado, los rasgos dinámicos suelen ser menos estables, y entre ellos se encuentran la firma, la voz, la escritura, el modo de caminar, la dinámica del tecleo, etc. Dependiendo de los rasgos a ser utilizados para la identificación o autentificación, los métodos pueden ser más o menos invasivos, y requerir o no de la cooperación de los individuos. A su vez, cada una de dichas características físicas o de comportamiento utilizadas se diferencian entre sí por distintos aspectos, como la fiabilidad, la facilidad de uso, la prevención de ataques, la aceptación y la estabilidad que presentan (Niklas y Barrera, 2017; Pérez San-José *et al.*, 2011; Thill, 2010).

Los comienzos de la biometría como ciencia

La biometría comenzó a tomar el carácter de ciencia recién hacia fines del siglo XIX cuando Alphonse Bertillon –un criminólogo francés que trabajaba para la Prefectura de Policía de París– creó el sistema de identificación antropométrico. Este fue uno de los métodos utilizados para identificar a delincuentes y "desviados", mediante la medición de distintas características anatómicas y registro de señales y marcas corporales de los individuos (Montiel Álvarez, 2016; Sirimarco, 2007).

Dicho método se basaba en los estudios de estadística de Lambert Adolphe Quetelet, quien había sido el primero en aplicarlos a las ciencias sociales, y en el método antropométrico habitualmente utilizado en la antropología para el estudio de las diferencias de lo que en ese momento se consideraban las "razas" humanas, de acuerdo al paradigma evolucionista de la época. Bertillon aplicó un nuevo uso a estas herramientas, ya que las utilizó para la identificación individual y no grupal. Su sistema atendía el problema práctico que se planteaba desde su puesto dentro de la Policía, es decir, la necesidad de establecer certeramente la identidad individual de los delincuentes para determinar la reincidencia (García Ferrari, 2007). Al mismo tiempo, estando al frente del taller fotográfico de la Prefectura de Policía de París, Bertillon codificó cómo debían realizarse las fotografías a detenidos a la hora de identificarlos y ficharlos (Montiel Álvarez, 2016). Posteriormente, la efectividad de la antropometría quedó desacreditada por las dificultades para diferenciar sujetos que presentaban prácticamente el mismo conjunto de medidas, como en el caso de los gemelos. Sería superado en efectividad por la dactiloscopia, técnica de identificación mediante las huellas dactilares que tiene vigencia hasta la actualidad (Pérez San-José *et al.*,

2011). Sin embargo, la técnica fotográfica que estableció Bertillon para identificar y fichar a detenidos, con fotografías de frente y de perfil, continúa siendo utilizada hasta el día de hoy (Montiel Álvarez, 2016).

Sir Francis Galton, un erudito inglés de la época victoriana, es reconocido en general a nivel europeo por ser el inventor del sistema de identificación dactiloscópica. Galton, quien se había interesado en la antropometría, montó un laboratorio para medir estadísticas humanas en la Exposición Internacional de Salud de 1884. Entre los datos recogidos había huellas dactilares, Galton consideraba que estas permanecían constantes a lo largo de la vida del individuo y podían ser utilizadas como identificadores únicos, agrupando los diseños en arcos, rizos y espirales (Sirimarco, 2007).

LA IMPLEMENTACIÓN DE LA IDENTIFICACIÓN BIOMÉTRICA EN ARGENTINA

De acuerdo con Romero (2004), en la segunda mitad del siglo XIX se llevó adelante un proceso de transformación socioeconómica y estabilización política en la Argentina. Las élites dirigentes llevaron a cabo un proceso de modernización del país con una apertura económica librecambista que afianzó un modelo agroexportador con una fuerte concentración de la tierra. El país necesitaba poblarse y aumentar su mano de obra, por lo que se fomentó la inmigración europea pero sin garantizarles la posesión de la tierra, que había sido repartida sistemáticamente entre grandes propietarios. De este modo, de 3.995.000 de habitantes que registraba el país en el censo de 1895, se pasó a 7.885.000 en 1914. La mayoría de esos migrantes eran personas empobrecidas de países del sur de Europa que, al no haber una política colonizadora, en su mayoría se asentó en la región litoral del país.

En un principio, la élite criolla embarcada en un proyecto modernizador valoraba negativamente a los pobladores nativos en comparación con la inmigración europea, considerada mejor adaptada para el mercado de trabajo que requería el modelo económico agroexportador de aquel entonces. Sin embargo, la masiva inmigración europea fomentada por la clase dirigente trajo consigo el surgimiento de organizaciones obreras anarquistas y socialistas. Dicha inmigración pasaría a ser el blanco del control y la Policía, como agente de control social, se encargó de la represión de actitudes contestatarias a nivel político, a la vez que realizó una vigilancia rigurosa para formar un registro de dichos militantes (Ruibal, 1993).

Siguiendo a García Ferrari (2010), Buenos Aires fue la más afectada por estos cambios, ya que entre 1880 y 1914 recibió la mayor cantidad de inmigrantes con relación a su población local a nivel mundial. Asimismo, fue la principal beneficiaria del nuevo desarrollo económico (Romero, 2004). Sin embargo, dicho proceso de acelerado crecimiento demográfico y también económico de Buenos Aires, estuvo caracterizado al mismo tiempo por una importante desigualdad social (Ruibal, 1993).

El crecimiento exponencial de la población debido a las olas inmigratorias generó que, a partir de la década de 1880, la población fuera mayormente anónima para las autoridades en Buenos Aires. A ello se sumaba el aumento de la criminalidad y la necesidad de control de la protesta social, lo cual tornó imperioso el desarrollo de técnicas que permitiesen a la Policía identificar de manera certera a los detenidos para poder detectar la reincidencia de los delincuentes. En tal sentido, en la Ciudad de Buenos Aires comenzó a funcionar en 1889 la primera Oficina de Identificación Antropométrica de América Latina bajo la órbita de la Policía de la Capital, institución policial creada a partir de la federalización de la Ciudad de Buenos Aires en 1880 (García Ferrari, 2010).

Minerva AÑO IV VOL 1 JUNIO 2020, pp 82-107

Por otra parte, de manera contemporánea a los desarrollos llevados adelante por Galton, la dactiloscopia fue introducida en la Policía argentina durante la década de 1890. Juan Vucetich, un inmigrante del Imperio Austrohúngaro (de la zona que posteriormente sería Croacia) creó la Oficina de Identificación Antropométrica y luego el Centro de Dactiloscopia de la Policía de la Provincia de Buenos Aires, del que fue director. En 1891 realizó las primeras fichas dactilares a nivel mundial con las huellas digitales de 23 procesados. Su sistema dactiloscópico (llamado inicialmente "Icnofalangometría" o "Método Galtoneano") sería posteriormente adoptado por la Policía de la Capital en 1905 (Sirimarco, 2007).

De todas maneras, este proceso de avance estatal en materia de identificación de ciudadanos argentinos por parte del Estado hacia fines del siglo XIX no estuvo exento de resistencias. La principal fue la conocida como "huelga de los cocheros" (Figura 1), que tuvo lugar en 1899 ante el intento de la entonces Municipalidad de la Ciudad de Buenos Aires de imponer a la población de cocheros de plaza el uso obligatorio de una libreta que incluía un retrato fotográfico. Para ello, los cocheros debían presentar dos retratos, uno que debía ir adjunto en la libreta y otro que sería archivado en la Intendencia. Si bien se les solicitaba un retrato de estudio fotográfico que permitiera el reconocimiento y no tuviera una uniformidad predefinida, la medida era considerada por el gremio de cocheros como inconstitucional y como una ofensa al honor, ya que el retrato fotográfico estaba ligado al mundo de la delincuencia (García Ferrari, 2010).

El conflicto tuvo lugar entre abril y junio de 1899 e incluyó, además del llamado a huelga, un mitin convocado por la recientemente creada Sociedad de Cocheros y peticiones a la municipalidad y al Concejo Deliberante que obtuvieron respuestas negativas. Finalmente, el 10 de junio, cuando vencía la posibilidad de presentar los retratos para rematricularse, los cocheros entregaron los retratos (García Ferrari, 2007).

Figura 1. Huelga de los cocheros de 1899 en Buenos Aires. Fuente: Archivo General de la Nación (Inventario 21862).

La automatización del reconocimiento biométrico

Hacia principios de los años sesenta del siglo XX, con la colaboración de empresas privadas tecnológicas, diversos organismos estatales de algunos países iniciaron proyectos de desarrollo de sistemas automatizados de identificación de huellas dactilares. Entre estos organismos estatales se encontraban el FBI de Estados Unidos, la Policía de París de Francia, el Ministerio del Interior del Reino Unido y la Policía Nacional de Japón (Moses *et al.*, 2011).

Por aquella época, distintos factores como el aumento de las agitaciones sociales y de los índices de criminalidad en diversos países hicieron crecer de manera constante los archivos de huellas dactilares que acumulaban distintos organismos estatales. Estos registros eran en tinta sobre papel y requerían cada vez un mayor empleo de trabajo manual por parte de técnicos, que debían examinar cada ficha individualmente para la búsqueda y correspondencia de huellas dactilares. Todo ello tornaba imperioso el desarrollo de un sistema automatizado que otorgara una lista de posibles coincidencias a ser cotejadas, lo cual finalmente sería posible gracias a que en aquellos años la informática comenzaba un rápido proceso de desarrollo con la aparición del circuito integrado o chip de silicio. Este dispositivo permitiría el almacenamiento, procesamiento y transmisión de datos e información en formato digital de manera automatizada (Moses *et al.*, 2011).

