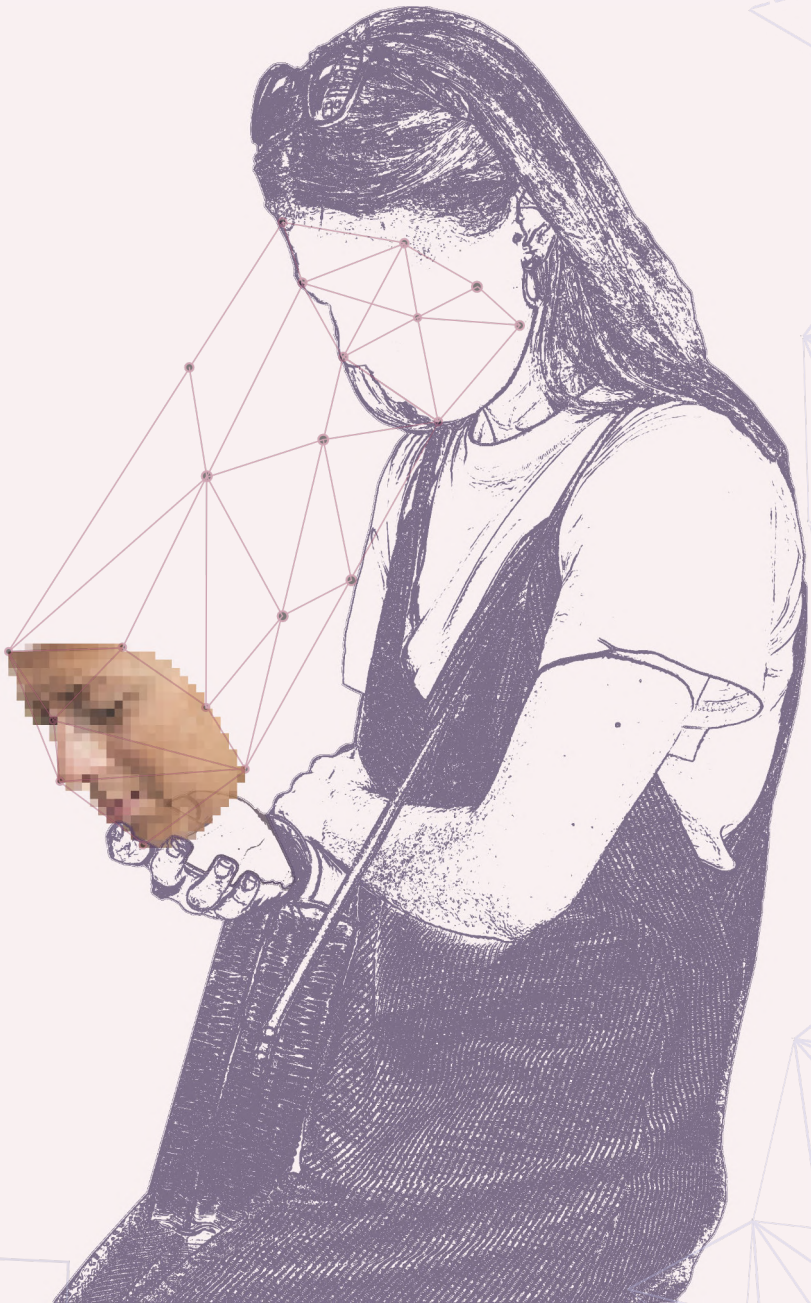
TU YO DIGITAL

Descubriendo las narrativas sobre identidad y biometría en América Latina: los casos de Argentina, Brasil, Colombia y México



APC
por los Derechos Civiles

Asociación por los Derechos Civiles

Abril 2019
https://adcdigital.org.ar | https://adc.org.ar

Este informe fue realizado como parte de un proyecto que contó con el apoyo de la Ford Foundation, 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/by-nc-sa/4.0/

La investigación para este trabajo contó con los aportes de InternetLab en Brasil, Fundación Karisma en Colombia y Red en Defensa de los Derechos Digitales (R3D) en México.

El documento *Tu yo digital. Descubriendo las narrativas sobre identidad y biometría en América Latina: los casos de Argentina, Brasil, Colombia y México* es de difusión pública y no tiene fines comerciales.

