La identidad que no podemos cambiar

Cómo la biometría afecta nuestros derechos humanos

por los Derechos Civiles

Área Digital
Asociación por los Derechos Civiles

por los Derechos Civiles

Con el apoyo de
PRIVACY INTERNATIONAL

Abril 2017
https://adcdigital.org.ar

Este trabajo fue realizado como parte de un proyecto financiado por el International Development Research Centre (IDRC), el mismo es publicado bajo una licencia Creative Commons Atribución–No Comercial–Compartir Igual. Para ver una copia de esta licencia, visite: https://creativecommons.org/licenses/byncsa/2.5/.

creative commons

El documento *La identidad que no podemos cambiar. Cómo la biometría afecta nuestros derechos humanos* es de difusión pública y no tiene fines comerciales.

Índice

La identidad que no podemos cambiar

Cómo la biometría afecta nuestros derechos humanos*

I Introducción

A comienzos de 2015, la ADC publicó su informe "Si nos conocemos más, nos cuidamos mejor"[1] enfocado en el análisis de las políticas de biometría en la Argentina. Este trabajo representó el primer paso de la organización en el estudio de las tecnologías de vigilancia que funcionan en base de las características biológicas y de comportamiento de las personas, y, en particular, buscó echar un poco de luz sobre el principal sistema estatal diseñado con tal fin: el Sistema Federal de Identificación Biométrica para la Seguridad, conocido como SIBIOS, y catalogado globalmente como uno de los más invasivos para la privacidad de las personas.[2]

Este primer acercamiento nos permitió arribar a ciertas conclusiones. Por un lado, el marco normativo bajo el cual se sustenta la recolección de datos de los ciudadanos cuenta con un dudoso matiz democrático. Por otro lado, la población argentina se ha acostumbrado y ha naturalizado este tipo de prácticas, a diferencia de lo que ocurre en otros países alrededor del mundo en donde la implementación de este tipo de sistemas ha encontrado diversos grados de resistencia por parte de la ciudadanía.[3] Finalmente, la investigación nos mostró que SIBIOS -hasta el momento de publicación del informe- aún no se encontraba completamente implementado.

---

*El presente informe fue elaborado por **Leandro Ucciferri**, abogado e investigador del Área Digital de la Asociación por los Derechos Civiles. Con la colaboración de **Valeria Milanes**, Directora del Área Digital de la ADC, **Eduardo Ferreyra**, abogado e investigador del Área Digital de la ADC, y **Alejandro Segarra**, Director del Área de Litigio Estratégico de la ADC.

[1] "Si nos conocemos más, nos cuidamos mejor", ADC, 2015, disponible en (PDF): http://www.adc.org.ar/wp-content/uploads/2015/05/InformeBiometriaADC2015.pdf

[2] Entrevista de Infobae a Julian Assange, junio de 2013: https://www.youtube.com/watch?v=h_Q6kLqpRuA

[3] Cabe mencionar el caso del Reino Unido en 2010: "Success Story: Dismantling UK's Biometric ID Database" [Casos de éxito: desmantelamiento de la base de datos de identificación biométrica del Reino Unido], EFF, https://www.eff.org/pages/success-story-dismantling-uk%E2%80%99s-biometric-id-database; y el caso de Australia según lo relatado por el siguiente informe de Privacy International en 1996: "On Campaigns of Opposition to ID Card Schemes" [Campañas de Oposición a los Esquemas de Tarjeta de Identidad], https://www.privacyinternational.org/node/921

Este documento se presenta como una continuación y actualización de nuestro trabajo iniciado en años anteriores. Con el fin de ser lo más precisos posible y facilitar la lectura de este informe, reiteraremos conceptos e información que ya han sido mencionados en nuestro documento previo.

Con el objetivo de obtener información detallada y relevante para actualizar nuestro trabajo, realizamos pedidos de acceso a la información pública como una herramienta crucial, no solo para nutrir nuestra investigación sino también para poner en evidencia la transparencia del Estado en temáticas sensibles como es la seguridad y la vigilancia. Los mismos fueron presentados ante el Ministerio de Seguridad, el Ministerio del Interior, el Ministerio de Modernización (específicamente la Oficina Nacional de Tecnologías de Información) y la Dirección Nacional de Protección de Datos Personales.

Este informe procede de la siguiente manera. En el segundo capítulo se explica cuáles son las principales problemáticas en el campo de la biometría desde un punto de vista tecnológico, exploramos los efectos que tiene la vigilancia en el comportamiento de las personas, y narramos brevemente dónde se encuentra parado el mundo en el debate por las tecnologías de identificación de personas. El tercer capítulo está dedicado al Sistema Federal de Identificación Biométrica para la Seguridad (SIBIOS), en donde analizamos su funcionamiento, qué datos son recolectados, cómo es el proceso de recolección de dichos datos, los organismos y provincias que forman parte del Sistema, la tecnología utilizada, y los usos prácticos del Sistema. Finalmente, concluimos en el cuarto capítulo ponderando la implementación de tecnología para la identificación biométrica y la actual y potencial vulneración de derechos fundamentales, para el caso de continuar la implementación de este sistema tal y como se viene realizando.

II Biometría y derechos humanos

i La infalible (in)seguridad de la tecnología biométrica

La biometría es el proceso por el cual se busca reconocer, autenticar e identificar a una persona, en base a sus características físicas o de comportamiento. Generalmente se la clasifica en tres categorías de características: biológicas, morfológicas y de comportamiento.

Las características biológicas son el ADN y la sangre; dentro de las morfológicas se incluyen la forma de la mano, la huella palmar, las huellas dactilares, los patrones de las venas, el rostro, el iris y el patrón de venas de la retina, la voz, y las orejas; finalmente, en las características de comportamiento encontramos la manera y postura al caminar, la firma, y el tipeo en el teclado.

La introducción de la biometría en tecnologías que utilizamos a diario ha cobrado un salto exponencial en los últimos años. Uno de los ejemplos más claros es la popularidad que ha logrado el reconocimiento de huellas dactilares entre los fabricantes de dispositivos como un método para

asegurarlos, pasando del nicho profesional orientado a negocios, a productos dirigidos al público en general. La incorporación de lectores de huellas dactilares en nuestros *smartphones* y tablets –como encontramos en los productos de Apple y los principales fabricantes de teléfonos con Android– ha comenzado a naturalizar el uso de rasgos biológicos en nuestra rutina diaria: desbloqueamos nuestro smartphone –aproximadamente 80 veces al día[4]–, compramos aplicaciones y contenido multimedia, todo con simplemente apoyar nuestro dedo en el lector. En igual sentido, Microsoft se ha encargado de introducir una nueva función en las últimas versiones de su sistema operativo que facilita el acceso de los usuarios, usando su huella dactilar (encontramos ejemplos de la implementación de esta tecnología en *notebooks* desde al menos principios del cambio de siglo) o su rostro, conocido como Windows Hello.[5]

Como bien menciona Deibert: "Uno de los mercados más lucrativos, y potencialmente el más preocupante para la privacidad, es el de la biometría y los sistemas de reconocimiento facial. Aunque desarrollado para fines militares, fuerzas de seguridad y de inteligencia – aproximadamente el 70 por ciento de los gastos actuales –, el mercado de consumidores más amplio [doméstico/civil] está creciendo rápidamente. Muchas plataformas móviles y de *social media* utilizan la tecnología de reconocimiento facial en sus aplicaciones de fotos digitales para que los usuarios puedan etiquetar, categorizar y verificar sus identidades y las de sus amigos".[6]

A pesar de ser alabada como una tecnología infalible, la biometría no está exenta de ser vulnerable.[7] En tal sentido, es dable destacar dos puntos clave en el análisis de los sistemas que utilizan datos biométricos.

En primer lugar, nuestra información biométrica es mayormente pública. Por su misma naturaleza éstas carecen de secretismo alguno, a diferencia de las contraseñas. Esta característica ya genera dudas al momento de utilizar la biometría como medida de seguridad o protección.

Nuestros rasgos faciales son fácilmente accesibles a través de fotografías que cada día subimos públicamente a internet, o incluso pueden ser analizados de fotografías que nos toman sin siquiera enterarnos. Nuestras huellas dactilares pueden ser capturadas de una infinidad de elementos que tocamos en nuestro camino a diario, e incluso pueden ser utilizadas sin nuestro consentimiento, como el caso del niño de seis años que utilizó el pulgar de su madre mientras dormía para comprar regalos en Amazon.[8]

[4] "Apple says the average iPhone is unlocked 80 times a day" [Apple establece que el iPhone promedioesdesbloqueado 80 veces al día"], Nick Statt, The Verge, Abril 2016, http://www.theverge.com/2016/4/18/11454976/apple-iphone-use-data-unlock-stats

[5] Windows Hello face authentication

[6] Deibert, Ronald J. "Black Code: Surveillance, Privacy, and The Dark Side of the Internet", 2013, P.67.

[7] Vulnerabilities in Biometric Systems: Attacks and Recent Advances in Liveness Detection, Galbally, Fierrez, Ortega-Garcia, http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.186.3317

[8] "Your Children Already Know What They're Getting for Christmas—Thanks, Internet", Laura Stevens, The Wall Street Journal, diciembre 2016, https://www.wsj.com/articles/those-ads-that-follow-you-around-the-internet-are-

Diversos expertos en seguridad informática e investigadores han expuesto sobre la facilidad con la cual las huellas dactilares pueden ser recobradas a partir de una fotografía. Tal es el caso de un estudio realizado por un grupo de investigadores japoneses que pudieron capturar las huellas dactilares de personas que posaron en fotografías imitando el símbolo de la paz[9]; por otra parte, el *hacker* Jan Krissler llevó a cabo una presentación en el 31º Chaos Communication Congress (2014)[10], una conferencia anual de *hacking*, seguridad y tecnología, en la cual demostró el proceso mediante el cual se puede obtener y realizar una copia de una huella dactilar a partir de una botella de vidrio, la pantalla de un *smartphone*, y una fotografía; en este último caso de la Ministra de Defensa de Alemania, Ursula von der Leyen.[11]

Estudios sobre el uso de modelos de huellas dactilares para engañar sistemas biométricos pueden encontrarse al menos desde comienzos del siglo. En el año 2000, Putte y Keuning llevaron a cabo varios análisis y métodos para la creación de copias de huellas dactilares –tanto con la cooperación del dueño de esa huella, como sin ella–, encontrando que 5 de cada 6 lectores de huellas las aceptaba en el primer intento, y el sexto aceptándola al segundo intento.[12] En el año 2002, Matsumoto, Yamada, y Hoshino, estudiaron 11 sistemas de identificación biométrica distintos en los cuales probaron copias de huellas dactilares creadas en gelatina, encontrando que los 11 sensores aceptaban las huellas de gelatina con más de 67% de probabilidad de identificación positiva.[13] En mayo de 2016, The Verge –medio de noticias de tecnología– publicó un artículo en el cual recrean una técnica para falsificar huellas dactilares y poder acceder a un *smartphone*.[14]

Por lo expuesto anteriormente, cuando es el Estado quien se encarga de la recolección de huellas dactilares de sus ciudadanos, ¿Cuáles son las salvaguardas que se toman para evitar la manipulación y adulteración de las copias de las huellas almacenadas? ¿Qué tipo de garantías se deben establecer

ruining-christmas-1482507745

[9] "Japan researchers warn of fingerprint theft from 'peace' sign" [Investigadores japoneses advierten del robo de huellas dactilares a partir del símbolo de la paz], Phys.org, Enero 2017, https://phys.org/news/2017-01-japan-fingerprint-theft-peace.html

[10] El Chaos Communication Congress es organizado por el Chaos Computer Club, más información en el siguiente vínculo: https://www.ccc.de/en/

[11] "Hacker fakes German minister's fingerprints using photos of her hands" [Hacker falsifica las huellas dactilares de una Ministra alemana utilizando fotografías de sus manos], Alex Hern, TheGuardian, Diciembre 2014, https://www.theguardian.com/technology/2014/dec/30/hacker-fakes-german-ministers-fingerprints-using-photos-of-her-hands La presentación completa en el CCC -en alemán- puede accederse en el siguiente vínculo: https://www.youtube.com/watch?v=YE1EoxKV53w

[12] "Biometrical Fingerprint Recognition: Don't Get Your Fingers Burned" [Reconocimiento biométrico de huellas dactilares: No te quemes los dedos], Ton van der Putte y JeroenKeuning, 2002, https://cryptome.org/fake-prints.htm

[13] "Impact of Artificial 'Gummy' Fingers on Fingerprint Systems" [El impacto de los dedos de gelatina artificiales en sistemas de huelas dactilares], Tsutomu Matsumoto, Hiroyuki Matsumoto, Koji Yamada, y Satoshi Hoshino, 2002, https://cryptome.org/gummy.htm

[14] "Your phone's biggest vulnerability is your fingerprint" [La vulnerabilidad más grande de tu teléfono es tu huella dactilar], Russell Brandom, Mayo 2016, http://www.theverge.com/2016/5/2/11540962/iphone-samsung-fingerprint-duplicate-hack-security

para asegurar la integridad de los datos obtenidos?