Es así como surge el Sistema Automático de Identificación Dactilar, más conocido por la sigla AFIS *(Automated Fingerprint Identification System),* que implicó un salto hacia la automatización de los sistemas de identificación biométrica. Dicho sistema permitió la identificación y autenticación de las huellas dactilares de manera automatizada al extraer los patrones característicos que las conforman. En décadas posteriores, surgirían otros sistemas de registro e identificación automatizados, como el de rostro e iris ocular, que son utilizados con frecuencia hoy en día tanto en el ámbito estatal como en el privado. Por este motivo, a estos sistemas de reconocimiento automático de rasgos biométricos se los suele denominar también de manera genérica como Sistemas Automáticos de Identificación Biométrica o ABIS *(Automated Biometric Identification Systems).*

FUNCIONAMIENTO DE LOS SISTEMAS DE RECONOCIMIENTO AUTOMATIZADOS

Para la identificación biométrica automatizada, inicialmente se debe registrar en el sistema la identidad de los individuos por medio de la obtención de los parámetros biométricos. Para ello, primero, un sensor electrónico captura las características biométricas de algún rasgo físico del individuo. Como mencionamos anteriormente, SIBIOS utiliza dos rasgos biométricos para su sistema de identificación automatizado: dactilar y facial. En el caso del reconocimiento dactilar, para la captura de la imagen de la huella se utiliza un lector de huellas digitales, que generalmente es un sensor óptico. En el caso del reconocimiento facial, para la captura de la imagen facial se utiliza una cámara fotográfica digital (Pérez San-José *et al.*, 2011).

Luego viene el proceso de procesamiento e inscripción, es decir, de las muestras se generan plantillas biométricas a través de algoritmos de reconocimiento. Estas plantillas se guardan en una base de datos y quedan allí registradas para su comparación. En el caso de la huella dactilar, las características extraídas son la ubicación, dirección y formas que poseen las crestas papilares, es decir, los relieves lineales sobre la epidermis de la yema del dedo. Las crestas se alternan con los valles interpapilares, que son las hendiduras situadas entre las crestas (Figura 2) (Rosales Cruz, 2009). En el caso del reconocimiento facial, se extraen como características la forma y posición relativa de los componentes de la cara, como la nariz, la mandíbula, los ojos, etc. Esa información puede ser guardada en una base de datos centralizada o en un dispositivo móvil, como una tarjeta inteligente. En este último caso, el usuario del sistema preserva el control de sus propios

datos biométricos en el dispositivo, ya que no requiere de una base de datos centralizada para almacenar la información (Pérez San-José *et al.*, 2011).

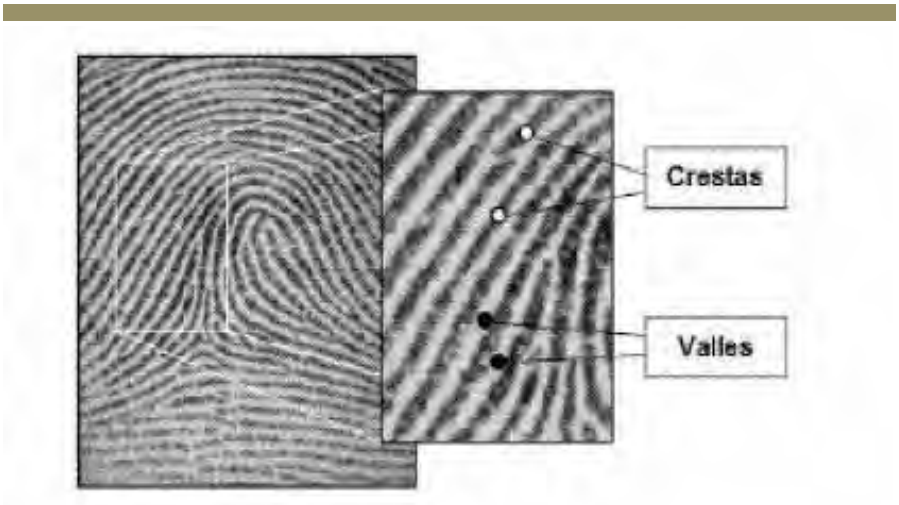

Figura 2. Crestas y valles de las huellas dactilares. Fuente: Sarzuri Flores (2014).

Para autenticar la identidad de un individuo, se realiza la captura de una muestra biométrica y se la compara con las plantillas ya registradas en la base de datos. Se buscan coincidencias a través de unos algoritmos numéricos que asignan una puntuación, la cual representa el grado de correlación que hay entre la muestra a autenticar y la registrada en la base de datos.

Dicho proceso de autenticación puede realizarse a través de la identificación o la verificación. La identificación consiste en la comparación de la muestra que se recoge a un individuo no identificado frente a una base de datos con muestras biométricas registradas previamente para que encuentre o no coincidencias con ellas. En la verificación, por el contrario, el individuo es identificado primero mediante otro medio, como alguna documentación, una tarjeta de acceso a una instalación o un nombre de usuario. De este modo, cuando se realiza la verificación de identidad, se compara la muestra a verificar con la que previamente se había registrado para dicho individuo en particular para obtener un resultado positivo o negativo (Barcelona, 2010; Pérez San-José *et al.*, 2011; Thill, 2010).

Para determinar el grado de correlación necesario entre una muestra y otra, el administrador del sistema biométrico tiene que haber predefinido un umbral. Si la puntuación que resulta de la comparación de muestras supera dicho umbral, el sistema biométrico puede determinar que son coincidentes aunque no sean necesariamente idénticas, ya que se contempla que puede haber ciertas deficiencias en la captura de las muestras. Existe la posibilidad de que el resultado sea inconcluyente, es decir que el sistema biométrico no pueda determinar si la muestra recogida es coincidente o no. En dicho caso, podría ser necesario tomar otra muestra de mejor calidad para determinar la coincidencia o no con las muestras de la base de datos (Figura 3) (Pérez San-José *et al.*, 2011).

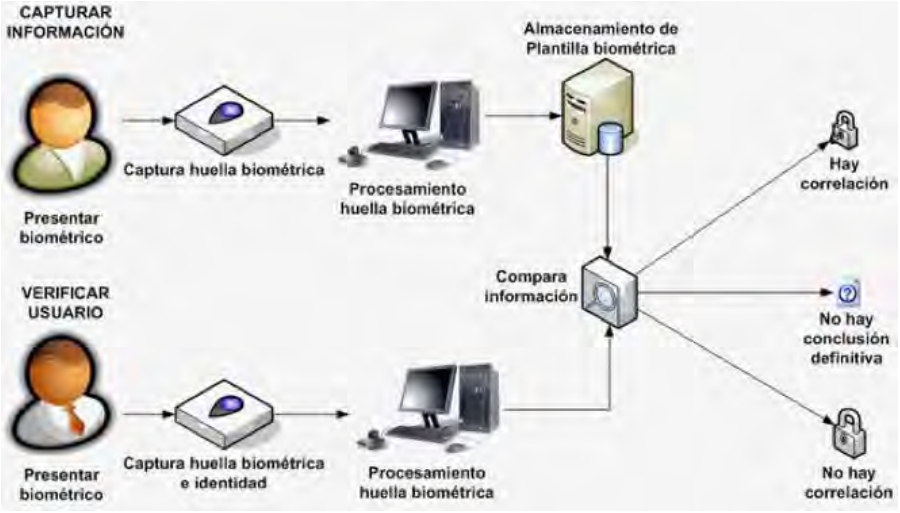

Figura 3. Procedimiento básico de captura, almacenamiento y consulta de datos para sistemas de identificación biométrica. Fuente: Barcelona (2010: 91-107).

El tipo de autentificación biométrica que realiza SIBIOS es bimodal, ya que incorpora dos tecnologías biométricas: el reconocimiento facial y la huella dactilar. Ello supera las limitaciones de un sistema biométrico unimodal –que incorpora solo una tecnología–, y de este modo al incorporar más se aumentan las posibilidades de identificación y la resistencia al fraude. Asimismo, tanto la huella dactilar como el reconocimiento facial poseen la ventaja de ser dos de las tecnologías que tienen mayor grado de implementación y desarrollo en el mercado biométrico, ya que también son dos de las más antiguas técnicas de reconocimiento biométrico. Ambas tienen un buen grado de aceptación entre los usuarios, es decir que en general están dispuestos a utilizarlas ya que no son demasiado intrusivas (Ortega García *et al.* 2008; Pérez San-José *et al.*, 2011).

Los Congresos CIBRA y biometría.gov.ar

Entre los años 2006 y 2013, se llevaron a cabo en la Ciudad de Buenos Aires los Congresos Internacionales de Biometría de la República Argentina (CIBRA), organizados por la Jefatura de Gabinete de Ministros de la Nación y auspiciados por distintas asociaciones y empresas privadas dedicadas a la tecnología. En estos congresos –declarados de Interés Nacional por la Secretaría General de la Presidencia (Resolución 169/2013) y de acceso libre y gratuito para el público en general con inscripción previa–, exponían e intercambiaban sus conocimientos expertos en materia de identificación biométrica, TIC y seguridad, tanto del ámbito público como privado a nivel nacional e internacional.

De Marinis (2004) observa que en Latinoamérica en los años 1980, y especialmente en los de 1990, "se verifica […] una complejización del entramado de relaciones entre lo público y lo privado, dando lugar a una inédita configuración de actores sociales y políticos". De este modo, "se erigen nuevos espacios sociales de intervención y surgen nuevos actores que desafían la clásica lógica dual de oposición del viejo esquema de relaciones entre 'Estado' y 'Sociedad Civil'" (p. 8). SIBIOS es creado en el año 2011 en este contexto de intercambio de conocimientos cercanos al discurso del management y a una criminología de tipo "actuarial". Se destaca asimismo la presencia de lo que podríamos llamar "analistas simbólicos" o "tecnopolíticos" para referirnos

Minerva AÑO IV VOL 1 JUNIO 2020, pp 82-107

a un tipo de actividad profesional que comenzó a proliferar en las últimas décadas, a la par de la revolución tecnológica y la globalización de los mercados financieros. Esta categoría es muy heterogénea y pueden encontrarse especialistas en diversas áreas temáticas. A su vez, en esta actividad de "servicios analítico-simbólicos", destaca un conjunto de actividades relacionadas con la identificación, solución y arbitraje de problemas mediante la manipulación de símbolos de diverso tipo, como datos, palabras, representaciones orales y visuales (De Marinis, 2004).

