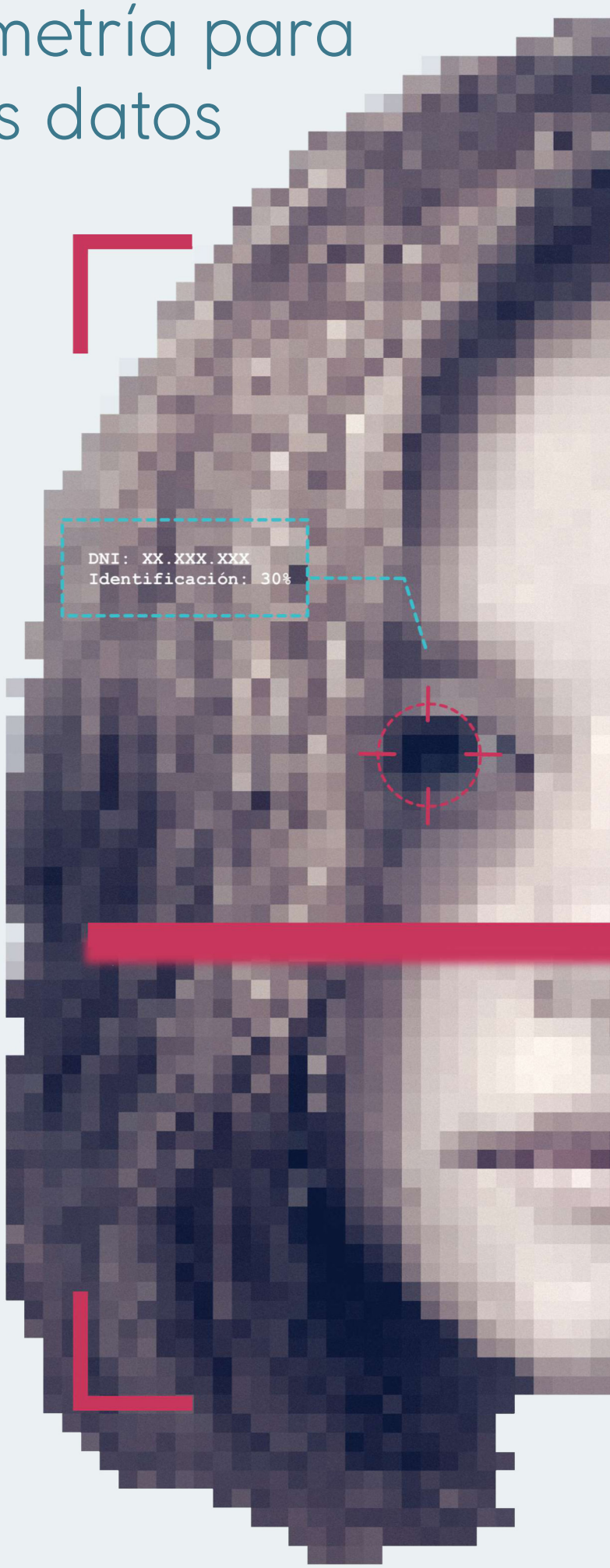
Desafíos de la biometría para la protección de los datos personales

Reflexiones sobre el caso SIBIOS



por los Derechos Civiles

Área Digital
Asociación por los Derechos Civiles

Mayo 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/.

Índice

Desafíos de la biometría para la protección de los datos personales: Reflexiones sobre el caso SIBIOS*

I. Las dos identidades de la biometría

Cuando imaginamos un futuro distópico en donde los seres humanos viven en medio de un ambiente omnipresente de represión política y social, el lugar común nos sugiere seguir la novela *1984* de George Orwell. Allí, la violación a los derechos de las personas está producida por acciones estatales que también generan dolor, temor, intimidación o alienación colectiva. En síntesis, a los individuos que viven en la sociedad *orwelliana* no se les oculta el control sofocante y la propaganda desmoralizadora cuyo objetivo es impedir cualquier intento de disenso o incluso el más mínimo ejercicio de pensamiento crítico.