En segundo lugar, un dato biométrico no puede ser reemplazado. Si olvidamos o nos roban nuestra contraseña podemos crear una nueva. En el caso de la biometría esto es prácticamente imposible; ¿Cómo generamos nuevas huellas dactilares para nuestros dedos? ¿Un nuevo rostro? ¿Una nueva voz? ¿Un nuevo iris?

Según establece el Dr. Hugo Scolnik[15], "Todos los métodos de identificación proceden primero a recoger información de un individuo (huellas dactilares, características de la cara como distancia entre ojos, forma de la boca, nariz, etcétera) y luego determinan una 'distancia' a los datos existentes en una base. Se decide si una persona se corresponde con una identidad si esa 'distancia' es menor que una 'tolerancia'. Entonces queda claro que los resultados dependen de ambos conceptos, y de ahí los posibles errores, pues con una 'tolerancia' grande se aumenta el número de 'coincidencias' y con una chica probablemente no haya ninguna, pues todo depende de, por ejemplo, la luz, el ángulo con el que se toma la fotografía, los colores de fondo, etcétera".[16]

Los desarrolladores de sistemas de identificación biométrica hablan de tres tipos de tasas de error:[17]

- **Tasa de rechazo falso**: En los casos en que el sistema no permite un acceso válido cuando se supone que debería;
- **Tasa de aceptación falsa**: En los casos en que el sistema valida el acceso cuando se supone que no debería hacerlo;
- **Tasa de error cruzada**: El punto en el cual la tasa de aceptación falsa es igual a la tasa de rechazo falso.

Esto es así pues el procedimiento de identificación biométrica se basa en estadísticas, no es una simple respuesta de "sí o no", por el contrario, es un proceso de probabilidades que implica lograr un equilibrio entre las tasas de error de acuerdo a los resultados que se pretendan obtener con el sistema de identificación, teniendo como resultado una identificación más o menos probable. Debido a que la determinación de las tasas de error depende exclusivamente de quien desarrolle la tecnología, aquí es donde entran en juego una infinidad de factores que pueden terminar por convertir al sistema en una herramienta capaz de afectar los derechos humanos.

[15] Lic. en Matemática por la Universidad de Buenos Aires y Doctor en Matemática por la Universidad de Zurich. Es profesor consulto titular del Departamento de Computación de la FCEN-UBA y CEO de la empresa Firmas Digitales SRL. Desde el 2009 se desempeña como Director Adjunto de la Maestría en Seguridad Informática de la Universidad de Buenos Aires.

[16] Informe elaborado para la Asociación por los Derechos Civiles, diciembre 2016. En Archivo en ADC.

[17] "Hidden Risks of Biometric Identifiers and How to Avoid Them", Dr. Thomas P. Keenan, Black-hat 2015. https://www.blackhat.com/docs/us-15/materials/us-15-Keenan-Hidden-Risks-Of-Biometric-Identifiers-And-How-To-Avoid-Them-wp.pdf

Un reciente estudio del *Center on Privacy & Technology*, de la Universidad de Georgetown, determinó que el reconocimiento facial tiene un grado de confiabilidad significativamente menor que, por ejemplo, la identificación a través de huellas dactilares, y que generalmente dichos sistemas no son exhaustivamente probados.[18] La baja confiabilidad de los sistemas de reconocimiento facial encuentra su razón de ser debido a determinados factores que influyen en cómo los algoritmos[19] determinan la probabilidad de identificación o verificación de una persona.

En tal sentido, encontramos que el ángulo desde el cual es tomada la fotografía, el tipo de fondo, la luz (si es natural o artificial, la hora del día, etcétera), el tamaño de la base de datos sobre la cual corre el sistema (es decir, la cantidad de fotografías de personas), el envejecimiento de la persona, el bello facial, las expresiones faciales, los elementos que obstruyan el rostro (como el pelo, anteojos, sombreros o gorras), pueden alterar el resultado alcanzado por el algoritmo del sistema de reconocimiento facial.[20]

Aun así, hay un problema de fondo que persiste. Existe una creencia generalizada de que la tecnología es amoral, objetiva y neutral. Si bien esto puede tener algún grado de certeza cuando pensamos en la tecnología *per se* –es decir, como simples objetos materiales– lo cierto es que no podemos disgregar al objeto material del fin para el cual fue concebido o para el cual se lo pretende utilizar. De esta forma, la objetividad de la tecnología se vuelve un concepto relativo, bajo el cual podemos afirmar que la misma adoptará el sesgo del individuo que pretenda utilizarla para un fin determinado.[21]

Entendiendo a los algoritmos como un conjunto de instrucciones o reglas que permiten calcular la respuesta a un problema, debemos partir de la base que dichas instrucciones han sido escritas por una persona, por lo que cabe la posibilidad de que, consciente o inconscientemente, sus sesgos y prejuicios sean trasladados al momento de escribir el código del algoritmo (*algorithmic bias*),[22] pues son estas personas quienes finalmente tomarán las decisiones de diseño en el desarrollo de la tecnología;[23] esto

[18] "The Perpetual Line-up: Unregulated Police Face Recognition in America", C. Garvie, A. Bedoya, J. Frankle, Center on Privacy & Technology, Georgetown University Law School, octubre 2016. https://www.perpetuallineup.org/findings/accuracy

[19] Un algoritmo es un "conjunto ordenado y finito de operaciones que permite hallar la solución de un problema". http://dle.rae.es/?id=1nmLTsh

[20] Para más información se puede consultar: "Face Recognition Vendor Test: Performance of Automated Gender Classification Algorithms", M. Ngan, P. Grother, NIST Interagency Report 8052, disponible en: http://nvlpubs.nist.gov/nistpubs/ir/2015/NIST.IR.8052.pdf; "Biometric Recognition: Challenges and Opportunities", J. N. Pato, L. I. Millett, The National Academies Press, disponible en: https://www.nap.edu/read/12720/chapter/1; "Face Recognition Algorithms", I. Marqués, Universidad del País Vasco, disponible en: http://www.ehu.eus/ccwintco/uploads/e/eb/PFC-IonMarques.pdf

[21] "Is Technology Neutral? Part II", Colin Rule, The Center for Internet and Society, Stanford Law School, septiembre 2006, https://cyberlaw.stanford.edu/blog/2006/09/technology-neutral-part-ii

[22] "The Foundations of Algorithmic Bias", Zachary C. Lipton, noviembre 2016, http://approximatelycorrect.com/2016/11/07/the-foundations-of-algorithmic-bias/

[23] Para más información, se pueden consultar las siguientes fuentes: "When Algorithms Discriminate", Claire C. Miller, The New York Times, julio 2015, https://www.nytimes.com/2015/07/10/upshot/when-algorithms-discriminate.html; "Why We Should Expect Algorithms to Be Biased", Nanette Byrnes, MIT Technology Re-

puede verse acentuado en el caso de los algoritmos de aprendizaje automático (*Machine Learning*)[24], en donde el sesgo puede ser replicado y aprendido por el algoritmo sin intervención humana.

Para hacer frente a los problemas de precisión que tienen los sistemas de reconocimiento facial, hay expertos en la temática que coinciden en que una persona debe revisar los resultados para asegurarse que sean correctos. Aunque, según el estudio de *Georgetown*, "la simple revisión humana de los resultados no es suficiente. Sin una formación especializada, los revisores humanos cometen tantos errores que la precisión general del reconocimiento facial puede disminuir cuando se toman en cuenta sus aportes. Los seres humanos comparan las caras con una serie de heurísticas psicológicas[25], que pueden convertirse en responsabilidades para los despliegues policiales del reconocimiento facial. Por ejemplo, hay estudios que muestran que los seres humanos son mejores en el reconocimiento de personas que ya conocen y de personas de la misma raza".[26]

Esto nos lleva a un punto fundamental cuando de tecnología se trata, que cobra aún más relevancia cuando es el Estado quien será el usuario. En el caso de la compra de la tecnología que da vida a los sistemas de identificación biométrica, ¿se han tenido en cuenta consideraciones mínimas sobre las características de la misma?

Dejando de lado la cuestión de los procesos formales de contratación en el ámbito estatal como son las licitaciones públicas, que pretenden asegurar el correcto uso de los fondos públicos y brindar transparencia al proceso de adquisición de bienes o contratación de servicios, la compra de tecnología presupone determinadas consideraciones a tener a cuenta al momento de elegir qué tipo de solución terminará sustentando el funcionamiento de un sistema y cómo se adecúa a las necesidades que tiene el usuario para los fines que tiene en mente.

A partir de lo reseñado en la presente sección del informe, vimos algunos de los principales problemas inherentes al funcionamiento del software que corren los sistemas de identificación biométricos. En tal sentido, cualquier adquisición que se planee hacer relacionada con esta tecnología debe estar sustentada y decidida sobre el análisis de factores mínimos como la exactitud del software de identificación o verificación (facial, de huellas dactilares, etcétera), lo cual implica responder y analizar una serie de preguntas, como por ejemplo ¿los algoritmos han sido probados? ¿en qué medida?, ¿cuáles fueron los resultados?, ¿cómo fue entrenado el algoritmo?, ¿puede haber conflictos

view, junio 2016, https://www.technologyreview.com/s/601775/why-we-should-expect-algorithms-to-be-biased/; y específicamente sobre algoritmos aplicados al reconocimiento facial: "Google apologises for Photos app's racist blunder", BBC News, julio 2015, http://www.bbc.com/news/technology-33347866

[24] https://es.wikipedia.org/wiki/Aprendizaje_autom%C3%A1tico

[25] "En la psicología, las heurísticas son reglas simples y eficientes que las personas a menudo usan para formar juicios y tomar decisiones. Son atajos mentales que suelen implicar centrarse en un aspecto de un problema complejo e ignorar a otros." https://en.wikipedia.org/wiki/Heuristics_in_judgment_and_decision-making

[26] "The Perpetual Line-up: Unregulated Police Face Recognition in America", C. Garvie, A. Bedoya, J. Frankle, Center on Privacy & Technology, Georgetown University Law School, octubre 2016, P.49. https://www.perpetuallineup.org/

con la identificación/verificación de determinadas etnias? ¿se ha evaluado la seguridad integral del sistema que se pretende correr?