En tal sentido, en los CIBRA expuso una amplia gama de profesionales, formados en variados campos, como ingenieros (de diversas ramas: civil, informática, computación, sistemas, electrónica, industrial, telecomunicaciones, nuclear), analistas de sistemas, licenciados en Ciencias de la Computación, licenciados en Ciencias Matemáticas, peritos (de variadas ramas, como identificación de voz, papiloscopía, balística, documentología, reconstrucción criminal, accidentología vial, levantamiento de rastros y/o huellas latentes), fonoaudiólogos, odontólogos, técnicos en Seguridad y en Scopometría, licenciados en Seguridad, calígrafos, criminólogos, físicos, abogados, economistas, licenciados en Administración de Empresas, sociólogos, historiadores, politólogos, psicólogos, licenciados en Letras, licenciados en Marketing, etc.

La información sobre los ocho congresos que se celebraron estaban disponibles en el sitio web www.biometria.gov.ar (Figura 4), creado por el gobierno nacional de aquel entonces y era de libre acceso al público general. En él, figuraba información acerca de los expositores, los sponsors, la programación de los eventos, videos y archivos adjuntos con el contenido de presentaciones realizadas, entre otras cosas. Desde el CIBRA 2006 al 2011, se subió en el sitio contenido acerca de las presentaciones realizadas.

El sitio web tenía un acercamiento para el público en general, que puede carecer de conocimientos acerca de la biometría. De esta manera, contaba con una introducción a algunos de los principales métodos biométricos que se utilizan para la identificación de las personas: huella dactilar, ADN, facial, iris, palmar y voz. También tenía una introducción a la historia de la biometría, así como un glosario, preguntas frecuentes, noticias referentes a la biometría y enlaces de interés. Fue actualizado desde el año 2006 al 2013, período en el cual se realizaron los congresos, y luego de alcanzada la meta de crear e implementar el nuevo DNI, el pasaporte electrónico y SIBIOS. Fue dado de baja en 2016, durante el gobierno de Mauricio Macri.[3]

3 Antes de que el sitio web fuese dado de baja, hemos realizado una copia del mismo que obra en nuestro poder.

Figura 4. Portada principal del sitio web www.biometria.gov.ar

En el marco de los congresos, la Jefatura de Gabinete de Ministros de la Nación editó los libros *Biometrías: herramientas para la identidad y la seguridad pública y Biometrías 2*, que compilaban algunas de las presentaciones que realizaron los expositores de los CIBRA 2010 y 2011, respectivamente.

Los temas de las presentaciones realizadas en los CIBRA versaron principalmente sobre los proyectos de creación de una base de datos biométrica única de todos los ciudadanos argentinos; el gobierno electrónico y la firma digital; sistemas biométricos implementados en la Argentina por parte de provincias, organismos estatales y fuerzas de seguridad; sistemas de identificación biométrica estatales implementados en el extranjero; el voto electrónico; documentos de identidad biométrico y pasaporte electrónico; estándares internacionales e interoperabilidad; estado de situación de la biometría; aplicaciones comerciales; seguridad de los sistemas biométricos y protección de los datos personales; robo de identidad; nuevos desarrollos en tecnologías biométricas.

EL NUEVO DNI ARGENTINO Y EL PASAPORTE ELECTRÓNICO

Una de las cuestiones debatidas en los CIBRA, y que resultaba imperiosa para que el Estado pudiese dar un salto cualitativo en materia de identificación biométrica, era la confección de documentos identificatorios de los ciudadanos argentinos con los datos biométricos de su portador digitalizados, a la vez que tuviese mayores medidas de seguridad para evitar su falsificación o adulteración.

El Documento Nacional de Identidad (DNI) argentino, que se utiliza hasta el día de hoy como documento único para la identificación de todos los argentinos y extranjeros domiciliados en el país, fue creado por la Ley 17.671 del año 1968 ("Ley de Identificación, Registro y Clasificación del Potencial Humano Nacional") durante el gobierno militar de facto presidido por Juan Carlos Onganía. El DNI es emitido por el Renaper y reemplazó a la Libreta de Enrolamiento y a la Libreta Cívica (documentos que identificaban a varones y mujeres, respectivamente).

La Ley 17.671 que creó el DNI establece asimismo en su artículo N° 7 que "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", abriendo de este modo la puerta a la incorporación de las nuevas tecnologías de identificación biométrica.

En virtud de ello, las innovaciones en los DNI fueron introducidas en 2009 por el Decreto 1501/09 y las Resoluciones del Renaper N° 1800/2009 y 585/2012. El mencionado decreto autoriza la utilización de tecnologías digitales en la identificación de los ciudadanos nacionales y extranjeros, así como también en la emisión del DNI. De este modo, el nuevo DNI incluye, entre otras cosas, una fotografía digital del rostro de la persona de frente, huella digitalizada de dígito pulgar y la firma también digitalizada.

El nuevo DNI con los datos biométricos digitalizados se empezó a emitir en noviembre de 2009, y desde el 1 abril de 2017 es el único válido por la Resolución 1740/2016 del Renaper. Asimismo, desde enero de 2012, se emite también para recién nacidos (Res. 3459/2011). Anteriormente a la versión digitalizada, el DNI llevaba en la primera hoja una impresión en tinta del dígito pulgar derecho, una foto carnet pegada y la firma manuscrita del titular. Además, se guardaba un registro

Minerva AÑO IV VOL 1 JUNIO 2020, pp 82-107

decadactilar en tinta sobre unas fichas de papel. Hoy en día ese registro decadactilar se guarda en formato digital apoyando las yemas de los dedos sobre sensores ópticos. A diferencia del DNI anterior, el nuevo posee medidas de seguridad que tornan casi imposible su falsificación, ya que contiene laminado holográfico, fondos guilloches y numismáticos, numeración por quemado láser en relieve, kinegramas, tinta OVI (ópticamente variable), código PDF417 (código de barras de dos dimensiones que contiene datos biográficos y biométricos), entre otras cosas (Figura 5) (Renaper, s.f.).

Figura 5. Características y medidas de seguridad del nuevo DNI. Fuente: Renaper (s.f.).

Además, mediante el Decreto N° 261/11 se estableció la emisión del pasaporte electrónico por parte del Renaper. Dicho decreto deroga el 2015/1966, mediante el cual se designaba a la PFA como emisora de los pasaportes. Paralelamente, desde febrero de 2011 la PFA dejó de emitir la cédula de identidad, la cual no era de posesión obligatoria, tenía un formato tarjeta y servía a varios efectos para acreditar la identidad del portador (CELS, 2012). Si bien no era un sustituto del DNI, poseía características similares al nuevo DNI tipo tarjeta, como el hecho de ser fácil de portar y de formato plástico, por lo que se optó por dejar de emitirla.

El pasaporte electrónico posee una imagen digitalizada del rostro de su portador, de su firma y su digito pulgar. Asimismo, contiene un chip RFID (de identificación por radiofrecuencia)

incrustado de manera oculta en su contratapa, el cual permite verificar su autenticidad ya que posee datos biométricos de información facial, dactilar y de identidad. Además, se dejó de aplicar el número de DNI para identificar a cada libreta de pasaporte emitida, y se adoptó una identificación compuesta por tres letras y seis números, de acuerdo a estándares internacionales de seguridad (MIRA, s.f.).[4] Al igual que el DNI, también posee medidas de seguridad que tornan casi imposible su falsificación, entre ellas: numeración y perforación láser, embozado con tinta virante, validación por inspección electrónica, guilloches y fondos de seguridad irisados, tintas fugitivas y termocromáticas, tintas luminiscentes y perforación láser cónica (Figura 6) (CM, s.f.).[5]

Figura 6. Pasaporte electrónico con chip RFID incorporado. Fuente: Ya está en vigencia el Nuevo Pasaporte, 19 de junio de 2012.

El Decreto 261/11 faculta también a la Dirección Nacional del Renaper a celebrar convenios con la Dirección Nacional del Registro Nacional de Reincidencia y con la PFA, con el objetivo de intercambiar información de antecedentes personales al momento de emitir pasaportes. De esta manera, el 4 de marzo de 2011 se celebró un convenio entre el Renaper y la PFA mediante el cual se acordó que, frente a los registros de nuevas tramitaciones para la confección de pasaportes nacionales, se expida información a la PFA, como consta en los considerandos del Decreto 1766/2011. Por consiguiente, si bien el decreto quitó la emisión de los pasaportes de la órbita de la PFA, habilitó la posibilidad de que se expida información a esta al emitirlos.

Hacia una base única de identificación de todos los ciudadanos argentinos

Según Janices (2010) –entonces Director Nacional de la Oficina Nacional de Tecnologías de Información (ONTI)– hacia el año 2000, la PFA implementó el primer sistema AFIS para los procesos de verificación de identidad. Dicho sistema permitía almacenar cinco millones de juegos decadactilares de huellas digitales, realizar búsquedas sobre cincuenta mil imágenes de rastros dactilares dubitados y comunicarse con los cincuenta equipos Morpho Touch (equipos móviles de verificación dactilar) que habían sido incorporados, suministrándoles las huellas y los datos de individuos con pedidos de captura. Con el correr de los años, diversos organismos estatales fueron incorporando registros biométricos que permitían realizar identificaciones de manera automática. De este modo, durante los congresos CIBRA, distintos organismos estatales

4 MIRA - Ministerio del Interior de la República Argentina. (s.f.). Tramitar el pasaporte: preguntas frecuentes. Recuperado de https://www.argentina.gob.ar/interior/pasaporte/preguntasfrecuentes. Última vez consultado el 23/10/2020.