Sin embargo, existe otra forma de imaginar una distopía. La novela *Un Mundo Feliz* de Aldous Huxley nos presenta un futuro en el cual los individuos viven en un estado de permanente felicidad y en el que problemas como la guerra y la pobreza han sido resueltos. No obstante, esta vida está lejos de ser ideal. A cambio de esos beneficios, la humanidad ha debido entregar muchas cosas: el arte, la manifestación de las emociones, la familia, la libertad de pensamiento, entre otras. En esta ocasión, la violación de derechos no va unida a acciones que producen dolor o temor, sino más bien todo lo contrario: el bienestar físico y material es condición esencial para el ejercicio del dominio político.

En el caso de la biometría, estos dos enfoques pueden combinarse perfectamente para dar cuenta del impacto que el uso de dichas tecnologías tiene en la vida de las personas. Por un lado, la posibilidad de identificar a cualquier individuo en todo momento y mediante un sencillo procedimiento recuerda al modelo de sociedad vigilada presente en *1984*. Por otro lado, la apelación constante a los beneficios que la implementación de estas herramientas tendrá para nuestras actividades y para el desarrollo

*El presente informe fue escrito por **Eduardo Ferreyra**, 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. Encargado de diseño y diagramación: **Leandro Ucciferri**.

de prácticas empresariales nos hace rememorar la sociedad "*perfecta*" de *Un Mundo Feliz*. Así, podríamos decir que la identidad de la biometría es bifronte: una (supuestamente) positiva que nos promete traer eficiencia y seguridad a nuestras vidas y actividades; y otra negativa, que amenaza con dejar un espacio muy acotado a nuestra privacidad.

Actualmente, la gran mayoría de los países de América Latina viven bajo regímenes democráticos. Esto no implica decir que los derechos de los latinoamericanos y las latinoamericanas son respetados o se encuentran satisfechos en su totalidad. Pero al menos significa que el estado policial de Orwell –aunque sea por el momento- se encuentra presente únicamente en su novela y no se ha materializado en la realidad de la gran mayoría de los países de la región. Esta situación produce la siguiente consecuencia: que los gobiernos se vean obligados a presentar la identidad "*positiva*" de la biometría para poder implementar su identidad negativa.

En el caso argentino, el anuncio de la implementación de SIBIOS por parte del gobierno en 2011 fue realizado bajo la promesa de que dicho sistema iba a contribuir a la prevención y sanción del delito. Es decir, se presentó su cara "*positiva*" pero no se dijo nada de su cara negativa.

En el informe "La identidad que no podemos cambiar"[1], nos hemos dedicado a reparar esa omisión, a través de un reconocimiento de esa faz negativa, cuya existencia es más cierta que los supuestos beneficios anunciados. Sin embargo, dicha tarea debe ser completada por un examen de las herramientas que las personas poseen para defenderse frente a una situación en la cual su posición de fuerza es extremadamente débil, a la luz de las poderosas capacidades tecnológicas del Estado y las grandes empresas. En ese sentido, la protección de datos personales puede cumplir un rol fundamental en revelar la cara negativa de la biometría. El ejemplo de SIBIOS nos servirá como caso de estudio para poner en evidencia esta afirmación.

II. Tres enfoques sobre la privacidad

Si bien la distinción entre la esfera privada y la esfera pública está presente desde la Antigüedad[2], no es sino hasta el advenimiento de la Modernidad que la idea de un ámbito de reserva del individuo se encuentra cristalizada bajo la forma de un derecho que puede ser esgrimido ante las autoridades judiciales en caso de sufrir una afectación. Es por ello que se considera una característica esencial de nuestras sociedades democráticas la existencia de un espacio en el cual el individuo es soberano, y en donde la acción del Estado y de otros particulares no puede llegar sin violar sus derechos. "Sin privacidad no hay democracia" es una máxima cuya veracidad puede comprobarse mediante el simple

[1] La identidad que no podemos cambiar, ADC, 2017, disponible en https://adcdigital.org.ar/2017/04/26/la-identidad-no-podemos-cambiar-biometria-sibios/

[2] Para un análisis acerca de las relaciones entre las esferas privadas y públicas en el mundo de la Antigüedad consultar ARENDT, HANNAH, La condición humana (Capítulo 2 "La esfera pública y la privada") Paidos Ibérica, Madrid, 2005.

recurso de echar un vistazo a los regímenes políticos en los cuales todo vestigio de espacio privado ha sido eliminado.