Resumen ejecutivo

Las tecnologías biométricas han permeado la vida diaria de las personas, siendo promovidas por los mismos Estados como la solución infalible ante los problemas estructurales de la sociedad. En esta investigación, nos adentramos en el análisis de las realidades de Argentina, Brasil, Colombia y México, respecto a las narrativas sobre la identidad de las personas y el vínculo con la implementación de tecnologías que recolectan, almacenan y procesan datos biométricos.

A través del estudio de los marcos normativos y las políticas públicas promovidas, damos cuenta del impacto que la tecnología biométrica presenta para el ejercicio de derechos. Este impacto se hace presente tanto en la faz individual de derechos como la privacidad y libertades como la expresión, reunión y asociación, así como también en derechos colectivos, tales como la salud, la educación y la seguridad social.

El vínculo entre la identidad y las personas, como algo de lo que el Estado se encuentra en su derecho para disponer y administrar, vislumbra una lógica de control, en la que las instituciones públicas pueden gobernar a la población como recursos. Esto se vuelve más evidente cuando el otorgamiento de beneficios o servicios sociales está condicionado a la entrega de datos biométricos, sin posibles alternativas, profundizando a su vez la desigualdad social.

El análisis normativo es complementado con un examen de diversos casos de estudio en cada país, que brindan una ventana hacia el razonamiento de estos sistemas promovidos por organismos Estatales. Finalmente, cerramos el presente informe con una serie de recomendaciones, destinadas a informar el camino a seguir en el desarrollo de políticas públicas, bajo el respeto y garantía de derechos fundamentales.

Índice

Tu yo digital:
Descubriendo las narrativas sobre identidad y biometría en América Latina*

I. Introducción

Establecer una fecha exacta en la cual las personas empezamos a otorgarnos nombres puede resultar intrincado, aunque sí podemos argumentar que el establecimiento y consolidación de las lenguas, la invención de profesiones y la propiedad privada –en paralelo al crecimiento de las comunidades en su camino a convertirse en sociedades– comenzó a marcar la necesidad de asignar una característica para poder diferenciarnos e interactuar entre nosotros. Incluso sin notarlo, esta característica que portamos en nuestro día a día, por más intangible que sea en realidad, puede teñir diversos aspectos en la manera en que nos relacionamos e interactuamos con la sociedad. El nombre, aquellas palabras que se nos asignan, generalmente al nacer, tiene potenciales efectos en cadena durante toda nuestra vida, dando forma al prisma a través del cual observamos y experimentamos todas las acciones y decisiones que nos mueven.

Cuando leemos u oímos un nombre, automática e implícitamente "comenzamos a asociarle diversas características, y usamos esa asociación –aún sin darnos cuenta– para emitir juicios no relacionados sobre la competencia y la idoneidad de su portador", explica Maria Konnikova.[1]

La construcción y evolución de las sociedades modernas, cada vez más complejas y de mayor dimensión, tanto en su expansión geográfica como poblacional, fueron reforzando la idea del nombre como parte irrevocable de la identidad de las personas.

---

*El presente documento fue elaborado por **Leandro Ucciferri**, analista de políticas públicas, abogado e investigador de la Asociación por los Derechos Civiles (ADC), con los aportes para los países por: **Dennys Antonialli** y **Maria Luciano** de InternetLab, para Brasil; **Juan Diego Castañeda**, **Lucía Camacho** y **Joan López** de la Fundación Karisma, para Colombia; y **Santiago Narváez** de la Red en Defensa de los Derechos Digitales (R3D), para México. Diseño de portada y diagramación: Leandro Ucciferri. https://adcdigital.org.ar | https://adc.org.ar

[1] Konnikova, Maria, "Why Your Name Matters", The New Yorker, 19 de diciembre de 2013, disponible en: https://www.newyorker.com/tech/annals-of-technology/why-your-name-matters

Sin embargo, en la búsqueda de alcanzar un mayor control sobre las personas, una forma de identificación empezaría a perfeccionarse. Mediante el uso de los rasgos biológicos, morfológicos o de comportamiento de las personas, se puede obtener una plantilla digital asignable a todo ser humano para reconocerlo en forma inequívoca.

En las últimas dos décadas, la cantidad de empresas del sector privado que desarrollan tecnología con base en datos biométricos, y el número de Estados que han implementado dicha tecnología en diversos ámbitos de la vida en sociedad, creció de manera exponencial.