5 CM - Casa de Moneda. (s.f.). Pasaporte electrónico. Ministerio de Economía de la República Argentina. Recuperado de www.casademoneda.gob.ar/news/pasaporte-electronico. Última vez consultado el 23/10/2020

y fuerzas de seguridad nacionales y provinciales presentaron sus proyectos e implementaciones en sistemas biométricos, que dejaron en evidencia lo dispersos que estaban los avances en la instauración de dichos sistemas hasta el momento en la Argentina. En tal sentido, hacia el año 2010 los siguientes organismos nacionales poseían sistemas con información biométrica: el Renaper, la PFA, la Gendarmería Nacional Argentina, la Prefectura Naval Argentina, la Policía de Seguridad Aeroportuaria, el Servicio Penitenciario Federal, la Dirección Nacional de Migraciones, el Registro Nacional de Reincidencia, la AFIP y la ANSES. Por su parte, los siguientes organismos provinciales poseían sistemas con información biométrica: la Policía de la Provincia de Buenos Aires, la Procuración de la Provincia de Buenos Aires, la Policía de Mendoza, la Policía de La Pampa, la Policía de Neuquén, la Policía de Chubut y la Policía de Córdoba (ONTI, 2010).

Entre los principales inconvenientes que identificaba la ONTI se encontraba que no había comunicación entre los diferentes sistemas existentes, que había una posible duplicación de registros biométricos con distintas identidades patronímicas, que no había un estándar para interoperabilidad biométrica, que no había un estándar para equipamiento biométrico, que la mayoría de las dependencias nacionales no había digitalizado aún el total de sus registros biométricos a formatos adecuados para aplicaciones automatizadas y que no había un registro biométrico de NN (personas no identificadas) (Ídem). En consecuencia, desde el primer congreso, celebrado en noviembre de 2006, se destaca la necesidad de que la Argentina cuente con una base de datos única y centralizada de todos sus ciudadanos, que esté alineada a estándares internacionales unificados para que sea interoperable con bases de datos biométricas de otros países.

Thill, entonces Subsecretario de Tecnologías de Gestión de la Secretaría de Gestión Pública de la Jefatura de Gabinete de Ministros de la República Argentina, y una suerte de moderador y presentador en los congresos CIBRA, planteaba que su propósito era "abrir el debate en general sobre la necesidad de contar con herramientas que faciliten al Estado el cumplimiento de sus fines esenciales en materia de identificación de personas y, al mismo tiempo, que protejan a los ciudadanos en su derecho a la identidad" (2010: 15). Asimismo, consideraba que "la posibilidad de contar con una base de datos única de identificación plena de individuos […] facilitaría enormemente la concreción de políticas públicas de seguridad y de gobierno electrónico, apoyando también la implementación de políticas sociales" (p. 17).

De acuerdo con esto, Thill (2011) considera que el ejercicio de los derechos de las personas requiere necesariamente de su identificación plena, y que el Estado es el responsable de garantizar la identificación de cada una de ellas. Similar enfoque al de Janices (2011), quien cree que la base de las políticas de seguridad pública es la correcta identificación de las personas. De este modo, para Janices dichas políticas

> son imprescindibles para la constitución de una Nación ya que posibilitan la defensa de la identidad de las personas, y son una herramienta esencial contra el robo de identidad ayudando a la prevención y lucha contra el delito, la optimización de los sistemas de registro de tránsito fronterizo, la autenticación en transacciones comerciales, el ejercicio de derechos sociales y electorales, entre otros". (pp. 37-38)

En tal sentido, si bien el propósito securitario es el principal en la creación de una base de datos biométrica única de todos los ciudadanos, se destacan otros supuestos beneficios que puede tener para el ejercicio de derechos ciudadanos, los cuales sin una correcta y certera identificación por parte del Estado no estarían garantizados. Puede observarse en ello que "la seguridad (como

campo de prácticas de gobierno) no se reduce a las intervenciones orientadas a la gestión del delito, sino que incluye muchas otras que apuntan a la restitución de ciertos parámetros de orden y 'tranquilidad'" (Ríos, 2017a: 1).

En la misma línea, SIBIOS tuvo un spot oficial con el slogan "si nos conocemos más, nos cuidamos mejor", haciendo referencia a que "con el registro biométrico lo que queda resguardado y re-asegurado es nuestra identidad, y ello redunda en nuestra seguridad y posibilidades de protección" (Ríos, 2017b: 13). Tanto al principio como al final del video, un locutor repite la frase "ahora vos, sos vos", en contraposición a un pasado en que el destinatario del aviso no sería necesariamente quien es, ya que sin estar fichado por ese registro biométrico identificador único automatizado del Estado que es SIBIOS, su identidad podría ser usurpada fácilmente (MSNA, s.f.).

En dicho spot se destacan distintos beneficios además del securitario, como el hecho de que asegura la identidad insustituible de las personas, contribuye a combatir el delito de suplantación de identidad, a identificar a personas sin documentación en un accidente, a fortalecer los registros migratorios, al esclarecimiento y resolución en casos posdelito, también a encontrar a personas desaparecidas así como a menores con registro de paradero.

Con el objeto de ejemplificar algunos de estos beneficios mencionados anteriormente, en el spot se apela a casos que han tenido gran repercusión en los medios de comunicación y la opinión pública. Por ejemplo, cuando el locutor menciona que SIBIOS permitiría la identificación de personas sin documentación en un accidente, se muestra un recorte de diario del caso de Lucas Rebolini Manso (hijo del actor Antonio Grimau), quien en 2010 había permanecido más de un mes como NN en la morgue judicial hasta que lograron identificarlo gracias a la búsqueda que generó la repercusión mediática luego de que su familia hizo la denuncia por su desaparición (MSNA, s.f.). Asimismo, cuando la presentadora explica que si se realiza un chequeo en vivo con el AFIS, se podría identificar a menores con registro de paradero –más allá de que presente un DNI adulterado o falso–, se muestran recortes de diarios del caso de Sofía Herrera. El caso trata de la desaparición de una niña de 3 años en un camping de la localidad de Río Grande (Tierra del Fuego) en septiembre de 2008 y que se encuentra desaparecida desde entonces (MSNA, s.f.).

Una cuestión que también se repite en varias de las presentaciones y charlas como un beneficio de la biometría es la prevención que brinda en materia securitaria, algo que Barcelona (2010) –entonces Jefe de la Sección Base de Datos de la Superintendencia de Policía Científica de la PFA y disertante en el CIBRA 2010– define como la herramienta fundamental de la seguridad. Asimismo, el entonces Jefe de la PFA y Vicepresidente de Interpol Comisario Gral. Néstor Valleca, en la apertura del CIBRA 2010, define a los sistemas biométricos como "herramientas necesarias en materia de policía de seguridad, en la prevención del delito, y en materia de policía judicial para la investigación criminal" (Apertura CIBRA, 2010). Asimismo, Janices (2011) manifiesta que "las políticas de seguridad ciudadana deben fundarse en la prevención y disuasión de los posibles actos delictivos; y parte sustancial de esta política es la correcta y precisa identificación de las personas siendo esta una función esencial del Estado para la correcta verificación de la identidad" (p. 35). Por su parte, Fabián González –entonces Director de la Subsecretaría de Seguridad en Espectáculos Futbolísticos– considera a las técnicas de biometría como "técnicas de apoyo para brindar a la esfera de la prevención de la seguridad en los espectáculos futbolísticos" (2009).

En línea con estas posiciones, los principales beneficios de SIBIOS con respecto al delito son de tipo preventivo, ya que permite la identificación inmediata de personas que puedan resultar

sospechosas, con antecedentes o pedido de captura. Ello puede realizarse a través de chequeos en vivo con el AFIS o de identificaciones mediante las miles de cámaras de seguridad instaladas en la vía pública, muchas de las cuales actualmente permiten el reconocimiento automático de rostros en la Ciudad de Buenos Aires (Rodríguez Larreta presentó, 2019). En tal sentido, el art. 1 del Decreto 1766/11 establece que SIBIOS se crea "a los fines de contribuir a la comprobación idónea y oportuna en materia de identificación de personas y rastros, en procura de optimizar la investigación científica de delitos y el apoyo a la función preventiva de seguridad". Retomando a Garland (2005), podemos ubicar a SIBIOS como una tecnología de control poswelfarista, y dentro de estas, más cercana a las criminologías de la vida cotidiana, con su enfoque preventivo del delito. La necesidad de la interoperabilidad y estándares internacionales ha estado también presente en muchas de las presentaciones. Eso permite el intercambio de información biométrica entre organismos estatales y con organismos de otros países, y de este modo contribuye a combatir el delito más allá de las fronteras provinciales o nacionales. De este modo, ayudaría a capturar a delincuentes que entran y salen del país, y a combatir delitos típicamente trasnacionales como el terrorismo, el tráfico de drogas y de armas, la trata de personas, etc.

De acuerdo con Thill,

> en entornos globalizados, es necesario que estas aplicaciones sean interoperables con otras similares en distintos países. Es así que la existencia de estándares tecnológicos se hace necesaria e imprescindible para una efectiva implementación de políticas públicas de seguridad basadas en sistemas biométricos de identificación de individuos. (2010: 26)

En base a esta necesidad de interoperabilidad y alineamiento a estándares internacionales es que SIBIOS está basado en el formato estadounidense ANSI/NIST para el intercambio de información biométrica.[6]

Los esfuerzos del gobierno de Estados Unidos en materia de identificación biométrica e interoperabilidad se exponenciaron después de los atentados terroristas a las Torres Gemelas en septiembre de 2001 (National Science and Technology Council [NSTC], 2008). En esa línea, varios organismos estatales de ese país como el NIST, el Federal Bureau of Investigation (FBI), el Department of Homeland Security (DHS), y de policía internacional como la Organización Internacional de Policía Criminal (Interpol) dieron sus respectivas charlas en los congresos CIBRA sobre sistemas de identificación biométrica, estándares e interoperabilidad.