La importancia de la privacidad se manifestó en el progresivo desarrollo que dicho concepto fue adquiriendo a lo largo de los años. Así, la evolución de las costumbres sociales y el desarrollo tecnológico ha ido ensanchando el conjunto de situaciones que consideramos "privadas" y, por lo tanto, sujetas a la protección de las leyes. No es el propósito de este breve apartado hacer una historia de la privacidad. Sin embargo, podemos distinguir tres etapas que -desde un punto de vista jurídico- son de suma relevancia.

En primer, lugar el concepto hizo referencia a una noción espacial[3]. Así, se consideraba que el derecho a la privacidad tenía por objeto los lugares que las demás personas no podían acceder ni tener conocimiento sin autorización de la persona titular del derecho. Dentro de ese enfoque, el domicilio constituía el ejemplo paradigmático, pues ahí su habitante tenía la facultad de impedir cualquier intromisión arbitraria. La Constitución argentina reconoció esa característica al declarar al domicilio "inviolable" (art. 18). Además del lugar físico de residencia, se consideró que determinados objetos también eran susceptibles de ser considerados dignos de protección: fue el caso de la correspondencia y demás papeles privados. En todos estos supuestos, la Constitución estableció la posibilidad de interferencia por parte de las autoridades públicas, bajo la condición de establecer los casos y justificativos a través de una ley.

En una segunda etapa, el concepto de privacidad se desplazó desde un enfoque espacial hacia uno que evaluaba la naturaleza de la conducta a regular. En esta ocasión, se entendió que los comportamientos que no generaban daños a terceros pertenecían a la esfera íntima del individuo y por ende, no debían ser sancionados por el derecho. Desde este punto de vista, el derecho a la privacidad protegía la autonomía personal en la elección de planes de vida, evitando la intromisión estatal en asuntos que sólo atañen a la moral del individuo[4]. Así, la tenencia de drogas para consumo personal o el matrimonio entre personas del mismo sexo son considerados como conductas incluidas dentro del ámbito privado de los individuos y por ende, no deben ser prohibidas por el Estado. Argentina ha consagrado este aspecto del derecho a la privacidad en el art. 19 de su Constitución, cuando establece que las "acciones privadas (...) están exentas de la autoridad de los magistrados".

Los dos conceptos de privacidad convivieron por mucho tiempo de manera exclusiva. Sin embargo, en los últimos tiempos surgieron nuevos fenómenos que volvieron necesaria una redefinición de las nociones tradicionales con las cuales el derecho se venía manejando. Por un lado, el rápido desarrollo

[3] Cierta doctrina considera este supuesto como ejemplo de un derecho a la intimidad, para diferenciarlo de un derecho a la privacidad, que se referiría a las acciones que no afectan a terceros. Cfr. NINO, CARLOS Fundamentos de Derecho Constitucional, Astrea, Buenos Aires, 2000, p.304. Sin embargo, tanto la jurisprudencia estadounidense como la Corte Suprema de Argentina utilizan los términos de manera indistinta, criterio que -a los efectos del presente trabajo- hemos seguido.

[4] IPOHORSKY, JOSE "El derecho a la intimidad" en Comentarios de la Constitución de la Nación Argentina, La Ley, Buenos Aires, 2016 p. 481

de las nuevas tecnologías provocó una penetración de lo digital en nuestras vidas cotidianas. Por otro lado, el rol trascendental que el conocimiento desempeña en las economías del siglo XXI ha impulsado una avidez inédita por la adquisición, consumo y difusión de información. La unión de estos dos fenómenos ha provocado que el concepto de privacidad haya ingresado en una nueva etapa, en donde ha empezado a relacionarse con el concepto de información[5]. Desde esta perspectiva, el derecho a la privacidad es el derecho a que toda información sobre la vida privada de una persona poseída por terceros -entre ellos, los Estados y las empresas- sea utilizada de una manera que no perjudique los intereses del titular de esa información[6]. En Europa se utiliza el término "protección de datos personales" para designar este derecho, el cual es considerado como un derecho independiente, aunque sin dejar de reconocer su fuerte vínculo con la privacidad.