Desde hace al menos cinco años que en la Asociación por los Derechos Civiles (ADC) trabajamos en el monitoreo, análisis y crítica de las políticas públicas que naturalizan y sistematizan la identificación de las personas mediante tecnologías biométricas, dada su potencial injerencia en derechos fundamentales, particularmente en la privacidad y la libertad de expresión.

A fines de 2016, en el marco del Foro de Gobernanza de Internet (IGF, por sus siglas en inglés) en Guadalajara, México, realizamos un evento en donde reunimos a un grupo de expertos de diversos países alrededor del mundo con el objetivo de intercambiar experiencias sobre iniciativas y políticas que buscan implementar tecnologías de biometría. El taller nos permitió trazar un primer mapeo del estado de situación en países como Perú, Chile, México, Colombia, Brasil, India, Paraguay, Canadá, Reino Unido, Estados Unidos y Polonia, principalmente a través de los ojos de la sociedad civil, evidenciando cómo esta temática es tratada en diversos contextos.

Considerando esta experiencia como antecedente, en mayo de 2017 publicamos nuestro primer informe regional, que da cuenta de las iniciativas y políticas públicas implementadas en América Latina para la identificación de personas utilizando tecnología biométrica. Este primer informe fue posible gracias a las contribuciones de profesionales y diversas organizaciones basadas en Chile, Brasil, Colombia, México, Paraguay, Perú y Venezuela.[2]

A partir de esta exploración inicial concluimos que, en general, las políticas públicas que pretenden implementar el uso de algún tipo de dato biométrico son concretadas con poca o nula transparencia de cara a la ciudadanía, arraigado a su vez a una falta de información sobre las tecnologías y mecanismos utilizados para la recolección, análisis y procesamiento de los datos biométricos; el alcance de las políticas; con quiénes se comparten esos datos y quiénes tienen acceso. Esto en un contexto en donde los marcos jurídicos parecen ser insuficientes para el adecuado tratamiento de los datos biométricos utilizados y el avance de las políticas de identificación.

Elaboramos el presente informe, donde examinamos con mayor detenimiento la situación de Argentina, Brasil, Colombia y México, con el fin de realizar un aporte en búsqueda de una mayor transparencia en las iniciativas y políticas públicas que implementan sistemas de identificación mediante tecnología biométrica. Al mismo tiempo, este trabajo busca profundizar el análisis de los

[2] ADC, "Cuantificando identidades en América Latina", mayo de 2017, disponible en: https://adcdigital.org.ar/portfolio/cuantificando-identidades-en-america-latina/

marcos jurídicos nacionales en los cuales se basan las mencionadas políticas, además de establecer una base para la comparación de las narrativas estatales que las justifican.

Este reporte fue posible gracias al trabajo de las organizaciones Internet Lab en Brasil, Fundación Karisma en Colombia, y Red en Defensa de los Derechos Digitales (R3D) en México, que colaboraron con la ADC en lo respectivo al contexto particular de su país, mediante un proceso que resultó en la confección de conclusiones conjuntas para dar cuenta de las cuestiones acuciantes que presenta esta temática.

El informe procede de la siguiente manera: en la segunda sección se analiza cómo los países abordan las definiciones sobre biometría y datos biométricos, dando cuenta de la necesidad de delimitar su concepción en la construcción de políticas públicas. En la tercera sección se exploran los marcos normativos de cada país para describir el escenario jurídico sobre el que se montan las narrativas de la identidad y la implementación de tecnología biométrica. En la cuarta sección se detallan determinados casos de estudio que han cobrado especial relevancia actualmente en cada país, para dar cuenta de las prácticas estatales en el uso de datos biométricos.

Finalmente, concluimos este reporte con las tendencias que surgen de los cuatro países en estudio, las falencias que se evidencian de las narrativas y marcos jurídicos, a partir de las cuales proponemos una serie de recomendaciones para encaminar el desarrollo de las políticas públicas sobre el uso de biometría.

II. Comparación de conceptos

La definición de lo que entendemos por biometría no se ha dado sin una serie de debates respecto a las diversas acepciones que distintas profesiones le fueron asignando.[3]

El origen de la palabra biometría surge de la unión de dos conceptos de la lengua griega: bio, la vida, y metron, medida o el acto de medir. En su definición más tradicional, la biometría hace referencia al análisis estadístico y matemático de fenómenos y observaciones biológicas, es decir, de aquello que tenga vida.