Hasta este punto vimos las vulnerabilidades que podemos encontrar en los sistemas de identificación biométrica *per se*, pero es menester destacar otro problema que podemos encontrar en la implementación de sistemas de identificación biométrica: la centralización de información en una base de datos única.

El ex Relator Especial sobre la promoción y protección de los derechos humanos y las libertades fundamentales en la lucha contra el terrorismo de la Organización de las Naciones Unidas, Martin Scheinin, determinó en su informe publicado en el año 2009 que, si bien el uso de la biometría se presenta en determinadas circunstancias como una herramienta legítima para la identificación de sospechosos por casos de terrorismo, preocupa especialmente "los casos en que la biometría no se almacena en un documento de identidad, sino en una base de datos centralizada, incrementando los riesgos para la seguridad de la información y dejando a los individuos vulnerables. A medida que aumenta la información biométrica, las tasas de error pueden aumentar significativamente".[27]

El incremento en las tasas de error puede llevar a la criminalización ilícita de individuos o a la exclusión social. A la vez, el Relator destaca un aspecto que mencionamos anteriormente, la irrevocabilidad de los datos biométricos. "(...) Una vez copiados y/o utilizados fraudulentamente por un actor malicioso, no es posible emitirle a un individuo una nueva firma [identidad] biométrica".[28]

El problema inherente con las bases de datos centralizadas yace naturalmente en las características de las mismas como un único punto de acceso, almacenamiento, e intercambio de información. Desde un punto de vista de la seguridad informática, esto presenta serias preocupaciones vinculadas con las medidas que deben tomarse para proteger los datos allí almacenados, pues si no se toman los suficientes recaudos, implicaría que una persona pueda acceder a la totalidad de la información que se guarda en los servidores.

En tal sentido, es menester destacar un reciente antecedente sobre seguridad informática que involucra al principal ministerio responsable de SIBIOS. A fines de enero del 2017, la cuenta de Twitter de la Ministra de Seguridad de la Nación, Patricia Bullrich, junto con más de 30 cuentas de emails institucionales del Ministerio de Seguridad, fueron *hackeadas* como resultado de un *phishing*[29], tal como informó la División de Delitos Informáticos de la Policía Federal Argentina,[30] y como pudieron

[27] Informe del Relator Especial sobre la promoción y protección de los derechos humanos y las libertades fundamentales en la lucha contra el terrorismo, Martin Scheinin, 2009, P.10-11. http://www2.ohchr.org/english/bodies/hrcouncil/docs/13session/A-HRC-13-37.pdf

[28] Íbid.

[29] El phishing es la suplantación de identidad, generalmente de un sitio web, con el fin de engañar a la víctima para robar su información, como sus credenciales de inicio de sesión (usuario y contraseña), tarjeta de crédito, etcétera. Para más información consultar: http://www.welivesecurity.com/la-es/2015/05/08/5-tipos-de-phishing/

[30] "También hackearon 30 correos del Ministerio de Seguridad", La Nación, febrero 2017, http://www.lanacion.com.ar/1980702-tambien-hackearon-30-correos-del-ministerio-de-seguridad

constatar los usuarios de Twitter durante el lapso de tiempo que la cuenta se encontraba en manos ajenas.[31]

Los hechos acontecidos ponen de manifiesto la casi sistemática falta de atención e importancia que se le ha dado a la seguridad de la información que manejan los organismos estatales, a la vez que genera un interrogante en relación a la aptitud del personal del Ministerio para mantener mínimas prácticas de seguridad informática con el fin de enfrentar las problemáticas que día a día son más comunes en el mundo digital.

En lo respectivo a temáticas de ciberseguridad, la ADC ha realizado un estudio sobre la situación de la Argentina, desde 2011 hasta mediados del 2016, en el cual se resalta la falta de una estrategia nacional que haga frente a los principales desafíos que enfrenta el país en materia de ciberseguridad, incluyendo la infraestructura pública y privada, la seguridad de la información, y el cibercrimen, por nombrar algunos.[32]

ii Los efectos invisibles de la vigilancia

Cuando hablamos de tecnologías que facilitan la identificación masiva de personas, uno de los aspectos que no debemos dejar pasar por alto es el efecto que genera la vigilancia en el ejercicio y goce de derechos humanos (*chilling effects*[33]).

Como bien establece Scheinin, "Además de constituir un derecho en sí mismo, la privacidad sirve de base a otros derechos y sin la cual los demás derechos no podrían ser efectivamente gozados".[34] La privacidad es el derecho del individuo para decidir por sí mismo en qué medida compartirá con los demás sus pensamientos, sus sentimientos y los hechos de su vida personal,[35] es gracias a ella que podemos crear zonas en las cuales compartimentar todo aquello que nos hace humanos, nuestros vínculos familiares y amorosos, vínculos de amistad, relaciones profesionales, gustos, pensamientos, en definitiva todo aquello que define nuestra personalidad.

Gracias a las zonas privadas que este derecho nos permite generar, es que otros derechos y libertades pueden ser ejercidos con plenitud, particularmente la libertad de expresión, de pensamiento y de

[31] "El hackeo a @PatoBullrich y al @MinSeg", enero 2017, https://twitter.com/i/moments/824754207437766656

[32] "Ciberseguridad en la era de la vigilancia masiva", ADC, 2016, https://adcdigital.org.ar/portfolio/ciberseguridad-era-vigilancia-masiva/

[33] *Chilling effect* es un término en el derecho anglosajón, que describe una situación en la cual se reprime un discurso o una conducta por el temor a sufrir una penalización o represalia en los intereses de un individuo o un grupo.

[34] Informe del Relator Especial sobre la promoción y protección de los derechos humanos y las libertades fundamentales en la lucha contra el terrorismo, Martin Scheinin, 2009, P.13. http://www2.ohchr.org/english/bodies/hrcouncil/docs/13session/A-HRC-13-37.pdf

[35] Indalia Ponzetti de Balbin c/ Editorial Atlántida S.A. s/ Daños y Perjuicios, Corte Suprema de Justicia de la Nación, diciembre 1984 http://bit.ly/2oM7SJf

opinión, la libertad de asociación y de reunión, la libertad de culto, así como también la libertad de buscar y recibir información.

La vigilancia afecta el comportamiento de los individuos sobre los cuales la misma es llevada a cabo.[36] Por temor a enfrentar represalias o sufrir consecuencias inesperadas, las personas tienden a modificar su conducta cuando saben o sospechan que se encuentran bajo escrutinio de terceros; en el ámbito digital, esto puede significar auto-censurarse en las expresiones que uno haría en condiciones normales en sus cuentas de Twitter o Facebook, no buscar determinados temas en internet, o dejar de consumir cierto tipo de contenido multimedia en YouTube, Vimeo, Netflix o Spotify, por nombrar algunos ejemplos. El efecto de la vigilancia es aún más grave cuando ponemos como presupuesto los casos en los cuales se logra coartar la denuncia de abusos de poder e injusticias, dicho en otras palabras, cuando las personas que desean disentir no se sienten seguras de ejercer con plenitud su derecho democrático de protestar contra las políticas del gobierno o aquellos que retienen el poder.

La sensación de exposición pública, de perder el control sobre nuestra información, nuestros gustos y relaciones, en definitiva, todo aquello que hace a nuestra imagen y personalidad, puede llevar a una reclusión auto impuesta, auto censurarnos al momento de expresarnos e incluso en cómo pensamos, limitar nuestras relaciones, vínculos, y el desarrollo de todas aquellas cualidades que nos hacen humanos.

De esta forma, la identificación biométrica también puede llevar a conflictos con la libertad de expresión, pues la tecnología puede ser utilizada por distintos actores para vigilar a quienes buscan participar de actividades políticas, religiosas, y cualquier otra actividad protegida por la libre expresión. Esto es aún más problemático cuando la filmación de protestas y demostraciones públicas por parte de las fuerzas de seguridad, como la Policía Federal Argentina, se ha ido convirtiendo a lo largo de los años en una práctica cada vez más común.[37]

La tecnología de identificación biométrica, y particularmente el reconocimiento facial, viene a redefinir el concepto de espacio público como lo comprendíamos, un cambio que comenzamos a experimentar con la llegada de las cámaras de vigilancia (*CCTV*) y que es acentuado con tecnologías que permiten adentrarse en detalle en la vida pública de las personas, bajo el pretexto de la investigación del delito.[38]

Hay ciertas acciones que desarrollamos en espacios públicos que por el mero hecho de ser realizadas en ellos pueden no ser consideradas como una expresión para la exposición pública, sino que por el

[36] "The Chilling Effect Of Mass Surveillance Quantified", Tim Cushing, Techdirt, mayo 2016, https://www.techdirt.com/articles/20160429/07512934314/chilling-effect-mass-surveillance-quantified.shtml

[37] Al respecto de la filmación de protestas y movimientos sociales por parte de la Policía Federal Argentina, se pueden consultar los siguientes Tweets: caso 1; caso 2; caso 3; caso 4; caso 5; caso 6; caso 7; caso 8; caso 9

[38] A comienzos del año 2013, el gobierno de la Ciudad de Buenos Aires se encontraba analizando la posibilidad de implementar tecnología de reconocimiento facial en las cámaras de seguridad de la red de subtes con el fin de detectar posibles delincuentes. http://www.infobae.com/2013/01/13/691102-evaluan-un-software-identificacion-facial-ubicar-pungas-el-subte/

contrario pueden entrar en lo que entendemos como la esfera privada de la persona. En tal sentido falló el Tribunal Europeo de Derechos Humanos en el caso *Peck v. United Kingdom* (2003),[39] determinando que existe una zona de interacción de la persona con los demás, incluso en un contexto público, que puede entrar en el ámbito de la vida privada.

Por su parte, en el derecho anglosajón encontramos una evaluación al respecto de la razonable expectativa de privacidad,[40] originado en el caso *Katz v. United States* (1967), la Corte Suprema estadounidense determinó que la Cuarta Enmienda de la Constitución protege a las personas, no a las cosas, estableciendo a su vez dos parámetros de evaluación: por un lado, que una persona ha exhibido una expectativa real (subjetiva) de privacidad, y por el otro, que la expectativa es una que la sociedad está dispuesta a reconocer como "razonable".[41]

iii Argentina, ¿única en el mundo?