6 El ANSI es el Instituto Nacional Estadounidense de Estándares, mientras que el NIST es el Instituto Nacional de Estándares y Tecnología, el cual es una agencia de la Administración de Tecnología del Departamento de Comercio de los Estados Unidos.

Creación de SIBIOS

SIBIOS se instaura un año después de que la Presidenta Cristina Fernández de Kirchner creara el Ministerio de Seguridad de la Nación, su autoridad de aplicación. El Decreto 1993/2010 puso en funciones a este Ministerio el 10 de diciembre 2010, y tiene bajo su dependencia al Consejo de Seguridad Interior, la PFA, la PSA, la GNA y la PNA. Entre sus principales funciones, el Ministerio tiene a su cargo la determinación de los objetivos y políticas de seguridad interior a nivel nacional, así como la planificación, coordinación y supervisión del accionar individual y de conjunto de las fuerzas de seguridad y policiales, según determina el mencionado decreto.

El Ministerio de Seguridad fue creado luego de algunos sucesos que detallaremos a continuación. Por un lado, el gobierno nacional de ese entonces sufrió una derrota electoral en las elecciones

legislativas de 2009, en las cuales el tema de la inseguridad fue eje de las campañas partidarias (Galvani *et al.*, 2015). Por otro lado, hubo dos hechos acaecidos ese mismo año que reinstalaron el debate acerca de la falta de control político de la PFA. Uno fue el asesinato del militante del Partido Obrero, Mariano Ferreyra, el 20 de octubre de 2010 por parte de un grupo de gremialistas de la Unión Ferroviaria que intentaba frenar una protesta de empleados tercerizados del Ferrocarril Roca. En aquel entonces, funcionarios de la PFA fueron acusados de liberar la zona y de abandono de persona. El otro de los hechos fue el violento desalojo, llevado a cabo entre el 7 y el 10 de diciembre de 2010, de la ocupación del Parque Indoamericano en Villa Soldati (Ciudad de Buenos Aires) por parte de cientos de familias en reclamo de viviendas. En dicho acontecimiento se evidenció una actuación descoordinada entre la entonces Policía Metropolitana de la Ciudad de Buenos Aires y la PFA, y un uso desproporcionado de la fuerza de ambas policías (Dallorso, 2012).

El SIBIOS se nutre de los datos de las fotografías faciales y las huellas dactilares que toma el Renaper (Registro Nacional de las Personas) –organismo dependiente del Ministerio del Interior y Transporte– en los trámites de pasaporte electrónico y DNI biométrico, y también de datos como el ingreso y egreso de personas del territorio nacional y de las personas con causas penales. Asimismo, en el futuro el sistema podría incorporar datos del ADN, la voz y el iris ocular (MSNA, s.f.). La ONTI, dependiente de la Jefatura de Gabinete de Ministros, es la encargada de brindar el asesoramiento en lo concerniente a pautas de estandarización y compatibilidad de equipamientos, plataformas de hardware y software (Decreto 1766/2011).

Como mencionamos anteriormente, SIBIOS se crea con un propósito explícitamente securitario, y uno de los principales beneficios para la labor de las fuerzas de seguridad es la identificación rápida de individuos, ya sea a través de su identificación en vivo o a través de las cámaras de seguridad. En este sentido, no es casual que la instauración de SIBIOS se haya producido en un contexto en el cual la problemática de la llamada "inseguridad" se instaló en la Argentina en el tope de las encuestas de opinión pública, de los principales actores políticos y de la agenda de los medios masivos de comunicación. La concepción hegemónica del problema de la inseguridad refiere principalmente al miedo a la proliferación de delitos violentos, de poca monta y generalmente de carácter urbano. Esta construcción asume al delito como realizado por un "otro" amenazante, con determinadas características y asociado generalmente a la pobreza (Ayos, 2014; Daroqui, 2003; Kessler, 2009; Mouzo, 2012; Rangugni, 2010; Rodríguez Alzueta, 2014).

En torno a la problemática así definida ha crecido durante los últimos años el enfoque preventivo en materia securitaria. Esto se vio plasmado en distintas acciones, como la creación de policías locales con un enfoque de proximidad, el equipamiento tecnológico de última generación para las fuerzas de seguridad, la instalación de cámaras de seguridad tanto por parte del gobierno nacional como de los gobiernos locales, así como intervenciones orientadas a la modificación en el diseño de espacios públicos, justificadas en una *aggiornada* ideología de la defensa social: para desalentar su uso "indebido" por sujetos considerados "indeseables" y potencialmente "peligrosos" (Galvani *et al.*, 2015).

En cierto modo, en el spot oficial de SIBIOS se deja entrever esta concepción hegemónica de la inseguridad cuando el locutor menciona que "las fuerzas de seguridad de todo el país quedan integradas en una misma base de datos, pudiendo efectuar un mayor control sobre los ciudadanos con prontuario, y protegiendo la identidad del resto de la ciudadanía". En ese instante, se ve una grabación de una cámara de seguridad en la que un joven con ropa deportiva y gorra amenaza con un cuchillo a otro joven de distinto aspecto y desarmado, quien alza las manos en señal de rendición frente a esa amenaza (MSNA, s.f.).

Minerva AÑO IV VOL 1 JUNIO 2020, pp 82-107

De acuerdo con Ayos (2014), durante a la década de 1990 se produjo en Argentina una importante reorganización del campo de la política criminal en torno a una nueva trama de sentidos. Dicho campo pasaría a estar estructurado a partir de una nueva forma de problematizarlo alrededor de la noción de "inseguridad" y del clivaje seguridad-inseguridad. En palabras del propio Ayos,

> este nuevo problema es delimitado por una articulación de prácticas que provienen de ámbitos diversos, como el campo académico, los medios de comunicación o el propio campo de agencias de política criminal; pero aunque exista una significativa heterogeneidad entre ellos, la in/seguridad como objeto de intervención y reflexión, como ámbito de debates y disputas, muestra un cierto anudamiento de elementos antes dispersos, una serie de problemas, sensibilidades, interpretaciones, prescripciones y formas de intervención nuevas. (2014: 177)

En la misma línea, Ríos señala que "lo que llamamos (in)seguridad es una configuración de hechos y maneras de significarlos producido socialmente, y que por lo tanto tiene un carácter histórico y un devenir sumamente concreto" (2017a: 2). Por su parte, Ruibal considera que "el delito no es un concepto a priori que permanece a lo largo del tiempo […] su definición y la transformación de la misma está en relación con los cambios que se operan en el conjunto de la sociedad" (1993: 33).

Biometría y protección de datos personales

La mayoría de las presentaciones en las conferencias CIBRA destacaron los beneficios en materia biométrica y casos de éxito en su aplicación, pero poco se habló sobre las consecuencias negativas que la biometría pudiera llegar a tener en relación con la privacidad y la protección de los datos personales. Con respecto a este tema, la Dirección Nacional de Datos Personales (DNPDP) dio unas charlas sobre biometría y protección de datos personales. Travieso (2010) –entonces Director de la DNPDP– destaca que la principal precaución es resguardar los datos biométricos que sean objeto de tratamiento con las medidas de seguridad necesarias para evitar accesos indebidos o sustracciones a dichos bancos de datos.

Asimismo, Travieso considera que la protección de datos personales (reconocida en el año 1994 en nuestra Constitución a través del art. 43, y luego reglamentada por la Ley 25.326 de Habeas Data en el año 2000) "es la herramienta moderna que el derecho nos otorga para protegernos antes los riesgos que genera el tratamiento electrónico/informático de la información personal, en particular la técnica biométrica" (2010: 215). La biometría es entendida, de este modo, como una especie dentro del género "información", ya que podemos informarnos sobre la identidad de las personas a través de ella, y por ello cabe incluir a los datos biométricos en la categoría de datos identificatorios.

Por su parte, Kronzonas (2006) –entonces responsable del Registro de Bases Públicas del Registro Nacional de Bases de Datos de la DNPDP– plantea su preocupación por lo que podría causar a la protección de los derechos y libertades fundamentales una utilización amplia y sin control de la biometría. En este sentido, el artículo 2° de la Ley 25.326 define a los datos personales como "información de cualquier tipo referida a personas físicas o de existencia ideal determinadas o determinables". Por lo tanto, los datos biométricos extraídos para la identificación son personales y, a los efectos de la ley se los debe tratar como tales.

En los congresos CIBRA de 2006 y 2007, el Ministerio del Interior realizó la presentación del proyecto BDUIPI (Base de datos Única de Identificación Plena de Individuos). Se trata de un antecedente a SIBIOS para la identificación biométrica de la totalidad de los ciudadanos argentinos que finalmente no se concretaría. En la presentación de 2007, se detalló cómo el esquema de la base de datos custodiaría la identidad de la personas, con una independencia del proveedor de identificación biométrica y contemplando una separación de los datos biográficos y biométricos durante su tratamiento para que hubiese mayor imparcialidad de criterio de parte de los peritos intervinientes (Lope de Barrios *et al.*, 2007 y 2007b). Sin embargo, esa intención de resguardo de la identidad de las personas en el tratamiento de los datos es algo que posteriormente no queda explicitada claramente cuando se implementa SIBIOS.

Cuestionamientos por parte de organizaciones de la sociedad civil

Contemporáneamente a la aplicación de SIBIOS, distintas organizaciones de defensa de los derechos humanos y civiles se manifestaron en contra de este sistema y las nuevas tecnologías biométricas aplicadas por el gobierno nacional presidido en aquel entonces por Cristina Fernández de Kirchner. A su vez, señalaban de manera crítica que se hubiera llevado a cabo por decreto y sin el debido debate social y parlamentario.