Argentina ha seguido el modelo europeo y actualmente cuenta con la ley 25.326 de protección de datos personales sancionada en el año 2000[7]. Tal como lo dice su art.1, uno de los objetivos de dicha norma es garantizar el "derecho a la intimidad de las personas" a fin de cumplir con lo establecido por la Constitución en su art. 43[8]. De esta manera, la protección de datos personales constituye un punto de apoyo indispensable para la defensa de los derechos de las personas frente a los peligros de las tecnologías biométricas.

III. Los datos biométricos son datos personales y sensibles

La ley argentina define los datos personales como toda "información de cualquier tipo referidas a personas físicas (...) determinadas o determinables" (art. 2). La amplitud de la definición permite que no sea muy difícil encuadrar a los datos biométricos como una especie de datos personales, ya que las tecnologías biométricas permiten la identificación ("determinación" en el lenguaje de la ley argentina) de las personas.

Cuando una muestra biométrica es sacada de una persona, los datos que se extraen de ella son analizados y convertidos en una plantilla que se almacena en una base de datos o en un objeto de posesión del individuo (como una tarjeta inteligente[9]). De esta manera, una muestra biométrica puede ser comparada con las plantillas almacenadas con el fin de identificar al individuo. Así, en la mayoría de los casos el uso de tecnologías biométricas implica la recolección de datos a partir

[5] Cfr. RICHARDS, NEIL M., Four Privacy Myths (April 22, 2014). Extraído de, "A World Without Privacy?" (Cambridge Press, Austin Sarat, ed. 2015). Disponible en SSRN: https://ssrn.com/abstract=2427808 p.13

[6] Esta definición no se refiere a los casos en los que la información sea utilizada en el marco del ejercicio del derecho a la libertad de expresión e información. Allí entran en juego otras consideraciones y por ende, el análisis de posibles conflictos entre tales derechos debe ser realizado desde un enfoque distinto al adoptado en el presente trabajo.

[7] Consultar en http://servicios.infoleg.gob.ar/infolegInternet/anexos/60000-64999/64790/norma.htm

[8] Consultar en http://servicios.infoleg.gob.ar/infolegInternet/anexos/0-4999/804/norma.htm

[9] Una tarjeta inteligente es una tarjeta que contiene un microprocesador interno para almacenar y procesar datos y registros. Puede utilizarse con finalidades comerciales, financieras, de transporte, entre otras.

de los cuales una persona puede ser identificada y por lo tanto su tratamiento debe ajustarse a las regulaciones vigentes en materia de protección de datos[10].

Sin embargo, debemos dar un paso más y preguntarnos si los datos biométricos no se encuadran dentro de una categoría especial de datos personales: los datos sensibles. Según la definición de la ley argentina, se considera dato sensible los "datos personales que **revelan origen racial y étnico**, opiniones políticas, convicciones religiosas, filosóficas o morales, afiliación sindical e información referente a la salud o a la vida sexual." (art. 2. El énfasis es propio). Al enfocar nuestro estudio sobre SIBIOS, nos referiremos únicamente a los datos almacenados en dicho sistema: las huellas dactilares (o palmares) y las fotografías de rostros.