La adopción de sistemas de identificación de la población por parte de los Estados a lo largo del mundo no se ha presentado sin controversias. Las sociedades de Australia, Canadá, Nueva Zelanda, el Reino Unido, y Estados Unidos, se han opuesto satisfactoriamente a la implementación de un

[39] En el caso de Peck contra el Reino Unido, el demandante se quejó de la divulgación a los medios de comunicación del material grabado por el circuito cerrado de televisión (CCTV), que dio lugar a la publicación y difusión de imágenes que lo mostraban en un intento de suicidio. La autoridad local que operaba el sistema CCTV, el Brentwood Borough Council, había dado las imágenes a los medios de comunicación con el objetivo de promover la eficacia del sistema en la detección y prevención de delitos. La Comisión de Televisión Independiente (ITC) y la Comisión de Normas de Radiodifusión (BSC) consideraron que el enmascaramiento era inadecuado ya que vecinos, colegas, amigos y familiares que veían los programas reconocían al demandante. El Tribunal Europeo de Derechos Humanos determinó que la divulgación de las imágenes a los medios de comunicación resultó en una infracción del artículo 8 de la Convención Europea. La Corte hace hincapié en que el solicitante estaba en una calle pública pero que no estaba allí para participar en ningún evento público, ni era una figura pública, y que la divulgación de las imágenes no era necesaria en una sociedad democrática. Case of Peck v. United Kingdom, Tribunal Europeo de Derechos Humanos, enero 2003, http://merlin.obs.coe.int/iris/2003/6/article2.en.html Más información disponible en: "CCTV and Human Rights: the Fish and the Bicycle? An Examination of Peck V. United Kingdom (2003) 36 E.H.R.R. 41", Caoilfhionn Gallagher, Surveillance & Society, 2004, http://www.surveillance-and-society.org/articles2(2)/humanrights.pdf

[40] Al respecto de la "expectativa de privacidad": https://www.law.cornell.edu/wex/expectation_of_privacy

[41] En el caso Katz contra Estados Unidos, el demandante utilizó una cabina de teléfono público para transmitir apuestas ilegales, sin saber que el FBI estaba grabando la conversación mediante un dispositivo de interceptación ubicado en el exterior de la cabina de teléfono, lo cual llevó a su consecuente condena. Katz apeló su condena estableciendo que las grabaciones habían sido obtenidas en violación de la Cuarta Enmienda de la Constitución. El caso llegó hasta la Corte Suprema, la cual falló a favor de Katz entendiendo que una cabina telefónica en donde uno cierra la puerta es una zona en la que, al igual que su casa, una persona tiene una razonable expectativa de privacidad amparada por la Constitución; que las intrusiones electrónicas y físicas en un lugar que es privado pueden constituir una violación de la Cuarta Enmienda; y que la invasión por parte de autoridades federales de una zona protegida constitucionalmente es presuntamente excesiva en ausencia de una orden judicial. El caso Katz estableció que las interceptaciones telefónicas por parte de autoridades federales y estatales se encuentran sujetas a los requerimientos de orden judicial bajo la Cuarta Enmienda. Katz v. United States, Corte Suprema de Justicia de Estados Unidos, diciembre 1967, https://www.law.cornell.edu/supremecourt/text/389/347

documento de identificación para sus habitantes.[42] Mientras tanto, en la Argentina, el Documento Nacional de Identidad tiene un rol preponderante en la vida cívica de los argentinos. Concebido con el fin de "identificar, registrar y clasificar el potencial humano nacional", el DNI fue arraigándose con el paso de los años hasta lograr que los habitantes no conciban un ejercicio de sus quehaceres cívicos sin el mismo; esta es la puerta de entrada a la vinculación con el Estado y también entre los particulares.

En nuestra primera incursión analizando la evolución de las políticas biométricas en Argentina, destacamos el dudoso tinte democrático que inviste a las mismas. En términos de identificación masiva de personas, fue el decreto-ley 17.671 que estableció el Documento Nacional de Identidad, introducido durante el gobierno de facto del militar Juan Carlos Onganía, el que marcó un antes y un después en la sociedad argentina.

El rol incuestionable de la identificación de la población se arraigó en la Argentina gracias a que las políticas introducidas no se encaminan por la vía legislativa, sino como actualizaciones tecnológicas enmarcadas en la modernización del Estado, justificadas en base a un decreto-ley firmado durante una dictadura militar; esto no solamente sesgó completamente el rumbo adoptado en este tipo de políticas públicas, sino que priva a la ciudadanía de cualquier tipo de información y debate que sin dudas está en interés del público.

La identificación de personas a partir de datos biométricos se ha convertido en una tendencia en constante crecimiento a lo largo del mundo. Actualmente encontramos este tipo de tecnología adoptada en países como Australia, Brasil, Canadá, Gambia, Alemania, Irak, Israel, Italia, Noruega, Ucrania, Reino Unido, Estados Unidos, y Países Bajos, por nombrar algunos.

Según determinó el estudio de la universidad de *Georgetown*, la mitad de la población adulta estadounidense se encuentra registrada en bases de datos biométricas para reconocimiento facial.[43] Los departamentos de policía en distintos estados utilizan software de reconocimiento facial para comparar imágenes de vigilancia con bases de datos de fotos de identificación (e.g. licencia de conducir, pasaporte), no solamente para confirmar la identidad de un sospechoso detenido, sino también para determinar a través de cámaras de vigilancia los movimientos particulares de una persona.

El *Center on Privacy & Technology* determinó que los algoritmos utilizados para identificar a las personas son inexactos aproximadamente en un 15% de oportunidades y son más propensos a identificar erróneamente a los afroamericanos, a lo cual se suma que organismos como el FBI no realizan pruebas de sus sistemas por falsos positivos ni por sesgos raciales, ya que para el FBI el sistema "es ciego a la raza", lo cual ha preocupado al *CPT* debido a que el FBI no sabe con qué

[42] "Mandatory National IDs and Biometric Databases", Electronic Frontier Foundation, https://www.eff.org/issues/national-ids

[43] "Half of American Adults Are in Police Facial-Recognition Databases", Kaveh Waddell, octubre 19, 2016, https://www.theatlantic.com/technology/archive/2016/10/half-of-american-adults-are-in-police-facial-recognition-databases/504560/

frecuencia el sistema identifica incorrectamente al sujeto incorrecto. Por otra parte, según Alvaro Bedoya –director ejecutivo del *CPT*– no hay una ley federal o decisión judicial que ponga límite a esta tecnología.[44]

En el campo de la identificación de personas, uno de los casos más paradigmáticos es el de la India. El sistema de identificación único implementado en el año 2010, conocido como *Aadhaar*, es el más grande del mundo, con más de 1200 millones de usuarios registrados al mes de marzo de 2017.[45] Los residentes pueden obtener su número *Aadhaar* luego de brindar sus datos patronímicos y biométricos (huellas dactilares, fotografía, e iris).[46] Este sistema ha ido cobrando cada vez mayor preponderancia en el desarrollo de la vida en el país, haciéndose necesario para el registro de inmuebles, declaración de impuestos, abrir una cuenta bancaria, acceder a becas académicas, ingresar a colegios y universidades, acceder a subsidios estatales (e.g. comida, gas), la emisión del pasaporte y el registro de conducir, y adquirir una tarjeta SIM.

La obligatoriedad del *Aadhaar* ha causado controversias,[47] en donde la Corte Suprema determinó que éste no puede ser obligatorio para el acceso a beneficios sociales.[48] Por otra parte, expertos de la sociedad civil india han puesto en duda la seguridad del sistema, así como la necesidad de una reforma legal que contemple mayores garantías en el manejo de los datos biométricos recolectados.[49]

En resumen, respondiendo a la pregunta que inicia este capítulo, el caso de Argentina forma parte de la creciente tendencia mundial en la adopción de soluciones tecnológicas que aprovechan los datos biométricos de las personas para identificarlas y controlarlas. La adopción de un documento único no es algo necesario o inevitable, como hemos visto, países de grandes tradiciones democráticas no exigen un documento de identificación único, ya que se ha ponderado en los debates y en las peticiones de la ciudadanía el impacto en los derechos fundamentales que este tipo de políticas pueden ocasionar. Si tenemos en cuenta que las políticas de identificación de la población en la Argentina han surgido de la mano de gobiernos de facto, resulta claro que la lógica de este tipo de medidas responde a un afán de control por parte del Estado que no se condice con una tradición completamente democrática más allá de la naturalización de estas prácticas en la sociedad.

[44] "Facial recognition database used by FBI is out of control, House committee hears", Olivia Solon, marzo 27, 2017, https://www.theguardian.com/technology/2017/mar/27/us-facial-recognition-database-fbi-drivers-licenses-passports

[45] "State-wise Aadhaar Saturation", Unique Identification Authority of India. Consultado el 23 de marzo de 2017, disponible en: https://uidai.gov.in/enrolment-update/ecosystem-partners/state-wise-aadhaar-saturation.html

[46] "State of Privacy: India", Privacy International y Center for Internet and Society, marzo 2017, https://privacyinternational.org/node/975

[47] "10 things you need Aadhaar for": https://www.youtube.com/watch?v=578WwTwcNyk

[48] "Aadhaar cannot be made mandatory for welfare schemes: Supreme Court", Indian Express, marzo 27, 2017, http://indianexpress.com/article/india/cannot-make-aadhaar-mandatory-for-welfare-schemes-supreme-court-to-centre-4587325/

[49] "Aadhaar uses fingerprints, linked to bank accounts: Is your identity safe?",Pranesh Prakash, abril 2, 2017, http://www.hindustantimes.com/india-news/what-s-really-happening-when-you-swipe-your-aadhaar-card-to-make-a-payment/story-2fLTO5oNPhq1wyvZrwgNgJ.html

III El Sistema Federal de Identificación Biométrica para la Seguridad

El Sistema Federal de Identificación Biométrica para la Seguridad (SIBIOS) fue introducido en el año 2011, a través del decreto 1766, el cual se basa en una lógica de seguridad y prevención del delito. Antes de continuar sobre el contenido del decreto, es menester detenernos en el decreto *per se* como instrumento de introducción de políticas públicas, y como herramienta de limitación de derechos fundamentales, como es el derecho a la privacidad.

Partiendo de las bases constitucionales, el artículo 18 es el que consagra el principio de legalidad, por el cual el accionar del Estado debe enmarcarse en una ley debatida y promulgada por el Congreso de la Nación, en el afán de evitar caer en la arbitrariedad de la voluntad de los funcionarios del gobierno de turno.

Cuando de derechos humanos se trata, los tratados, pactos, y convenciones internacionales, establecen entre sus cláusulas bajo qué circunstancias puede limitarse el goce y ejercicio de los derechos allí consagrados. En tal sentido, la Declaración Universal de Derechos Humanos determina en el artículo 29, inciso 2º, que "En el ejercicio de sus derechos y en el disfrute de sus libertades, toda persona estará solamente sujeta a las limitaciones establecidas por la ley con el único fin de asegurar el reconocimiento y el respeto de los derechos y libertades de los demás, y de satisfacer las justas exigencias de la moral, del orden público y del bienestar general en una sociedad democrática"[50]; de igual manera, la Convención Americana de Derechos Humanos establece en el artículo 30 que "Las restricciones permitidas, de acuerdo con esta Convención, al goce y ejercicio de los derechos y libertades reconocidas en la misma, no pueden ser aplicadas sino conforme a leyes que se dictaren por razones de interés general y con el propósito para el cual han sido establecidas".[51]

En el año 1999, a través del Comentario General Nº 27,[52] el Comité de Derechos Humanos –organismo encargado de la supervisión y aplicación del Pacto Internacional de los Derechos Civiles y Políticos (PIDCP)– fijó su posición respecto a los parámetros que deben ser considerados al momento de imponer limitaciones a los derechos consagrados en el PIDCP, fijando un marco sobre el cual se pueden analizar las políticas públicas que pretendan avanzar sobre derechos fundamentales.

Al establecerse este sistema biométrico mediante decreto, se evita la reflexión y merecido debate que el uso de datos biométricos debiera tener en el Congreso. A modo de ejemplo, los datos biométricos son una especie de dato sensible dentro del género de los datos personales, y el reconocimiento de este tipo particular de datos como "dato sensible" todavía se encuentra pendiente. La relación directa entre esta falta de análisis y su reconocimiento legal, sumado a la afectación que este tipo de información ocasiona en derechos fundamentales (privacidad y autodeterminación informativa, en

[50] http://www.un.org/es/universal-declaration-human-rights/

[51] https://www.oas.org/dil/esp/tratados_b-32_convencion_americana_sobre_derechos_humanos.htm

[52] http://hrlibrary.umn.edu/gencomm/hrcom27.htm

ese caso), pondría a este sistema (SIBIOS) en falta con el principio de legalidad, establecido tanto por la Constitución como por tratados internacionales.