Las tecnologías biométricas facilitan la captura, almacenamiento y procesamiento de la información biométrica de las personas, es decir, sus rasgos biológicos, morfológicos y de comportamiento. Dichos rasgos o características son luego convertidos en una matriz o plantilla digital que pueden ser leídos por computadoras para ser comparados con otros, generalmente del mismo tipo. Una vez que estas plantillas digitales son vinculadas con el perfil de una persona, entonces las mismas pueden usarse

[3] Ver: https://bib.irb.hr/datoteka/425577.IJCSI_SchattenBacaCubrilo2009.pdf; y https://www.merriam-webster.com/dictionary/biometry

para identificar[4] o verificar[5] su identidad.

El procedimiento de identificación o verificación 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, por ejemplo, causando discriminación a grupos vulnerables al ser más propensa a identificar mal a las personas que no posean tez blanca.

En tal sentido, desde un punto de vista conceptual, surge entonces la necesidad de diferenciar entre "biometría", "tecnologías biométricas" y "datos biométricos", para evitar referirse a ellos de manera indistinta, lo que sería un error, dado las consecuencias que ello acarrea en el ámbito jurídico, como veremos a lo largo de esta sección.[6]

Es importante analizar cómo es entendida la biometría en diferentes países y contextos socioeconómicos, debido a que, por una parte, la diversidad de datos que pueden integrar un sistema biométrico modifican la manera en la que el sistema puede tener injerencia en diversos derechos fundamentales.

Por otro lado, brindar una delimitación en forma clara y precisa sobre los conceptos utilizados promueve la construcción de normativas que respeten el principio de legalidad y avancen hacia una agenda de cumplimiento con estándares mínimos de necesidad y proporcionalidad.

De los países en estudio en el presente informe, ninguno introduce, mediante una ley del órgano legislativo, una definición expresa y detallada sobre los conceptos individualizados anteriormente.

En Argentina, el uso del término biometría vinculado a la identificación de personas comenzó a tener sus primeras apariciones en diversos decretos y resoluciones a partir de 2011, con el Sistema Federal de Identificación Biométrica para la Seguridad, conocido como SIBIOS. Este Sistema marcó un punto de inflexión para la introducción de la tecnología biométrica en diversos organismos públicos, significando un antes y un después en la manera en que el Estado aborda la identidad de las personas.[7]

[4] Se entiende por identificación cuando se comparan los datos biométricos de una persona con los de un número determinado de personas almacenados en una base de datos, es decir, comparar esos datos con los de un grupo entero, representado como *1:n*.

[5] Por verificación se entiende el proceso de corroborar que los datos biométricos de la persona se condicen con los registros que la misma posee en una base de datos, es decir, una comparación *1:1*.

[6] Catherine Jasserand, "Avoiding Terminological Confusion Between the Notions of 'Biometrics' and 'Biometric Data': An Investigation Into the Meanings of the Terms From a European Data Protection and a Scientific Perspective", 1 de septiembre de 2015, disponible en: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3230339

[7] ADC, "Si nos conocemos más, nos cuidamos mejor", 2015, disponible en: https://adcdigital.org.ar/portfolio/nos-conocemos-mas-nos-cuidamos-mejor/

No obstante, el país fue pionero en el uso de huellas dactilares para la identificación de personas desde fines del siglo XIX, específicamente a través del trabajo de Juan Vucetich (1858-1925) en la Policía de la Provincia de Buenos Aires, quien exportó sus prácticas al resto de América Latina y Europa, motivo por el cual desde antes de 2011 encontramos en uso el término dactiloscopia[8].

La primera normativa que utilizó este concepto fue el decreto-ley 17.671 de "Identificación, registro y clasificación del potencial humano nacional" dictada bajo el gobierno de facto del militar Juan Carlos Onganía en 1968. El artículo 9 habilita al uso de "fotografías" e "impresiones dactiloscópicas" para la identificación de personas. Si bien es lógico que originalmente no hiciese referencia a la biometría como tal, es importante destacar que este decreto-ley nunca fue enmendado para incorporar expresamente este término, ni brindar una definición de "tecnología biométrica" o "dato biométrico".