Respecto al primer supuesto, una investigación de la Universidad de Carolina del Norte ha encontrado diferencias significativas entre las huellas dactilares pertenecientes a personas de ascendencia africana y personas de ascendencia europea.[11] Si bien los propios investigadores afirman que es necesaria una muestra mayor de personas y un análisis de etnias más diversas para obtener una conclusión definitiva, los primeros resultados científicos indican una alta posibilidad de que las huellas dactilares reflejen patrones propios de una etnia específica.[12]

En cuanto a las fotografías, resulta indudable que de la exhibición de nuestro rostro puede determinarse a qué etnia pertenecemos. Asimismo, las imágenes también pueden revelar otro tipo de datos sensibles. Si vemos la foto de una persona usando un *hijab*, sabremos identificar cuál es la religión que profesa. Por otro lado, se debe tener presente que las tecnologías de reconocimiento facial poseen un grado de confiabilidad bastante cuestionable. Debido a la variabilidad con que se manifiestan diversos factores que influyen en la captación de la imagen - como el ángulo desde el cual es tomada la fotografía, el tipo de fondo, la luz, el tamaño de la base de datos sobre la cual corre el sistema, el envejecimiento de la persona, el vello facial y las expresiones faciales-, existe el riesgo de que la identificación o la verificación realizada por el sistema de reconocimiento no sea la correcta.[13]

Finalmente, el derecho a la imagen personal ha sido consagrado por el Código Civil y Comercial, que en su art. 53 establece como regla general la necesidad de obtener el consentimiento de la persona

[10] Cfr. WOO, RODERICK B Challenges Posed By Biometric Technology On Data Privacy Protection And The Way Forward, Hong Kong, 2010. Disponible en https://www.pcpd.org.hk/english/news_events/speech/files/speech_20100104.pdf p.1

[11] FOURNIER, N. A. and ROSS, A. H. (2016), Sex, Ancestral, and pattern type variation of fingerprint minutiae: A forensic perspective on anthropological dermatoglyphics. Am. J. Phys. Anthropol., 160: 625–632. doi: 10.1002/ajpa.22869. Puede consultarse el abstract en http://onlinelibrary.wiley.com/doi/10.1002/ajpa.22869/full

[12] GRAY, RICHARD Fingerprints reveal whether you're black or white: Distinctive patterns show whether a person is of African or European descent. Mail Online, 29 de septiembre de 2015, disponible en http://www.dailymail.co.uk/sciencetech/article-3253295/Fingerprints-reveal-black-white-Distinctive-patterns-person-African-European-descent.html

[13] Cfr. Asociación por los Derechos Civiles (ADC) La identidad que no podemos cambiar. Cómo la biometría afecta nuestros derechos humanos. Buenos Aires 2017 p.9, disponible en https://adcdigital.org.ar/wp-content/uploads/2017/04/La-identidad-que-no-podemos-cambiar.pdf

para poder captar o reproducir su imagen.[14] Asimismo, su inclusión dentro del capítulo de "Derechos y actos personalísimos" es una muestra de la importancia otorgada a la imagen personal en el actual ordenamiento jurídico. Esta caracterización implica que el consentimiento para su utilización no debe presumirse, es de interpretación restrictiva y puede ser revocado libremente (art.55) De esta manera, la estricta regulación que el Código Civil y Comercial consagra para el tratamiento de la imagen personal constituye un argumento adicional para su consideración como dato sensible.

Por lo tanto, resulta claro que los datos almacenados por SIBIOS reúnen las condiciones exigidas para ser calificados como datos sensibles. Esta interpretación se ve respaldada por la más moderna legislación sobre la materia. En efecto, el flamante Reglamento General sobre Protección de Datos de la Unión Europea[15] ubica a los datos biométricos -en tanto identifiquen de manera unívoca a una persona- dentro del apartado dedicado al tratamiento de categorías especiales de datos personales (art.9), nombre utilizado por la normativa para designar a los datos sensibles.

La caracterización de los datos biométricos como datos sensibles provee a aquéllos de fuertes restricciones en lo que respecta a su utilización por parte de terceros. En ese sentido, podría decirse que la regla general es la prohibición de todo tipo de tratamiento de datos sensibles. Esta lectura encuentra su apoyo en dos disposiciones que se encuentran en el art. 7 de la ley argentina de protección de datos personales. La primera, presente en el inc.1, establece que "ninguna persona puede ser obligada a proporcionar datos sensibles". La segunda se encuentra en el inc. 3 cuando se dispone que "queda prohibida la formación de archivos, bancos o registros que almacenen información que directa o indirectamente revele datos sensibles".