Según surge del artículo 3º del Decreto 1766/11, la autoridad de aplicación del Sistema es el Ministerio de Seguridad de la Nación, mientras que el responsable de la administración y mantenimiento del mismo es la Policía Federal Argentina, mediante la Superintendencia de Policía Científica.

El artículo 5º del Decreto 1766 establece la creación de una Unidad de Coordinación dentro del Ministerio de Seguridad, la cual debe estar 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 Policía Federal Argentina, Gendarmería, Prefectura Naval y Policía de Seguridad Aeroportuaria. En relación con lo mencionado anteriormente, en consideración de la naturaleza de los datos biométricos como una especie de dato sensible, es menester destacar la ausencia de la Dirección Nacional de Protección de Datos Personales (DNPDP) como especialistas asesores del Ministerio de Seguridad.

Ante la consulta en nuestro pedido de informes por las actividades llevadas a cabo por la Unidad de Coordinación, sus tareas y acciones (reuniones, capacitaciones, decisiones tomadas, etcétera), el Ministerio de Seguridad determinó que a septiembre de 2016, casi cinco años después de firmado el Decreto que crea SIBIOS, la misma no ha sido conformada, a la vez que establece que en la práctica, quien lleva a cabo tal coordinación es la Dirección Nacional de Policía Científica, dependiente de la Subsecretaría de Investigación del Delito Organizado y Complejo, de la Secretaría de Seguridad del Ministerio de Seguridad de la Nación.

A comienzos de abril de 2017, el Poder Ejecutivo firmó el decreto 243, que introduce modificaciones al articulado del decreto 1766.[53] En el artículo 2 del decreto 243 se establece que la Unidad de Coordinación y Seguimiento será llevada a cabo por la Dirección Nacional de Policía Científica mencionada anteriormente, dando cuenta en los considerandos del decreto que la Unidad no había sido creada como lo dictaba el decreto 1766. Los especialistas que asesoran a la Unidad no fueron modificados, respecto a lo cual reiteramos la ausencia de la DNPDP.

De acuerdo a la respuesta recibida por parte del Ministerio de Seguridad al pedido de informes realizado por ADC, la base de datos de SIBIOS se compone de dos tipos de datos: Biométricos y patronímicos (es decir, el nombre y apellido con el cual se identifica a una persona).

El Ministerio de Seguridad establece que los datos biométricos almacenados por SIBIOS son: huellas dactilares, huellas palmares y registros de rostros (reconocimiento facial). A continuación, presentamos tres gráficos elaborados por ADC a partir de la información brindada por el Ministerio en relación a la cantidad de datos totales almacenados en SIBIOS de acuerdo a cada tipo de dato.

[53] Decreto 243/2017, Boletín Oficial, https://www.boletinoficial.gob.ar/#!DetalleNorma/161771/20170410

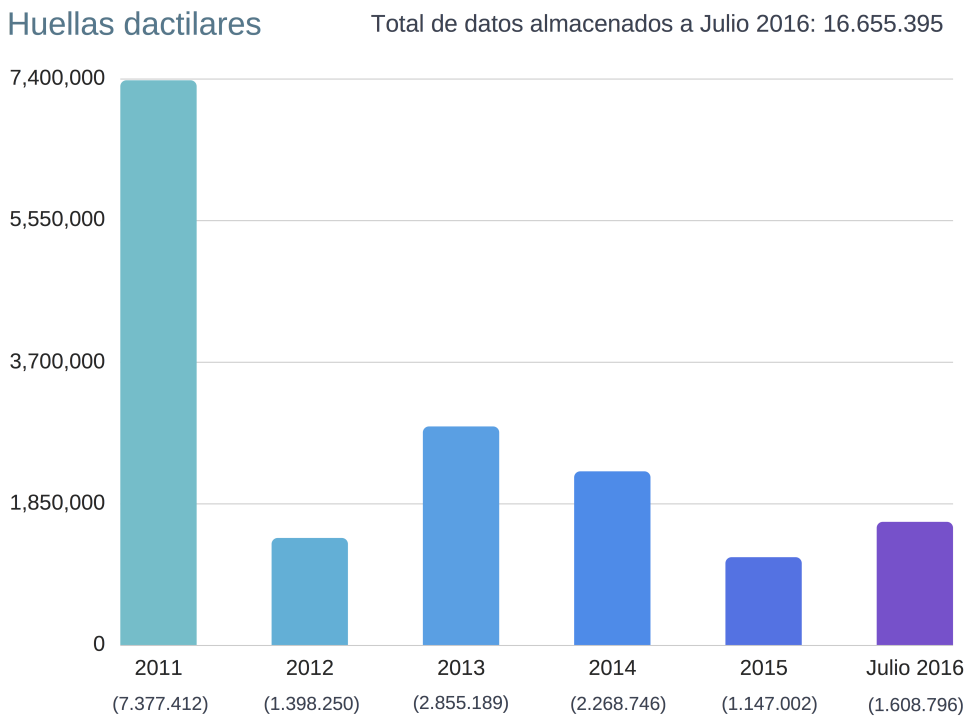

Gráfico 1 de elaboración propia, septiembre 2016.

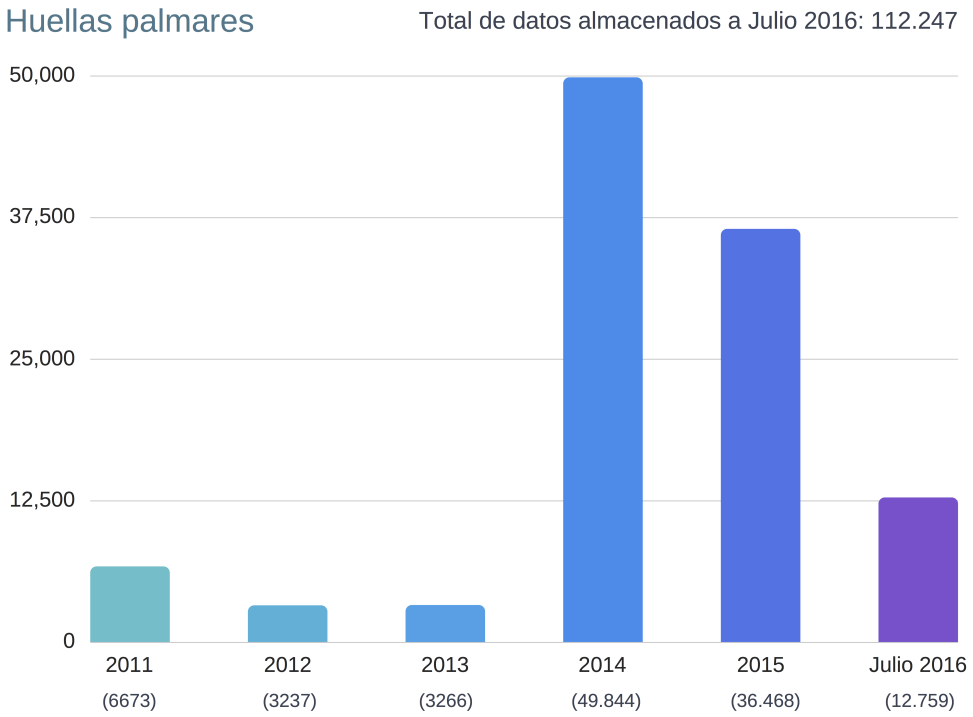

Gráfico 2 de elaboración propia, septiembre 2016.

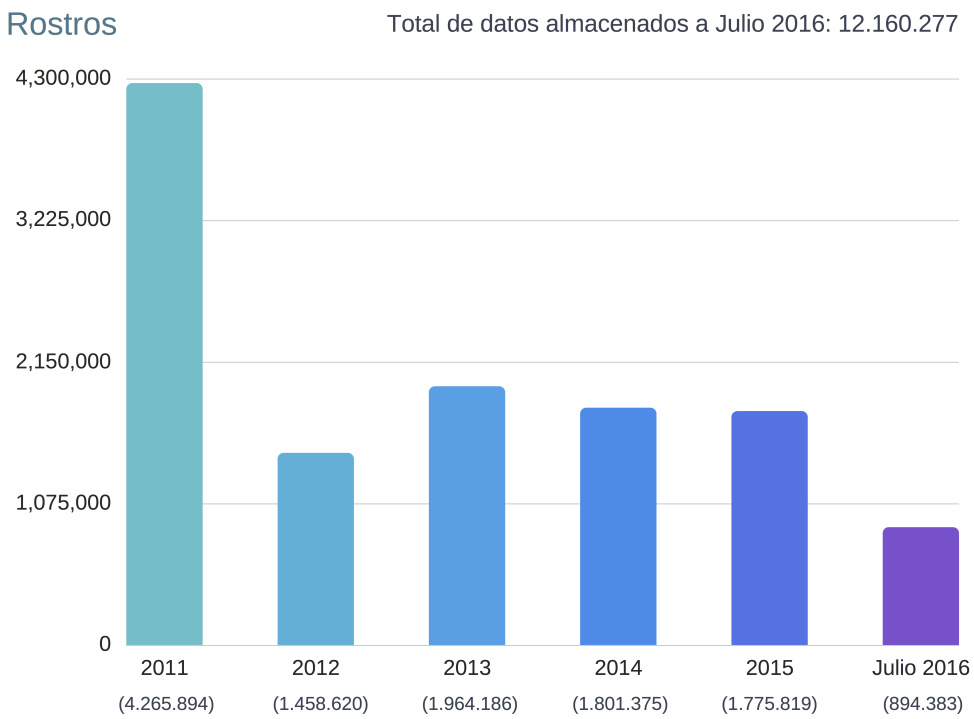

Gráfico 3 de elaboración propia, septiembre 2016.

El decreto parece tratar de justificar la implementación de tecnología biométrica en dos párrafos puntuales, destacando "la relevancia de la identificación biométrica a los efectos de comprobar la identidad de una persona, mediante el uso de un sistema informático de comparación y análisis fisionómico de una persona respecto de una base de datos preparada para tal fin", y que por lo tanto "resulta imprescindible usufructuar al máximo las herramientas tecnológicas en dotación, teniendo en cuenta que la utilización de técnicas biométricas resulta un aporte fundamental a las funciones de seguridad pública en materia preventiva y respecto de competencias de investigación y policía científica (. . .)".

Es por esto, y por lo expuesto anteriormente, que el decreto que sustenta la implementación de SIBIOS no aparece como compatible con el test de limitaciones admisibles establecido por los pactos internacionales, ya que falla en determinar la suficiente necesidad del Sistema, no solamente para una sociedad democrática, sino, aún más gravemente, para alcanzar el objetivo que se plantea.

Teniendo en cuenta que la biometría no es una tecnología infalible, como vimos en el capítulo sobre las distintas vulnerabilidades que pueden afectar a los sistemas de identificación biométrica, y que el decreto de SIBIOS no hace menciones concretas sobre las necesidades en las cuales se basa su implementación, mencionando tan solo vagamente la "protección esencial del derecho a la seguridad", pero evitando desarrollar sobre amenazas concretas, ni incluyendo un análisis fáctico, cualitativo y cuantitativo de ventajas/desventajas de su implementación en relación con el sistema

anterior, el decreto parece basar toda su lógica en la facilidad y agilidad de la identificación de personas a través de la tecnología biométrica, no porque sea la mejor solución para la necesidad concreta de seguridad, sino porque está disponible. Al evitar el debate legislativo, se pierde toda dimensión de las garantías que deben ponerse en lugar para resguardar el ejercicio de derechos humanos.

i ¿Cómo son incorporados los datos a SIBIOS?