Entre los principales argumentos en contra de la implementación de este tipo de tecnologías biométricas, se destaca el hecho de que no todos los países del mundo poseen un documento único identificatorio de la totalidad de sus ciudadanos como lo es el DNI argentino. Inglaterra, Irlanda, Estados Unidos, Australia, Canadá y Nueva Zelanda, por ejemplo, carecen de sistemas con este alcance de generalización (The World Bank Group, 2008). Se trata de países anglosajones de tradición liberal, que otorgan un lugar preponderante a la libertad del individuo, minimizando la intervención del Estado en la vida social y económica. En esos países donde no hay un documento único identificatorio, generalmente se utilizan distintos tipos de documentación personal establecidos para diversos fines a efectos de certificar la identidad de un individuo.

Asimismo, medidas similares a la creación de SIBIOS tuvieron que ser retrotraídas en otros países debido a la repercusión negativa que generaron en la opinión pública. En este sentido, en el Reino Unido, en el año 2010, una ley obligó al Estado a cancelar la creación de una tarjeta de identidad para todos los ciudadanos y a destruir todos sus datos biométricos almacenados (Identity, 2010). Por otra parte, en Francia, en el año 2012, se declaró inconstitucional una ley para crear un base de datos biométricos que afectaba a la casi totalidad de sus ciudadanos y que podía ser utilizada con fines policiales o judiciales, señalando que vulneraba derechos fundamentales vinculados a la privacidad y a las libertades públicas de los ciudadanos (Sentencia, 2012).

De acuerdo con la Asociación por los Derechos Civiles [ADC] (2014), este tipo de políticas de identificación masiva son aceptadas acríticamente por los ciudadanos argentinos, quienes siempre han tenido algún tipo de documento identidad de alcance nacional que los identificase. Asimismo, en la Argentina este tipo de medidas no se llevan a cabo a través de cambios legislativos, sino de actualizaciones tecnológicas por decreto, lo que también coarta la posibilidad de debatirlas. Por otra parte, si bien en materia de protección de datos personales el marco legal argentino puede considerarse uno de los mejores de la región (con una garantía constitucional en el artículo 43 introducida en la reforma de 1994), la Ley 25.326 de Protección de Datos Personales presenta dos debilidades estructurales: por un lado, un órgano de control débil y dependiente del Poder Ejecutivo, y por otro "una excesiva permisividad hacia el Estado en relación al almacenamiento, tratamiento y cesión de datos personales" (ADC, 2014).

Minerva AÑO IV VOL 1 JUNIO 2020, pp 82-107

En tal sentido, la garantía de consentimiento no aplica cuando los datos son recolectados por el Estado, ya que si bien el art. 5 de la Ley 25.326 exige el consentimiento libre, expreso e informado para el tratamiento de datos personales, establece también que no será necesario cuando los datos "se recaben para el ejercicio de funciones propias de los poderes del Estado o en virtud de una obligación legal". Asimismo, la ley dispone en su art. 11 que para la cesión de datos personales el titular de ellos tiene que haber dado su consentimiento. Sin embargo, este consentimiento tampoco es exigido cuando la cesión se realice directamente entre dependencias de los órganos del Estado, en cumplimiento de sus correspondientes competencias. Ello habilita al Estado a recabar los datos biométricos para SIBIOS sin consentimiento previo de su titular, así como compartir esta base de datos con distintos organismos del Estado, entre ellos, las fuerzas de seguridad, también sin el consentimiento del titular de los datos (ADC, 2014; ADC y Privacy International, 2016).

Otro de los puntos identificados como un problema es que la DNPDP no se encuentra como organismo especialista asesor del Ministerio de Seguridad en el Decreto 1766/11 que dispone la creación de SIBIOS, teniendo en cuenta que la DNPDP es el órgano de control que la Ley 25.326 estableció para el cumplimiento de los objetivos y demás disposiciones de la ley. En cambio, el art. 5 del decreto designó la creación de una Unidad de Coordinación que funcionaría dentro de la órbita del Ministerio de Seguridad y que estaría integrada por representantes de dicho Ministerio, del Renaper y de la Dirección Nacional de Migraciones, además de contar con el asesoramiento de especialistas de las áreas de la Policía Científica de la PFA, GNA, PNA y la PSA. Sin embargo, esta unidad nunca se creó, y, en la práctica, la coordinación la lleva a cabo la Dirección Nacional de Policía Científica, que se encuentra bajo la órbita de la Subsecretaría de Investigación del Delito Organizado y Complejo dependiente de la Secretaría de Seguridad del Ministerio de Seguridad de la Nación. Finalmente, en 2017, el Decreto 243 estableció que la Unidad de Coordinación y Seguimiento fuera llevada adelante directamente por la Dirección Nacional de Policía Científica (ADC, 2017).

Según la ADC y Privacy International (2016: 8), "la pobre supervisión de los órganos de inteligencia y de seguridad, y el hecho de que un amplio número de instituciones gubernamentales pueden acceder a SIBIOS significa que el sistema podría facilitar la vigilancia masiva". De este modo, SIBIOS se establecería como un dispositivo tecnológico de control y vigilancia que instituye un poder estatal omnipresente y constante sobre la totalidad de la ciudadanía argentina (Foucault, 2008).

También, advierten el riesgo de que SIBIOS pueda ser utilizado para fines distintos a los previstos, como en el caso del padrón electoral que incorpora las fotos de los ciudadanos provistas por el Renaper. Vale mencionar que en 2013, por una falla de seguridad, el sistema permitía descargar mediante un código de programación las imágenes de los votantes a través del sitio web oficial del padrón (ADC, 2014).

La Fundación Vía Libre es una de las que alzó su voz en contra de SIBIOS. Según Beatriz Busaniche, miembro de esta fundación, sistemas de esta naturaleza puestos en marcha a partir de la doctrina de la seguridad revierten la presunción de inocencia. Es decir, si anteriormente quedaban fichados en la base de datos por la Policía aquellos individuos con antecedentes (o quienes decidían tramitar la cédula de identidad o el pasaporte, los cuales eran expedidos por la PFA), ahora la totalidad de la ciudadanía queda fichada en esta gran base de datos. Este razonamiento advierte que ante la duda, todos quedamos fichados desde el nacimiento y seríamos considerados como presuntos delincuentes, aunque no hayamos cometido ningún delito. A su vez, Busaniche destaca

que tampoco fueron explicitados por el gobierno argentino los recaudos tomados a la hora de montar esta base de datos ni las condiciones de acceso a ella (Estado de vigilancia, 2012).

Otro documento que expresó su preocupación por los avances tecnológicos en materia biométrica y de trazabilidad electrónica impuestas por el gobierno nacional de aquel entonces fue el titulado "Los DNI electrónicos violan nuestros derechos", elaborado en octubre de 2014 y firmado por: Madres de Plaza de Mayo Línea Fundadora, la Asamblea Permanente por los Derechos Humanos, la Liga por los Derechos del Hombre, el Servicio Paz y Justicia, la Comisión Provincial por la Memoria, la Asociación por los Derechos Civiles, la Fundación Vía Libre y la Asociación Pensamiento Penal (Asociación Pensamiento Penal *et al.*, 2014).

Este último documento surgió a partir de que el entonces Ministro del Interior y Transporte Florencio Randazzo anunció que el DNI incluiría dos chips electrónicos con datos personales de índole biométrico, clínico, biográfico, de la movilidad diaria y del consumo de todos los ciudadanos argentinos (lo cual finalmente no se concretó). Las organizaciones firmantes consideraron injustificado que el DNI contuviera tanta información del ciudadano, y pusieron en duda que ello fuese a mejorar y simplificar los trámites que realiza la ciudadanía con el Estado. A su vez, cuestionaron también el pasaporte electrónico por poseer un chip con información integrada a una base de datos nacional, a diferencia de otras normativas como las de la Unión Europea, de Estados Unidos, Canadá y Australia, donde la información queda contenida en el chip como propiedad del ciudadano y solamente es utilizada para certificar su identidad en las terminales aeroportuarias.

Además, estas organizaciones manifestaron que era desproporcionado e innecesario que la SUBE fuera registrada con el DNI y domicilio de su portador, y de este modo permitiera trazar sus datos de movilidad y microconsumos. Consideran que estas iniciativas –junto con SIBIOS, al cual las fuerzas de seguridad tienen acceso irrestricto– exceden las competencias que debe tener el Estado y violan el derecho a la privacidad establecido en el art. 19 de la Constitución Nacional, el art. 11 de la Convención Americana de Derechos Humanos y el art. 12 de la Declaración Universal de Derechos Humanos.

Señala Avaro (2017) que la trazabilidad es un concepto que proviene del campo de la ingeniería y de la genética, pero que es bastante utilizado en el campo de estudio sobre la sociedad de vigilancia. Así es que "trazar no sólo consiste en identificar, clasificar, catalogar, archivar y almacenar, sino también relacionar, disponer, ubicar, vigilar y prestar atención a lo largo del tiempo a aquello que fue anteriormente identificado. La trazabilidad puede aplicarse a un objeto, pero también a las personas" (p. 257).

En estos análisis críticos, se parte desde una perspectiva que no reproduce acríticamente las utopías técnicas, sino que reconocen "que la relación que se da entre la utilización de las TIC y el desarrollo social no es una relación directa o inmediata" (Ríos, 2017a: 5). Antes bien, "la aplicación de las TIC en el campo de la seguridad y las discusiones que se dan en torno a su empleo constituyen un potente analizador del modo en que se estructura este campo de prácticas de gobierno" (Ríos y Fasciglione, 2015: 117).

Siguiendo a Galimberti (2001) podemos vislumbrar en estos planteos la idea de que la técnica –entendida como "el universo de los medios (las tecnologías), que en conjunto componen el aparato técnico, como la racionalidad que precede su empleo en términos de funcionalidad y eficiencia" (p. 2)– no es neutral. Es decir, se alejan de la idea de que la técnica ofrece los medios

Minerva AÑO IV VOL 1 JUNIO 2020, pp 82-107

que luego las personas decidirán si utilizar para el bien o para el mal, ya que crean un mundo con determinadas características y hacen contraer hábitos que inevitablemente transforman a las personas.