La regla antedicha no es absoluta y posee excepciones. Dejando de lado aquellas que no hacen al análisis del presente informe,[16] conviene detenernos en el supuesto del inc.2. Allí se determina que "los datos sensibles sólo pueden ser recolectados y objeto de tratamiento cuando medien **razones de interés general autorizadas por ley**" (énfasis propio). Esta disposición debe ser considerada con mucho cuidado ya que una mala interpretación de la misma puede romper todo el esquema protectorio creado para proteger los datos sensibles.[17] Efectivamente, bastaría que el Estado diga que una cuestión es de interés general para que no se apliquen las garantías previstas.

[14] Si bien existen excepciones al consentimiento fijadas por la norma (actos públicos, interés científico, cultural o educacional, o ejercicio del derecho a informar) ninguna se aplica a las actividades de SIBIOS, con lo cual su caso se rige bajo la regla general. Ver art. 53 Código Civil y Comercial en http://servicios.infoleg.gob.ar/infolegInternet/anexos/235000-239999/235975/texact.htm#6

[15] Consultar en http://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:32016R0679&from=ES

[16] Ellas son: el tratamiento que se realice con finalidades estadísticas o científicas cuando no puedan ser identificados sus titulares; los datos relativos a antecedentes penales o contravencionales o el registro de sus miembros que puedan hacer la Iglesia Católica, las asociaciones religiosas y las organizaciones políticas y sindicales.

[17] Algo similar sucede con el régimen general, en el cual la mayoría de las garantías establecidas a favor de las personas no se aplican cuando es el Estado el encargado de realizar el tratamiento de datos personales. Para profundizar más en este punto, consultar ASOCIACIÓN POR LOS DERECHOS CIVILES, El Estado Recolector, Buenos Aires, 2014 disponible en https://adcdigital.org.ar/wp-content/uploads/2016/01/El-Estado-recolector.pdf

Es por ello que una lectura que se ajuste a un régimen democrático y republicano de gobierno debe siempre tratar de limitar el accionar estatal a fin de respetar los derechos de los individuos. Afortunadamente, el ordenamiento jurídico argentino dispone de las herramientas para llevar a cabo esa tarea con éxito.

En primer lugar, la propia ley 25.326 establece que las razones de interés general deben ser "autorizadas por ley". Al momento de desentrañar el significado de "ley", la Corte IDH ha dicho que en caso que la misma tenga por objeto la restricción de un derecho o libertad, se debe entender que se trata de una "norma jurídica de carácter general (...) emanada de los **órganos legislativos constitucionalmente previstos** y democráticamente elegidos..."[18] (énfasis propio). Por lo tanto, no resulta admisible el dictado de decretos u otros instrumentos de similar naturaleza, ya que el Poder Legislativo no puede intervenir en ellos. Esta disposición pone en cuestión desde el principio la legalidad de SIBIOS, el cual fue creado a través de un decreto presidencial.[19]

En segundo lugar, no debemos olvidar que el sistema de protección de datos personales está conformado por un conjunto de principios que deben ser respetados al momento de realizar un tratamiento de datos. Si tenemos en cuenta que estos principios deben ser cumplidos en el caso de datos personales en general, con más razón se aplican cuando los datos revisten el carácter de sensibles, tal como lo son los datos biométricos. Por lo tanto, al momento de examinar la legalidad del tratamiento, se debe exigir un cumplimiento estricto de los requisitos de licitud, exactitud, finalidad, calidad y demás.[20] En ese sentido, la falta de publicidad con la que SIBIOS realiza sus actividades de tratamiento de datos y la ausencia de órganos de supervisión fuertes impiden que se ejerza un control efectivo de la manera en que se realizan las operaciones de tratamiento.