Para poder funcionar como una base de datos centralizada, uno de los puntos elementales de SIBIOS es poder nuclear información de distintas dependencias estatales y fuerzas de seguridad, las cuales en mayor o menor medida mantenían bases de datos propias. Con la llegada de SIBIOS esto significó que todas esas bases independientes sean digitalizadas (en caso de no estarlo) y cargadas en el Sistema.

Debido a que las bases existentes con anterioridad al Decreto 1766/11 se encontraban incompletas, y con el fin de poder tener los registros de los más de 40 millones de habitantes del país, el principal punto de partida para alimentar la base de datos de SIBIOS es el Registro Nacional de las Personas (RENAPER) del Ministerio del Interior, Obras Públicas y Vivienda de la Nación, el cual desde el año 2009 cuenta con la facultad de "utilizar tecnologías digitales en la identificación de ciudadanos nacionales y extranjeros".[54]

El RENAPER es el encargado de remitir la información biométrica y patronímica recolectada a través de la realización del Documento Nacional de Identidad (DNI) y del Pasaporte Nacional. En el año 2012 fueron lanzados tanto el DNI digital[55] como el pasaporte electrónico, el cual almacena en un chip *RFID*[56] los datos de su titular y su información biométrica con el fin de poder identificar a su titular a través de su huella dactilar, su iris y/o su rostro.[57]

Por otra parte, debido a que SIBIOS pretende ser una base de datos federal, se determinó un esquema por el cual cada provincia pueda hacer uso del Sistema y aportar sus propios registros. Así, los Estados Provinciales pueden firmar el Acta de Adhesión con el Estado Nacional, a partir del cual la Superintendencia de Policía Científica de la PFA procede a cargar las fichas decadactilares (correspondientes a los 10 dedos de las manos), rostros, huellas palmares y datos patronímicos que haya aportado cada Policía provincial en cuestión. Luego, para mantener el Sistema actualizado, la Provincia puede realizar la incorporación de registros pertinentes directamente.

[54] Decreto 1501/2009, http://servicios.infoleg.gob.ar/infolegInternet/anexos/155000-159999/159070/norma.htm

[55] Resolución 585/2012, Registro Nacional de las Personas, http://servicios.infoleg.gob.ar/infolegInternet/anexos/195000-199999/195199/norma.htm

[56] Radio Frequency IDentification, o identificación por radiofrecuencia. https://es.wikipedia.org/wiki/RFID

[57] Resolución 1474/2012, Dirección Nacional del Registro Nacional de las Personas, http://servicios.infoleg.gob.ar/infolegInternet/anexos/195000-199999/198662/texact.htm

En el pedido de informes presentado ante el Ministerio de Seguridad, buscamos determinar cuáles son las medidas y garantías de seguridad con las que cuenta la infraestructura bajo la cual funciona SIBIOS y la base de datos que alimenta al sistema. Sobre lo cual el Ministerio respondió que "la Sección Sistema Electrónicos de Registros e Identificación de la Policía Federal Argentina, realiza un riguroso registro de los accesos '*logueos*' de aquellos usuarios autorizados para ingresar al Sistema (. . .), mediante la realización de auditorías periódicas".

Por otra parte, agregó que "los distintos Organismos que hagan uso del Sistema (. . .), están sujetos a las medidas de seguridad, requisitos de autenticidad, integridad, confidencialidad y deber de reserva de la información obtenida, disponibilidad y estándares técnicos compatibles, en comunión con los lineamientos previstos por el Artículo No 23 y concordantes de la Ley 25.326 de Protección de Datos Personales"; evitando mencionar cuáles los detalles técnicos para la seguridad de los servidores y del sistema que da vida a SIBIOS, tal como solicitó la ADC en su pedido de informes.

Ante la pregunta de ADC si han existido casos de extracción no autorizada de información de SIBIOS, el Ministerio de Seguridad determinó que "No existen registros de informes que se hayan comunicado a este Ministerio de Seguridad de la Nación ni a la Policía Federal Argentina".

ii ¿Qué organismos forman parte de SIBIOS?

De acuerdo al artículo tercero del Decreto 1766, los principales usuarios del Sistema son: Policía Federal Argentina, Gendarmería Nacional, Prefectura Naval, Policía de Seguridad Aeroportuaria, Registro Nacional de las Personas y Dirección Nacional de Migraciones. A estos se suman a su vez las policías de las provincias que hayan suscrito el Acta de Adhesión.

El decreto 243/2017, firmado a comienzos de abril, establece en su primer artículo la ampliación de la invitación para adherirse a SIBIOS, modificando el artículo cuarto del decreto 1766 para incluir a "(. . .) todos aquellos organismos dependientes del Poder Ejecutivo o del Poder Judicial tanto Nacionales, como Provinciales y de la Ciudad Autónoma de Buenos Aires (. . .)" para que puedan formular consultas biométricas en tiempo real.

En nuestro informe anterior se determinó que la cantidad de provincias adheridas a SIBIOS en septiembre de 2014 eran 11, de 23 provincias totales y una ciudad autónoma, a saber: Chaco, Mendoza, San Juan, Tucumán, Catamarca, Santiago del Estero, Santa Fe, Santa Cruz, Entre Ríos, Salta, y La Rioja. En el reciente informe brindado por el Ministerio de Seguridad se establece que —a septiembre de 2016— como se puede observar en el gráfico 4, casi la totalidad de las provincias ya se encuentran adheridas a SIBIOS, con excepción de Córdoba y Formosa; aunque algunas inconsistencias en la respuesta obtenida por parte del Ministerio de Seguridad, sugiere que SIBIOS se encuentra implementado en todo el territorio nacional, lo cual buscaremos esclarecer mediante un próximo pedido de informes.

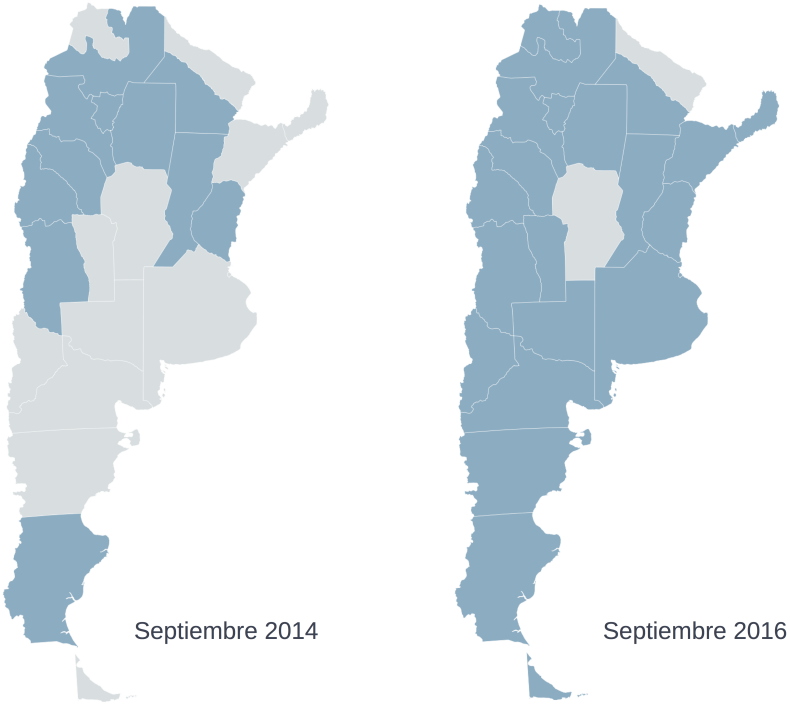

Gráfico 4 de elaboración propia, septiembre 2016.

Cada usuario de SIBIOS tiene instalado en sus oficinas una computadora que está configurada para poder ingresar al Sistema y acceder a los servidores, donde se encuentra la base de datos, a través de una Red Privada Virtual.[58] El único requisito, además de estar autorizado, tanto el organismo que figurará como usuario de SIBIOS como la persona encargada de su uso en la dependencia, por el Ministerio de Seguridad, es haber realizado el Curso de Operador del Sistema, capacitación que es brindada también por dicho Ministerio.

De acuerdo al Ministerio de Seguridad, los motivos por los cuales se puede ingresar al Sistema son:

- Consulta de datos
- Carga de rastros (Huellas dactilares, huellas palmares, rostros)
- Almacenamiento de impresiones de huellas dactilares totales o parciales
- Almacenamiento de impresiones palmares totales o parciales

[58] Una Red Privada Virtual, o VPN por sus siglas en inglés, "es una red privada que utiliza una red pública (por lo general Internet) para conectar sitios remotos o usuarios. En vez de utilizar una conexión exclusiva del mundo real como una línea alquilada, una VPN utiliza conexiones 'virtuales' enrutadas a través de Internet desde la red privada de la empresa hasta el sitio remoto o el empleado". http://www.cisco.com/cisco/web/support/LA/7/74/74718_how_vpn_works.pdf

- Almacenamiento de rostros
- Realización de cotejos
- Carga de datos biométricos
- Carga de datos patronímicos

iii La tecnología detrás de SIBIOS

Debido a que SIBIOS es una base de datos utilizada para la identificación de personas a través de su información biológica, además del dato propiamente dicho (la huella, el rostro, el iris), la otra parte fundamental es la tecnología utilizada para el procesamiento de toda esa información y para efectivamente llevar a cabo el uso del Sistema en las distintas dependencias estatales; la biometría, después de todo, es la tecnología y procesos por los cuales podemos *leer* al cuerpo humano.

De acuerdo a las respuestas obtenidas por ADC frente a los pedidos de informe presentados ante el Ministerios de Seguridad y el Ministerio del Interior, pudimos verificar quiénes son los desarrolladores de la tecnología sobre la cual está sustentado SIBIOS, en tal sentido desarrollamos la información de cada ministerio por separado, pues cada uno de ellos cuenta con un distribuidor distinto de la tecnología que utilizan.

i Ministerio de Seguridad

Hasta el año 2012, el sitio *"biometria.gov.ar"*[59] aclaraba en su pie de página que contaban con el apoyo de organismos, principalmente estadounidenses, como el *National Institute of Standards and Technology*, *FBI Biometrics Center of Intelligence* y *"biometrics.gov"* (página de información sobre actividades vinculadas con biometría del gobierno de Estados Unidos), además de *INTERPOL*.

Al poner en evidencia esta situación, y consultar específicamente quiénes o qué organismos y/o empresas colaboraron en el desarrollo e implementación de SIBIOS, el Ministerio de Seguridad determinó que la empresa interviniente es "Morpho Safran", quien llevó a cabo la instalación y configuración del equipamiento para el Sistema Automático de Identificación de Huellas Dactilares (o AFIS por sus siglas en inglés), sin brindar mayores precisiones.

SAGEM era una empresa francesa fundada en 1924 dedicada al desarrollo de tecnología militar para defensa, tecnología de consumo y sistemas de comunicaciones. En el año 2005 se fusionó con

[59] Para consultar una versión del sitio web del 1/10/2012: https://web-beta.archive.org/web/20121001201359/http://www.biometria.gov.ar

Snecma (*Safran Aircraft Engines*),[60] también de origen francés, para crear *Safran Group*[61], una compañía enfocada en motores para aviación y cohetes, componentes aeroespaciales, y tecnología para defensa y seguridad.