Conclusiones

SIBIOS es una herramienta que constituye un salto cualitativo significativo en lo referente a las técnicas de control por parte del Estado, y su instauración plantea posibles tensiones y riesgos para el ejercicio de los derechos y libertades ciudadanos. Sin embargo, ha pasado desapercibido para gran parte de la opinión pública argentina, y tanto su creación como sus condiciones de aplicación no han sido objeto de un debate público exhaustivo ni tampoco parlamentario.

Hay distintos factores que pueden ayudar a entender esta naturalización de la recolección sistemática de datos biométricos por parte del Estado argentino. Por un lado, el DNI es obligatorio para la identificación los ciudadanos y, por ende, para el reconocimiento de distintos derechos así como el otorgamiento de beneficios sociales. De hecho, el propio Renaper utiliza la consigna "la puerta de entrada a tus derechos" para promover la emisión del DNI (ADC, 2019).

Por otro lado, los gobiernos democráticos han utilizado la Ley 17.971 como base para ampliar los sistemas de identificación biométricos mediante decretos o resoluciones, ya que establece que el Renaper debe inscribir a los ciudadanos asignándoles un legajo de identificación con el testimonio de su nacimiento, impresiones dactiloscópicas, fotografías, descripción de señas físicas, datos individuales y grupo y factor sanguíneo. En este sentido, la ley sobre la cual está cimentado el sistema de identificación de la ciudadanía se encuentra atravesada por una lógica que tiene su origen en la ideología de una dictadura militar, situación que nunca fue cuestionada política o judicialmente (Ídem).

La continuidad de esta lógica a lo largo de los gobiernos democráticos puede observarse en que SIBIOS no solo continuó funcionando sin cuestionamientos bajo el gobierno de Mauricio Macri, sino que se amplió la cantidad de instituciones estatales con acceso a él mediante el Decreto 243/17. Por último, resulta interesante dejar abierto el planteo realizado por la Fundación Vía Libre en conjunto con la Electronic Frontier Foundation, sobre qué hubiese sucedido si en vez de estar en el poder de un gobierno democrático y con garantías constitucionales para los derechos de los ciudadanos, una base de datos de estas características hubiese caído en manos de un gobierno como el de la última dictadura militar argentina. Según ellos, el debate público se tendría que dar sobre ese poder y los límites que deberían fijársele (Rodríguez, 2012).

Bibliografía

Apertura Cibra (29 de noviembre de 2010). Archivo de video. 5º *Congreso Cibra.* Jefatura de Gabinete de Ministros, Presidencia de la Nación, Buenos Aires, Argentina. Recuperado de www.biometria.gov.ar

Asociación Pensamiento Penal et al. (6 de octubre de 2014). *Los DNI electrónicos violan nuestros derechos.* Recuperado de https://www.pensamientopenal.org/wp-content/uploads/2014/10/Solicitada-corregida-III-1.pdf. Última vez consultado el 23/1/2020.

Asociación por los Derechos Civiles [ADC] (2014). *El estado recolector. Un estudio sobre la Argentina y los datos personales de los ciudadanos*. Recuperado de https://adcdigital.org.ar/portfolio/el-estado-recolector/

Asociación por los Derechos Civiles [ADC] (2017). *La identidad que no podemos cambiar. Cómo la biometría afecta nuestros derechos*. Recuperado de: https://adcdigital.org.ar/2017/04/26/la-identidad-no-podemos-cambiar-biometria-sibios/

Asociación por los Derechos Civiles [ADC] (2019). *Tu yo digital. Descubriendo las narrativas sobre identidad y biometría en América Latina: los casos de Argentina, Brasil, Colombia y México.* Recuperado de https://adc.org.ar/wp-content/uploads/2020/06/050-tu-yo-digital-04-2019.pdf

Asociación por los Derechos Civiles (ADC) y Privacy International (2016). *El derecho a la privacidad en Argentina.* Recuperado de: https://privacyinternational.org/sites/default/files/2018-01/argentina_spanish.pdf

Avaro, D. (2017). Trazabilidad ciudadana y democracia: una aproximación desde la experiencia argentina. *Revista Mexicana de Ciencias Políticas y Sociales*, LXII (231), pp. 255-276. Recuperado de http://www.redalyc.org/articulo.oa?id=42152785010

Ayos, E. (2014). ¿Una política democrática de seguridad? Prevención del delito, políticas sociales y disputas en torno a la 'inseguridad' en la Argentina (2000-2010). *Revista del CLAD Reforma y Democracia,* (58), pp. 167-200. Recuperado de http://old.clad.org/portal/publicaciones-del-clad/revista-clad-reforma-democracia/articulos/058-Febrero-2014/Ayos.pdf

Barcelona, G. D. (2010). Biometría, la llave del futuro. Uso de herramientas biométricas aplicadas a políticas de seguridad. La experiencia de la Policía Federal Argentina. En Thill, E. (Comp.), *Biometrías: herramientas para la identidad y la seguridad pública.* Buenos Aires: Jefatura de Gabinete de Ministros, Presidencia de la Nación.

CELS - Centro de Estudios Legales y Sociales (2012). *Derechos Humanos en Argentina: informe 2012*. Buenos Aires: Siglo Veintiuno Editores.

CM - Casa de Moneda. (s.f.). *Pasaporte electrónico.* Ministerio de Economía de la República Argentina. Recuperado de www.casademoneda.gob.ar/news/pasaporte-electronico. Última vez consultado el 23/1/2020

Dallorso, N. (2012). La compleja relación entre el poder político y las fuerzas de seguridad: desafíos para el análisis de la emergencia del Plan Unidad Cinturón Sur de la Ciudad de Buenos Aires. *Hologramática: revista académica de la Facultad de Ciencias Sociales de la Universidad Nacional de Lomas de Zamora*, 2 (17), pp. 97-121. Recuperado de https://cienciared.com.ar/ra/usr/3/1410/hologramatica_n17v2pp97_121.pdf

Daroqui, A. (2003). Las seguridades perdidas. Argumentos. *Revista de crítica social,* 1(2). Recuperado de https://publicaciones.sociales.uba.ar/index.php/argumentos/article/view/815/701

De Marinis, P. (2004). In/seguridad/es sin sociedad/es: cinco dimensiones de la condición postsocial. En I. Muñagorri y J. Pegoraro (coords.). *La relación seguridad-inseguridad en centros urbanos de Europa y América Latina: Estrategias, políticas, actores, perspectivas y resultados.* Madrid: Dykinson.

"Estado de vigilancia generalizado en Argentina" (10 de mayo de 2012). Fundación Vía Libre. Recuperado de https://www.vialibre.org.ar/2012/05/10/estado-de-vigilancia-generalizado-en-argentina/. Última vez consultado el 23/1/2020.

Foucault, M. (2008). Ilegalismos y delincuencia. En *Vigilar y Castigar: nacimiento de la prisión.* (2° ed. argentina). Buenos Aires: Siglo XXI.

Galimberti, U. (2001). Psiché y Techné: Introducción. *Revista Artefacto. Pensamientos sobre la técnica*, (4). Recuperado de http://postitulo.sociales.infd.edu.ar/archivos/repositorio/250/398/TSMC_Clase-1_Galimberti.pdf

Galvani M.; Rios A. y Cañaveral, L. (2015). *Seguridad, policía y gobiernos locales: el Programa Integral de Protección Ciudadana*. Buenos Aires: CLACSO.

García Ferrari, M. (2007). "Una marca peor que el fuego". Los cocheros de la ciudad de Buenos Aires y la resistencia al retrato de identificación. En L. Caimari (comp.), *La ley de los profanos: Delito, justicia y cultura en Buenos Aires* (1870-1940). Buenos Aires: Fondo de Cultura Económica.

García Ferrari, M. (2010). *Ladrones conocidos / Sospechosos reservados: identificación policial en Buenos Aires, 1880-1905*. Buenos Aires: Prometeo Libros.

Garland, D. (2005). *La cultura del control: crimen y orden social en la sociedad contemporánea.* Barcelona: Gedisa.

González, F. (24 de noviembre de 2009). Utilización de la biometría para la seguridad en los espectáculos futbolísticos [Archivo de video]. *4º Congreso Cibra.* Jefatura de Gabinete de Ministros, Presidencia de la Nación, Buenos Aires, Argentina. Recuperado de www.biometria.gov.ar

Identity Documents Act 2010 (chapter 40). Parlamento del Reino Unido, Londres, 21 de diciembre de 2010. Recuperado de http://www.legislation.gov.uk/ukpga/2010/40/pdfs/ukpga_20100040_en.pdf. Última vez consultado el 23/1/2020.

Janices, P. (2010). *Argentina Biométrica. La tecnología al servicio de la defensa de la identidad y la seguridad pública*. En E. Thill (comp.). *Biometrías: herramientas para la identidad y la seguridad pública* (pp. 41-53). Buenos Aires: Jefatura de Gabinete de Ministros, Presidencia de la Nación.

Janices, P. (2011). Herramientas biométricas para la inclusión social y digital. En E. Thill (Comp.), *Biometrías 2*. Buenos Aires: Jefatura de Gabinete de Ministros, Presidencia de la Nación.

Kessler, G. (2009). *El sentimiento de inseguridad: sociología del temor al delito.* Buenos Aires: Siglo Veintiuno Editores.

Kronzonas, D. (noviembre, 2006). Biometría y la Ley Nº 25.326. En 1º Congreso Internacional de Biometría de la República Argentina (CIBRA). Jefatura de Gabinete de Ministros, Presidencia de la Nación, Buenos Aires, Argentina.