Al respecto, se debe señalar que en Abril de 2017 hubo una modificación en la estructura institucional y la Unidad de Coordinación y Seguimiento de SIBIOS quedó a cargo de la Dirección Nacional de Policía Científica -bajo la órbita del Ministerio de Seguridad-, con el asesoramiento de especialistas del Registro Nacional de las Personas, de la Dirección Nacional de Migraciones y de las áreas de policía científica de la Policía Federal Argentina, la Gendarmería Nacional, la Prefectura Naval Argentina y la Policía de Seguridad Aeroportuaria.[21] Así, se perdió una inmejorable oportunidad para fortalecer

[18] CORTE INTERAMERICANA DE DERECHOS HUMANOS Opinión Consultiva OC-6/86 La expresión "leyes" en el artículo 30 de la Convención Americana sobre Derechos Humanos, Costa Rica, 1986 cons. 38, disponible en http://www.corteidh.or.cr/docs/opiniones/seriea_06_esp.doc

[19] Ver decreto 1766/2011 en http://servicios.infoleg.gob.ar/infolegInternet/anexos/185000-189999/189382/norma.htm

[20] Para un análisis de los sistemas de protección de datos en América Latina ver ASOCIACIÓN POR LOS DERECHOS CIVILES El sistema de protección de datos personales en América Latina. Oportunidades y desafíos para los derechos humanos Buenos Aires, 2017 disponible en https://adcdigital.org.ar/wp-content/uploads/2017/02/Sistema-proteccion-datos-personales-LatAm.pdf. En el caso argentino se puede profundizar el análisis normativo en ASOCIACIÓN POR LOS DERECHOS CIVILES, Legislación argentina sobre datos personales, Buenos Aires, 2017 disponible en https://adcdigital.org.ar/wp-content/uploads/2017/01/Legislacion-argentina-sobre-proteccion-de-datos-personales-ADC.pdf

[21] Anteriormente, la Unidad estaba integrada por representantes del Ministerio de Seguridad, el Registro Nacional de

los mecanismos de control a través de la incorporación de organismos como la Dirección Nacional de Protección de Datos Personales.

Por último, no debemos dejar de mencionar lo dispuesto en el art. 23 inc. 2[22], ya que un primer vistazo a dicha disposición pareciera llevarnos a la conclusión de que el tipo de tratamiento realizado por SIBIOS se encuentra habilitado. Sin embargo, una lectura más atenta permite sacar otras conclusiones.

Lo primero a destacar es que la redacción habla de "datos personales". Si tenemos en cuenta que cuando la ley ha querido referirse a los datos sensibles, los ha llamado precisamente de esa manera[23], resulta lógico concluir que el tratamiento de datos biométricos -en tanto datos sensibles- no puede justificarse en base a esta disposición. Así, su legalidad debería juzgarse en base al régimen más estricto previsto para los datos sensibles en el art.7.

No obstante, si por hipótesis aceptamos la regulación del art. 23 inc.2, el análisis tampoco resulta demasiado favorable para SIBIOS. La disposición permite el tratamiento de datos que resulten "necesarios" para el cumplimiento "estricto" de las misiones legalmente asignadas, en este caso, la seguridad pública y la represión de delitos. Esta doble restricción es prueba de la intención del legislador de acotar al máximo las facultades de tratamiento de esta clase de datos. Es por ello que debemos examinar estos requisitos a la luz del criterio de "peligro real". Esta fórmula ha sido seguida por la legislación española[24] -inspiración de la ley argentina de protección de datos personales- y constituye un medio para evitar la arbitrariedad del accionar estatal. Desde este enfoque, resulta difícil de justificar el modo de operar de un sistema que funciona de manera permanente las 24 horas de los 365 días del año, más allá de que exista o no un "peligro real" para la seguridad de las personas.

las Personas y la Dirección Nacional de Migraciones, contando con el asesoramiento de las áreas de policía científica de la Policía Federal Argentina, la Gendarmería Nacional, la Prefectura Naval Argentina y la Policía de Seguridad Aeroportuaria. Para la actual integración, consultar Art. 2 decreto 243/2017 modificatorio del decreto 1766/2011 disponible en https://www.boletinoficial.gob.ar/#!DetalleNorma/161771/20170410