Conocida anteriormente como *Sagem Sécurité* en 2007, luego renombrada *Morpho* en 2010, actualmente denominada *Safran Identity and Security*, es la división del grupo Safran encargada del desarrollo de tecnologías de biometría, con más de 8400 empleados en más de 40 países alrededor del mundo y ganancias estimadas en mil millones y medio de euros.[62]

El desarrollo de productos varía desde soluciones para la identificación de personas,[63] como registros de votantes y ciudadanos, Identificación Nacional, documentos de viaje (pasaportes), registro de conductores, beneficios sociales y de salud; para la seguridad pública,[64] como herramientas para investigación (identificación biométrica de sospechosos, ADN, análisis de videos), controles migratorios, detección de explosivos y narcóticos; y para el ámbito comercial,[65] enfocados en tecnología para empresas de telecomunicaciones y entidades financieras.

Safran es el principal distribuidor para el *FBI*,[66] *INTERPOL*[67] y la policía de Nueva York (NYPD)[68], además de la Administración de Seguridad del Transporte (TSA, por sus siglas en inglés) del Departamento de Seguridad Nacional de Estados Unidos, el Ministerio del Interior de los Emiratos Árabes Unidos, la policía y el Ministerio del Interior francés, entre otros. Recientemente la empresa ha anunciado un contrato de cinco años con el Instituto Nacional Electoral en México para implementar sus sistemas de identificación multi-biométricos.[69]

[60] https://en.wikipedia.org/wiki/Snecma

[61] Sitio web oficial: http://www.safran-electronics-defense.com

[62] Sitio web oficial de Morpho, información de agosto 2014: https://web-beta.archive.org/web/20150526044815/http://www.morpho.com/qui-sommes-nous

[63] http://www.morpho.com/en/government-id-solutions-facilitate-and-secure-identity-management

[64] http://www.morpho.com/en/mobile-and-automated-systems-improve-public-security

[65] http://www.morpho.com/en/ensuring-trusted-authentication-and-transactions-online

[66] "Morpho Trak Technology Goes Operational for the FBI", comunicado de prensa de Morpho, 2011, http://www.morpho.com/en/media/morphotrak-technology-goes-operational-fbi-20110418 (también disponible en: http://web.archive.org/web/20150607084516/http://www.morpho.com/actualites-et-evenements/presse/morphotrak-technology-goes-operational-for-the-fbi?lang=en)

[67] "Sagem Sécurité to provide Interpol and its 186 member states with latest AFIS, Automated Fingerprint Identification System", comunicado de prensa de Morpho, 2008: http://www.morpho.com/en/media/sagem-securite-provide-interpol-and-its-186-member-states-latest-afis-automated-fingerprint-identification-system-20080204 (también disponible en: http://web.archive.org/web/20150607090048/http://www.morpho.com/news-events-348/press/sagem-securite-to-provide-interpol-and-its-186-member-states-with-latest-afis-automated-fingerprint-identification-system?lang=en) "Safran Identity & Security is the exclusive partner of INTERPOL for facial recognition", comunicado de prensa, 2016: http://www.morpho.com/en/media/safran-identity-security-exclusive-partner-interpol-facial-recognition-20161123

[68] "Morpho Trak Deploys Morpho Biometric Identification System at NYPD", comunicado de prensa de Morpho, 2012: http://www.morpho.com/en/media/morphotrak-deploys-morpho-biometric-identification-system-nypd-20120919 (también disponible en: http://web.archive.org/web/20150607084015/http://www.morpho.com/news-events-348/press/morphotrak-deploys-morpho-biometric-identification-system-at-nypd?lang=en)

[69] "Safran Identity & Security to modernize Mexico's multi-biometric identification system", comunicado de prensa

Si bien el Ministerio de Seguridad no brindó mayores precisiones sobre el tipo y las características del producto o productos específicos adquiridos a *Safran*, información del año 2013 de una fuente cercana a la PFA nos permitió conocer mayores detalles sobre la tecnología utilizada por esta fuerza de seguridad, que es una de las principales usuarias de SIBIOS.

Además del sistema AFIS para la identificación de huellas dactilares, la PFA lleva a cabo identificación facial utilizando tecnología de Safran, específicamente el producto "Morpho Face Investigate Pilot" (MFIP).

Gracias a los documentos publicados por WikiLeaks, conocidos como *The Spy Files*,[70] una serie de documentos que lanzaron entre 2011 y 2014 con el fin de exponer a la industria global de la vigilancia masiva, pudimos acceder a un PDF de *Safran* dedicado al producto mencionado en la presentación de la PFA, titulado "An Introduction to Morpho Face Investigate Pilot".[71]

De acuerdo a este documento, las principales características de *MFIP* son:

- "Cargar y administrar una base de datos de hasta 350.000 retratos, con una opción para una extensión de 2.000.000 de retratos;
- Buscar una o más imágenes en la base de datos de retratos utilizando la tecnología de reconocimiento facial Morpho;
- Adquirir imágenes de rostros desde archivos, o utilizando una cámara o un escáner;
- Extraer las imágenes faciales desde archivos de vídeo y buscarlas en la base de datos;
- Extraer rostros de imágenes que muestren a varias personas;
- Comprobar el resultado de las búsquedas de reconocimiento facial e informar sobre la decisión tomada;
- Administrar subconjuntos de la base de datos de retratos -llamadas listas de vigilancia- para habilitar la restricción de alcances de búsqueda."[72]

A su vez, también aclara que *MFIP* "puede ser implementado y utilizado con mínimo esfuerzo, incluso para usuarios sin conocimiento, o conocimiento limitado, sobre reconocimiento facial".[73]

---

de SafranIdentity and Security, 2016: http://www.morpho.com/en/media/safran-identity-security-modernize-mexicos-multi-biometric-identification-system-20161221

[70] https://wikileaks.org/spyfiles/

[71] "An Introduction to Morpho Face Investigate Pilot", 2011: https://wikileaks.org/spyfiles/document/safran/SAFRAN-2011-AnIntrto-en/ También disponible en: https://sii.transparencytoolkit.org/docs/Morpho_MorphoFace_Product-Descriptionsii_documents

[72] Ibíd, p.2

[73] Ibíd, p.2

El proceso para el reconocimiento facial de *MFIP* funciona de la siguiente manera:[74] todo comienza con la adquisición de la imagen del rostro (sea por una cámara de video "en vivo" o mediante el archivo de una foto JPG, por ejemplo), para luego proceder a determinar dónde se encuentra ubicado el rostro dentro de la imagen y señalar el centro de los ojos, a partir de la cual se extrae una plantilla o modelo, esta es una representación de la imagen que es adecuada para ser comparada (la plantilla puede representar tanto rasgos físicos visibles, como la ubicación de la nariz y las cejas, o pura información matemática). A medida que se analizan las imágenes se realiza un control de calidad, en el cual se determina si una imagen es de baja o alta calidad, en el caso de ser de baja calidad un operador puede confirmar la ubicación de los rasgos faciales para asegurar la exactitud del sistema.

Una vez finalizado el proceso para la carga de las imágenes a la base de datos que alimenta a *MFIP*, se puede realizar la comparativa de rostros. Cada comparativa devuelve un valor, cuanto más alto sea este, mayor probabilidad de que el rostro comparado sea similar.

ii Ministerio del Interior

"Queremos agradecer especialmente a la República de Cuba la colaboración para desarrollar este sistema, este software de muy bajo costo, que se integra al AFIS y entonces va a permitir en tiempo real conocer y saber quién es la persona que está frente a un personal de seguridad o en cualquier otro lado si es esa persona, y si no es esa persona, quién es en realidad".[75] De esta manera presentaba la ex Presidente de Argentina, Cristina Fernández de Kirchner, a SIBIOS durante el primer discurso en el cual se lo introdujo a la sociedad en el año 2011.

Consecuentemente, el periódico Página12 volvió a confirmar con el Ministerio del Interior el rol que había desempeñado Cuba en el desarrollo de la tecnología detrás del Sistema, determinando que "el apoyo cubano resultó de importancia porque en la región latinoamericana es Cuba el único país que aplica la identificación biométrica de los ciudadanos".[76]

En octubre de 2015, el Ministerio del Interior comunicó nuevamente que se encontraban trabajando con Cuba para continuar implementando tecnología biométrica. De acuerdo al ex Ministro del Interior, Florencio Randazzo, "con este convenio se dará inicio a una nueva etapa de implementación de tecnología biométrica en nuestro país, ya que podremos identificar a una persona contrastando una imagen nítida contra toda la base [de datos] del ReNaPer obteniendo su identidad únicamente desde una fotografía", y agregó, "En el caso de la fotografía, hasta hoy la herramienta de verificación

[74] Ibíd, p.3-4

[75] "Creación Sistema Federal de Identificación Biométrica (SIBIOS)", 7 de noviembre de 2011, Cristina Fernández de Kirchner, a partir del minuto 2:27: https://www.youtube.com/watch?v=GcKrHKqBzwo

[76] "Ya nunca más habrá que tocar el pianito", Página12, 8 de noviembre de 2011: https://www.pagina12.com.ar/diario/sociedad/3-180795-2011-11-08.html

era comparando una imagen contra otra que pertenezca a algún individuo concreto, (...) ahora también podremos identificar a una persona sin otro dato más que su imagen, ya que podremos contrastar una fotografía contra toda la base de datos de ReNaPer".[77]

Gracias a estos datos, en el pedido de informes remitido al Ministerio del Interior para el presente informe solicitamos explícitamente que determine en qué consistió la colaboración con el gobierno de Cuba, la empresa o entidad que intervino en el desarrollo de la tecnología, y los términos del acuerdo.

La empresa cubana en cuestión es DATYS, fundada en el año 2005, con sede en La Habana y presencia en las provincias de Matanzas, Villa Clara, Holguín y Santiago de Cuba, la cual cuenta con más de 700 empleados, de acuerdo a su sitio web.[78]

DATYS clasifica sus productos en cinco categorías correspondientes a biometría, identidad, seguridad, gestión y minería de datos.

En la respuesta a nuestro pedido de informes, el Ministerio del Interior no especificó cuál es el software en concreto, la Dirección de Tecnología del RENAPER se limitó en establecer que "La herramienta transferida por el gobierno de Cuba permite trabajar con imágenes de rostro. La utilización de esta herramienta está referida a reforzar el sistema automático de identificación. El método principal de identificación automática utilizando el sistema AFIS es mediante la comparación de huellas. Como método secundario se utiliza la comparación de rostros de una misma persona."[79]

Según el sitio oficial de DATYS, los productos en el área de biometría son tres: BIOMESYS, una plataforma de identificación multibiométrica; PMAIC, Plataforma Multibiométrica de Investigación Criminal; y BIOMESYS framework Bioapi, el marco o estructura para el despliegue biométrico.

Las principales características de BIOMESYS son:

- "Enrolamiento de las personas a través de la captura de datos biográficos y biométricos, en particular las impresiones dactilares, rostro y la firma.
- Identificar personas incluidas en el sistema.
- Entre los servicios de identificación y verificación biométrica están:
  - Impresiones Dactilares vs Impresiones Dactilares.
  - Huellas Latentes Dactilares vs Impresiones Dactilares.