Lope de Barrios, Nicolás; Alonso, Diego y Mantovani, Ariel (2007). Base de Datos Única de Identificación Plena de Individuos (BDUIPI) [Diapositiva de PowerPoint]. 2º Congreso Cibra. Jefatura de Gabinete de Ministros, Presidencia de la Nación, Buenos Aires, Argentina. Recuperado de www.biometria.gov.ar

Lope de Barrios, Nicolás; Alonso, Diego y Mantovani, Ariel (30 de noviembre de 2007b). Base de Datos Única de Identificación Plena de Individuos [Archivo de video]. 2º Congreso Cibra. Jefatura de Gabinete de Ministros, Presidencia de la Nación, Buenos Aires, Argentina. Recuperado de www.biometria.gov.ar

MIRA - Ministerio del Interior de la República Argentina. (s.f.). *Tramitar el pasaporte: preguntas frecuentes.* Recuperado de https://www.argentina.gob.ar/interior/pasaporte/preguntasfrecuentes. Última vez consultado el 23/1/2020.

Montiel Álvarez, T. (2016). La fotografía policial en el siglo XIX: el sistema Bertillon. *ArtyHum: Revista Digital de Artes y Humanidades,* (1), pp. 148-159. Recuperado de: https://www.artyhum.com/descargas/PDF/ArtyHum%20n%C2%BA%2021.pdf

Moses, K.; Higgins, P.; McCabe, M.; Prabhakar, S. y Swann, S. (2011). Chapter 6: Automated Fingerprint Identification System (AFIS). En *The Fingerprint Sourcebook.* Washington D.C.: National Institute of Justice. Recuperado de: https://www.ncjrs.gov/pdffiles1/nij/225320.pdf

Mouzo, K. (2012). Inseguridad y "populismo penal". *URVIO*, *Revista Latinoamericana de Seguridad Ciudadana,* (11), pp. 43-51.

MSNA - Ministerio de Seguridad de la Nación Argentina (23 de octubre de 2017). *Identificación biométrica para la seguridad: El SIBIOS ya tiene cobertura nacional.* Recuperado de https://www.argentina.gob.ar/noticias/identificacion-biometrica-para-la-seguridad. Última vez consultado el 23/1/2020.

MSNA - Ministerio de Seguridad de la Nación (s.f.). *Spot oficial de Sibios* [Archivo de video]. Recuperado de https://www.youtube.com/watch?v=ggnhxVDayiA. Última vez consultado el 23/1/2020.

National Science and Technology Council (NSTC). (2008). *Biometrics in Government Post 9/11.* Recuperado de https://www.hsdl.org/?view&did=235185

Niklas P., Barrera G. (2017). Biometría aplicada a la seguridad. En Vercelli, A. y Zukerfeld, M. (Presidencia). *Simposio Argentino sobre Tecnología y Sociedad (STS) – 46 Jornadas Argentinas de Informática (JAIIO).* Universidad Tecnológica Nacional (UTN), Facultad Regional de Córdoba, Córdoba, Argentina. Recuperado de http://www.clei2017-46jaiio.sadio.org.ar/sites/default/files/Mem/STS/STS-16.pdf

ONTI - Oficina Nacional de Tecnologías de la Información (2010). *Red nacional de información biométrica* [Diapositiva de PowerPoint]. Subsecretaría de Tecnología de Gestión, Jefatura de Gabinete de Ministros, Presidencia de la Nación. Recuperado de https://www.nist.gov/system/files/documents/2016/12/12/argentina.pdf Última vez consultado el 23/1/2020.

Ortega García, J., Alonso Fernández, F., Coomonte Belmonte, R. (2008). *Biometría y seguridad.* Madrid: Fundación Rogelio Segovia para el Desarrollo de las Telecomunicaciones.

Pérez San-José, P.;Álvarez Alonso, E.; de la Fuente Rodríguez, S.; García Pérez, L.; Gutiérrez Borge, C. (2011). *Estudio sobre las tecnologías biométricas aplicadas a la seguridad.* Madrid: Instituto Nacional de Tecnologías de la Comunicación (INTECO).

RAE - Real Academia Española (s.f.). Biometría. *Diccionario de la lengua española.* Recuperado de https://dle.rae.es/biometría. Última vez consultado el 23/10/2020.

Rangugni, V. (2010). El problema de la in/seguridad en el marco del neoliberalismo en Argentina. En S. Torrado (Directora). *El costo social del ajuste* (Argentina 1976-2002). Buenos Aires: EDHASA.

Renaper (s.f.). *Características y medidas de seguridad de tu DNI.* Ministerio del Interior. Recuperado de https://www.argentina.gob.ar/interior/dni/caracteristicas-y-medidas-de-seguridad-de-tu-dni. Última vez consultado el 23/1/2020.

Ríos, A. L. (2017a). Las TICs y el gobierno de la seguridad. En *1º Jornadas de estudios sociales sobre delito, violencia y policía "La seguridad en cuestión".* Universidad Nacional de La Plata y Universidad Nacional de Quilmes, La Plata y Quilmes, Argentina.

Ríos, A. L. (2017b). El empleo de las TIC's y la reconfiguración del campo del gobierno de la seguridad: el Sistema Federal de Identificación Biométrica para la Seguridad (SIBIOS) de Argentina. En XXXI *Congreso Alas.* Asociación Latinoamericana de Sociología, Montevideo, Uruguay.

Ríos, A. y Fasciglione, L. (2015). Nuevas tecnologías de la información y comunicaciones (TICs) en el campo de la seguridad. En *Minerva. Revista de la Secretaría de Investigación y Desarrollo del Instituto Universitario de la Policía Federal Argentina,* (1), 116-124. Recuperado de https://www.universidad-policial.edu.ar/pdf/iyd/iyd_RevistaMinerva_2015-1_1.pdf

Rodríguez Alzueta, E. (2014). *Temor y control: La gestión de la inseguridad como forma de gobierno.* Ciudad Autónoma de Buenos Aires: Futuro Anterior Ediciones.

Rodríguez, K. (10 de enero de 2012). *Biometría en Argentina: la vigilancia masiva como política de estado.* Fundación Vía Libre y Electronic Frontier Foundation. Recuperado de https://www.vialibre.org.ar/2012/01/10/biometria-en-argentina-la-vigilancia-masiva-como-politica-de-estado/. Última vez consultado el 23/10/2020.

Rodríguez Larreta presentó el Sistema de Reconocimiento Facial De Prófugos: "El objetivo es que los vecinos estén más seguros" (26 de abril de 2019). Sitio web del Gobierno de la Ciudad de Buenos Aires. Recuperado de https://www.buenosaires.gob.ar/jefedegobierno/noticias/rodriguez-larreta-presento-el-sistema-de-reconocimiento-facial-de-profugos. Última vez consultado el 23/1/2020.

Romero, J. L. (2004). *Breve historia de la Argentina.* Buenos Aires: Fondo de Cultura Económica.

Rosales Cruz, A. (2009). *Clasificación de huellas digitales mediante minucias.* Tonantzintla: Instituto Nacional de Astrofísica, Óptica y Electrónica (INAOE). Recuperado de: https://ccc.inaoep.mx/~esucar/Clases-mgp/Proyectos/reporte_modelos_huellas.pdf

Ruibal, B. C. (1993). *Ideología del control social:* Buenos Aires 1880-1920. Buenos Aires: Centro Editor de América Latina.

Sarzuri Flores, V. (2014). Algoritmo de Clasificación de Huellas Dactilares Basado en Redes Neuronales Función Base Radial. *Revista del Postgrado en Informática* (1). Recuperado de: http://www.revistasbolivianas.org.bo/scielo.php?pid=S3333-77772014000100021&script=sci_arttext. Última vez consultado el 23/01/2020.

Sentencia N° 2012-652 DC (22 de Marzo de 2012). Ley relativa a la protección de la identidad. Consejo Constitucional de Francia. Recuperado de https://www.conseil-constitutionnel.fr/es/decision/2012/2012652DC.htm Última vez consultado el 23/1/2020.

Sirimarco, M. (2007). Indicios. Semiología policial del cuerpo de los "otros". *Ultima Ratio*, 1(1), 199-229.

The World Bank Group (2008). *Global Identification For Development (ID4D) Dataset 2018.* Recuperado de https://development-data-hub-s3-public.s3.amazonaws.com/ddhfiles/94586/wb_id4d_dataset_2018_0.xlsx. Última vez consultado el 23/01/2020.

Thill, E. (2010). Biometría y políticas de seguridad: de la ciencia ficción a la agenda pública. En Thill, E. (comp.). *Biometrías: herramientas para la identidad y la seguridad pública*. Buenos Aires: Jefatura de Gabinete de Ministros, Presidencia de la Nación.

Thill, E. (2011). El rol de la identificación de personas en las políticas de desarrollo e inclusión digital: el Marco para la Identificación Electrónica Social Iberoamericana. En Thill, E. (Comp.), *Biometrías 2.* Buenos Aires: Jefatura de Gabinete de Ministros, Presidencia de la Nación.

Travieso, J. A. (2010). La protección de los datos personales y la biometría: ¿derechos en oposición o en conjunción? En Thill, E. (Comp.), *Biometrías: herramientas para la identidad y la seguridad pública*. Buenos Aires: Jefatura de Gabinete de Ministros, Presidencia de la Nación.

Ya está en vigencia el Nuevo Pasaporte (19 de junio de 2012). Agencia de Noticias San Luis. Recuperado de http://www.agenciasanluis.com/notas/2012/06/19/ya-esta-en-vigencia-el-nuevo-pasaporte. Última vez consultado el 23/01/2020.

* El artículo se basa en la ponencia "Debates públicos en torno a la creación del Sistema Federal de Identificación Biométrica (SIBIOS): tensiones entre seguridad y privacidad", presentada en las XIII Jornadas de Sociología en la Facultad de Ciencias Sociales de la Universidad de Buenos Aires (agosto de 2019), y en las X Jornadas de Jóvenes Investigadorxs del Instituto de Investigaciones Gino Germani (IIGG) de la Universidad de Buenos Aires (noviembre de 2019). Asimismo, es parte de un proyecto de investigación para la realización de la tesina de grado de Ciencias de la Comunicación (UBA).