[22] Art. 23 inc. 2 de la ley 25.326: "El tratamiento de datos personales con fines de defensa nacional o seguridad pública por parte de las fuerzas armadas, fuerzas de seguridad, organismos policiales o inteligencia, sin consentimiento de los afectados, queda limitado a aquellos supuestos y categoría de datos que resulten necesarios para el estricto cumplimiento de las misiones legalmente asignadas a aquéllos para la defensa nacional, la seguridad pública o para la represión de los delitos. . . "

[23] La intención del legislador de distinguir ambas categorías se pone de manifiesto en la dedicación de un apartado exclusivo a su regulación (art. 7).

[24] El art. 22 inc. 2 de la LOPD dice: "La recogida y tratamiento para fines policiales de datos de carácter personal por las Fuerzas y cuerpos de Seguridad sin el consentimiento de las personas afectadas están limitados a aquellos supuestos y categorías de datos que resulten necesarios para la prevención de un peligro real para la seguridad pública o para la represión de infracciones penales, debiendo ser almacenados en ficheros específicos establecidos al efecto, que deberán clasificarse por categorías en función de su grado de fiabilidad.". Si bien el modelo para la elaboración de la ley argentina fue la derogada Ley Orgánica de Regulación del Tratamiento automatizado de los datos de carácter personal (LORTAD) el presente artículo es muy similar al anterior.

IV. Conclusión

La identidad "positiva" de la biometría nos presenta a una herramienta eficaz para la prevención del delito. Pero luego de ser sometida a un examen de reconocimiento, otra identidad se nos revela. Esa identidad "negativa" nos dice que el uso de tecnologías biométricas presenta serios desafíos a los derechos de las personas, en particular el derecho a que sus datos personales sean protegidos.

Los datos biométricos brindan información sobre lo más íntimo de un ser humano: su cuerpo. A su vez, el carácter permanente de ellos impide que en caso de ser divulgados de manera ilegítima, el daño pueda ser reparado. A diferencia de una contraseña, no podemos volver a configurar nuestro iris o nuestra huella digital. Por eso, no hay nada más personal que un dato biométrico.

Asimismo, los datos biométricos nos revelan aspectos muy delicados de un individuo como su origen racial o étnico o su salud. De esta manera, pueden ser utilizados para el ejercicio de prácticas discriminatorias y estigmatizantes sobre sus titulares. Por lo tanto, los datos biométricos no solo son personales: son datos personales *sensibles*.

En consecuencia, todo uso de tecnologías de biometría debe ser realizado de manera acorde al régimen de tutela especial establecido en la ley para el tratamiento de datos de esta naturaleza. Frente a este principio, no puede alegarse de *manera ligera* la existencia de una cuestión de seguridad, de defensa u otro interés. La organización institucional de Argentina está basada en el reconocimiento de derechos preexistentes al establecimiento de toda autoridad.[25] No es el individuo el que debe acomodar sus derechos al accionar del gobierno. Es el gobierno el que debe ajustar su conducta a los derechos de las personas.

En el caso de SIBIOS, pareciera que se optó por una lógica distinta a la señalada. Con base en alusiones genéricas a cuestiones de seguridad, el gobierno argentino ha creado un sistema que contiene las huellas digitales y fotografías de todas las argentinas y todos los argentinos. Este tipo de información puede ser utilizada de maneras que perjudiquen gravemente la privacidad, la intimidad y la libertad de expresión de las personas. Así, en nombre de una supuesta eficiencia, se pone en riesgo una de los objetivos principales de su ordenamiento jurídico: "*asegurar los beneficios de la libertad, para nosotros, para nuestra posteridad, y para todos los hombres del mundo que quieran habitar en el suelo argentino*".[26]

[25] Es la doctrina que emana del art. 33 CN: "Las declaraciones, derechos y garantías que enumera la Constitución no serán entendidos como negación de otros derechos y garantías no enumerados; pero que nacen del principio de la soberanía del pueblo y de la forma republicana de gobierno".

[26] Cita extraída del Preámbulo de la Constitución Argentina.


por los Derechos Civiles