[77] "Randazzo anunció que 'Argentina incorporará tecnología biométrica que permitirá ayudar a la Justicia a identificar identidades desde imágenes'", 13 de octubre de 2015, Ministerio del Interior: http://www.mininterior.gov.ar/prensa/prensa.php?i=4594

[78] Sitio web oficial: http://datys.cu/, una versión archivada del sitio al 24/11/2016 puede accederse en: https://web-beta.archive.org/web/20161124082804/http://datys.cu/spa/site/index

[79] Respuesta del Ministerio del Interior al pedido de informes presentado en julio 2016, en archivo en la ADC

- Huellas Latentes Dactilares vs Huellas Latentes Dactilares de Casos no resueltos.
- Impresiones Palmares vs Impresiones Palmares.
- Huellas Latentes Palmares vs Impresiones Palmares.
- Huellas Latentes Palmares vs Huellas Latentes Palmares de Casos no resueltos.
- Rostro vs Rostro.
- Rostros Editados vs Rostro, Retrato Hablado vs Rostro.
- Voz vs Voz, ADN vs ADN.

◆ El intercambio de información con otros sistemas."[80]

Como parte de la respuesta al pedido de informes, el Ministerio del Interior brindó también información sobre el acuerdo mencionado anteriormente, firmado el mes de octubre de 2015, específicamente las adendas número 6 y 7 al Acuerdo de Cooperación Internacional original, suscrito el 17 de junio de 2011.

Estas adendas establecen la actualización del sistema biométrico provisto por DATYS que utiliza el Ministerio del Interior y sus distintas dependencias. En la adenda 6 se establece que la actualización de la plataforma biométrica licenciada al gobierno cubano consiste en "(...) la incorporación de nuevos servicios web bajo estándar BIAS[81] que permitan realizar identificaciones de rostro 1:N y de mejoras a las herramientas de verificación y control de calidad para la identificación a partir del reconocimiento facial 1:1 (...)".

En biometría, un sistema "1:N" es utilizado para la identificación, en donde "N" es generalmente la totalidad de los registros almacenados en una base de datos, por lo que se busca responder "¿Quién es esa persona?"; por otra parte, un sistema "1:1" es utilizado para verificación, buscando responder "¿Es esa la persona que dice ser quién es?".

Por su parte, la adenda 7 versa sobre la contratación de los servicios de soporte técnico y mantenimiento de las herramientas para la identificación biométrica, además de la capacitación de personal técnico del Ministerio del Interior para el diagnóstico y resolución de problemas.

La actualización del sistema biométrico, de acuerdo a la adenda 6, tuvo un costo total de un millón ochenta mil dólares estadounidenses (U$D 1.080.000), mientras que el soporte técnico contratado en la adenda 7 lleva un costo de ciento ochenta mil dólares estadounidenses (U$D 180.000) por año de vigencia de la adenda, la cual fue suscrita por un término de cinco años contados a partir del 2016, pero con la posibilidad de revisar los términos y condiciones del contrato al finalizar cada año.

[80] Sitio web oficial, DATYS, archivo del 28 de noviembre de 2016: https://web-beta.archive.org/web/20160428071558/http://www.datys.cu/spa/site/product/5

[81] Por las siglas en inglés de "Biometric Identity Assurance Services (BIAS)", o Servicios de Aseguramiento de Identidad Biométrica.

iv SIBIOS en la práctica

Recapitulando lo mencionando hasta el momento, vimos que el recorrido de la información que alimenta a SIBIOS comienza, por una parte, con la emisión del Documento Nacional de Identidad digital y del nuevo Pasaporte biométrico, en manos del RENAPER, y por otra parte, con la previa carga de registros por parte de las fuerzas de seguridad nacionales y provinciales adheridas. Una vez almacenada esta información en la base de datos, puede ser utilizada por los distintos usuarios avalados por la normativa y los convenios suscritos con las provincias.

De esta forma, la Dirección Nacional de Migraciones utiliza SIBIOS para controlar los puntos migratorios de egreso e ingreso a la Argentina, tanto ciudadanos argentinos como extranjeros son ingresados a la base de datos de SIBIOS en su paso por los aeropuertos internacionales del país y la terminal portuaria de Buquebus.

Si bien la información pública disponible en relación al uso que realizan de SIBIOS las fuerzas de seguridad –PFA, PSA, Prefectura, y Gendarmería– es prácticamente nula, información del año 2013 de una fuente cercana a la Policía Federal nos permitió conocer algunos casos en los cuales se hizo uso del mismo; aparentemente, uno de los usos que le da la PFA a SIBIOS es en el caso de catástrofes con el fin de identificar a las víctimas, como el caso de las inundaciones en la ciudad de La Plata,[82] y los accidentes ferroviarios de la línea Sarmiento en Castelar[83] y Once.[84] Para la identificación de las víctimas, la PFA utilizaría un dispositivo del grupo Safran, modelo "*Morpho RapID*", un equipo inalámbrico de captura e identificación de huellas dactilares.[85]

Por la forma en la cual está actualmente estructurado SIBIOS, y por cómo fue en sí concebido el sistema, las fuerzas de seguridad no requieren de orden judicial alguna (es decir, que un juez en el marco de un proceso penal abierto, autorice con su firma una orden para llevar a cabo la tarea) para utilizar la base de datos e identificar a las personas allí registradas. Esto pone en duda la conformidad del Sistema con los principios legales que aseguran el debido proceso, y particularmente la presunción de inocencia.

Es que permitir el acceso irrestricto para que las policías federales y provinciales (y recientemente cualquier organismo dependiente del Poder Ejecutivo y/o Judicial) accedan a la identificación biométrica de todas las personas que habitan o transitan el país, parece responder a una lógica

[82] "Ya son al menos 48 los muertos por el temporal en La Plata", La Nación, 4 de abril de 2013, http://www.lanacion.com.ar/1569096-inundacion-en-la-plata "Confirmaron 89 muertos por la inundación del 2 de abril de 2013 en La Plata", Télam, 4 de julio de 2014, http://www.telam.com.ar/notas/201407/69935-la-plata-justicia-89-muertos-inundacion.html

[83] "El Gobierno confirmó que hay tres muertos y 315 heridos por el choque de trenes del Sarmiento", Clarín, 13 de junio de 2013, http://www.clarin.com/ciudades/chocaron-trenes-sarmiento-castelar_0_HkvPcVDsvXg.html

[84] "Choque de un tren en Once: hay 50 muertos y 676 heridos", Clarín, 22 de febrero de 2012, http://www.clarin.com/sociedad/descarrilo-tren-sarmiento-llegaba-once_0_Syp-jfDhwmx.html

[85] Más información sobre las terminales móviles de la empresa Safran disponible en su sitio web: http://www.morpho.com/en/biometric-terminals/mobile-terminals

bajo la cual todos los ciudadanos registrados en la base de datos de SIBIOS pasan a ser sospechosos hasta que se pruebe lo contrario. Esta situación es un ejemplo claro de la forma en la que la tecnología ha reconfigurado la investigación penal y por lo tanto debe ser abordada con sumo cuidado a fin de evitar posibles abusos a los derechos.

Otra de las inquietudes que surgen del uso de SIBIOS en el ámbito penal por las fuerzas de seguridad, es la total discrecionalidad con la que se utiliza el Sistema, dado que la normativa no establece lineamientos específicos para su uso en materia de investigaciones criminales. ¿Se utiliza para la investigación de cualquier tipo de delito, sin importar su magnitud o el bien jurídico tutelado? ¿Es la primera medida de investigación que se utiliza? Estos puntos en particular se encuentran actualmente en estudio en la ADC y serán materia de un posterior trabajo.

IV Conflictos con derechos fundamentales

Luego del análisis desarrollado a lo largo del presente trabajo, cabe finalizar con los puntos elementales y los interrogantes principales partir de los cuales podemos –y debemos– estudiar el impacto de las tecnologías de identificación biométrica introducidas como políticas públicas en los derechos de las personas:

- La introducción de SIBIOS mediante un decreto del Poder Ejecutivo pone en duda su legitimidad, a la luz del principio de legalidad consagrado en la Constitución y los tratados internacionales de derechos humanos.

- El acceso a SIBIOS por parte de las fuerzas de seguridad sin requerimiento de orden judicial, a la vez que estas nuevas tecnologías presentan nuevos desafíos respecto a su utilización en la persecución del delito, ponen en tensión las interpretaciones tradicionales de las garantías de defensa en los procesos legales, lo cual lleva a preguntarnos ¿Bajo qué criterios es utilizado SIBIOS por parte de los distintos usuarios? ¿Es necesaria la existencia de una investigación penal abierta para hacer uso de la base de datos, o acaso las fuerzas de seguridad pueden hacer un uso corriente del mismo?

- Por la naturaleza misma de los datos biométricos, en su carácter de datos sensibles, estos representan las características más íntimas de las personas. En tal sentido cabe preguntarnos ¿Cuáles son los nuevos desafíos que plantea la identificación de personas a partir de estos datos para evitar caer en prácticas discriminatorias? Como vimos anteriormente, la tecnología puede adoptar los sesgos de quienes la desarrollan e implementan, ¿Cuáles son las garantías planteadas por el Estado para evitar que estos sistemas se vuelvan herramientas de segregación o sean utilizados exclusivamente contra determinados grupos sociales?

- Respecto a la finalidad para la cual fue implementada SIBIOS, ¿Cuál es la evidencia que sustente la introducción del mismo? ¿Qué tan efectivo ha sido este Sistema en la prevención y persecución del delito? ¿Podemos afirmar que SIBIOS ha servido para solucionar los problemas que se plantean en el discurso del Estado en términos de seguridad?

- Como vimos en la sección del análisis tecnológico de la identificación biométrica, no solamente encontramos problemas en términos de cómo pueden ser explotados este tipo de tecnologías, sino que la recolección de los datos biométricos presenta un grave riesgo per se. Sistemas como SIBIOS otorgan inmensos poderes al Estado a costa de libertades individuales, pero llegado el caso ¿qué ocurre cuando el gobierno cambia? ¿Cuáles son las protecciones que deben establecerse para evitar el potencial abuso por parte de los gobiernos de turno?

El uso de sistemas de identificación biométrica, y particularmente SIBIOS en Argentina, se encuentran revestidos de un manto de opacidad característica de las instituciones tradicionales del ámbito de inteligencia y militar, lo cual se encuentra arraigado en el nacimiento de las políticas de identificación de los ciudadanos. La falta de transparencia en cómo el Estado utiliza estos sistemas, cómo se resguarda la información y los datos biométricos almacenados en las bases de datos, cuáles son los estudios en los que se sustentan las decisiones de adopción de tecnología, cuáles fueron los parámetros de consideración para la adquisición de las soluciones tecnológicas, son preguntas que tienen respuesta pendiente.

Todas las respuestas a estos interrogantes deberán tener en consideración los elementos previstos en la Constitución y los principales tratados internacionales de derechos humanos: la Declaración Universal de los Derechos Humanos, el Pacto Internacional de Derechos Civiles y Políticos, la Convención Americana sobre Derechos Humanos. Todos estos instrumentos coinciden en reconocer que la privacidad, la libertad de expresión, de pensamiento y de opinión, la libertad de asociación y de reunión, la libertad de culto, así como también la libertad de buscar y recibir información, son derechos esenciales del hombre ya que hacen a su dignidad. Por lo tanto, cualquier interferencia por parte del Estado debe estar basada en fuertes fundamentaciones, sustentadas en datos duros y diagnósticos serios e independientes, a fin de cumplir con las condiciones de necesidad y proporcionalidad requeridas para la legitimidad de toda medida que pretenda limitar derechos fundamentales.


por los Derechos Civiles