La Ley 25.326 de Protección de Datos Personales tampoco menciona el término "biometría" o "datos biométricos". Sin embargo, en enero de 2019, la Agencia de Acceso a la Información Pública (AAIP), organismo encargado de su fiscalización, publicó la Resolución 4/19[9] en donde determina que es necesario establecer qué entienden por dicho término en concordancia con la normativa de datos personales vigente en el país, debido a que las legislaciones más modernas en la materia ya lo contemplan y es menester adaptarse a la tendencia internacional.

En tal sentido, la AAIP determina que "los datos biométricos son aquellos datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona humana, que permitan o confirmen su identificación única" y serán considerados sensibles[10] solo cuando su uso pueda resultar potencialmente discriminatorio para su titular.[11]

En Brasil, la ley 13.709 de protección de datos personales, sancionada en 2018, incluye a los datos biométricos dentro de la clasificación de los datos personales sensibles[12], ligados a mayores restricciones en su procesamiento con base en el consentimiento del titular de los datos (art. 11).

En la legislación brasileña no existe una definición expresa de los términos "biometría" o "datos

[8] La dactiloscopia es la disciplina basada en el estudio y la comparación de las huellas dactilares para la identificación de las personas. La primera aparición del término registrada en el Boletín Oficial data de 1912, disponible en: https://www.boletinoficial.gob.ar/#!DetalleNormaBusquedaAvanzada/11370722/19120903

[9] Disponible en: https://www.boletinoficial.gob.ar/#!DetalleNormaBusquedaAvanzada/200224/20190116

[10] El artículo 2 de la Ley 25.326 establece que los datos sensibles son 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".

[11] Un análisis detallado sobre la biometría y los datos personales bajo la lupa de la legislación vigente en la materia puede encontrarse en: https://adcdigital.org.ar/portfolio/desafios-la-biometria-la-proteccion-los-datos-personales/ (ADC, 2017)

[12] El artículo 5. II de la Ley 13.709 establece que los datos personales de tipo sensible son aquellos que permitan determinar el origen racial o étnico, la convicción religiosa, la opinión política, la afiliación a sindicato u organización de carácter religioso, filosófico o político; como también los datos referentes a la salud o a la vida sexual, y el dato genético o biométrico, cuando está vinculado a una persona natural.

biométricos", a pesar de que distintas regulaciones de los sistemas de identificación mencionan dichos conceptos.

Debido a que la Justicia Electoral utiliza esta tecnología para la identificación de votantes mediante huellas dactilares, el Tribunal Superior Electoral tiene un glosario de términos dentro de los cuales encontramos los conceptos de "biometría", definido como la "tecnología que permite identificar a una persona por sus características biológicas únicas, es decir, elementos corporales que tienen diferencias particulares como el iris, la retina, la huella digital, la voz, el formato de la cara y el formato de la mano."[13]

Por su parte, el concepto de "identificación biométrica" es definido como el "sistema de identificación que funciona con la recolección de datos biométricos (huellas digitales y fotos) de los electores garantizando que cada persona sea única en el catastro electoral, descartando la posibilidad de que un elector se pase por otro en el acto de votar."[14]

En Colombia, la ley de protección de datos personales, al momento de realizar la clasificación de los datos, determina que los mismos serán catalogados como sensibles si hay en ellos el potencial de afectar la intimidad de la persona o de generar discriminación[15], e incluye también aquellos datos relativos a la salud, a la vida sexual y los datos biométricos. La Corte Constitucional y la Delegatura para la Protección de Datos[16] han entendido que lo sensible del dato radica en que hace parte de la intimidad[17] de la persona.

A pesar de esta mención expresa, la ley no brinda un concepto específico sobre qué entiende por datos biométricos. Sin embargo, solo la Delegatura de Protección de Datos ha apuntado alguna definición general. En esencia, el dato biométrico sería aquel que parte del reconocimiento de una característica física de una persona que resulta única en cada individuo y que permite así distinguirlo de cualquier otro.[18] Aunque a partir de la definición se pueden pensar en muchas especies de datos

[13] Disponible en: http://www.tse.jus.br/eleitor/glossario/termos-iniciados-com-a-letra-b#biometria

[14] Disponible en: http://www.tse.jus.br/eleitor/glossario/termos-iniciados-com-a-letra-i#identificacao-biometrica

[15] Ley 1581 de 2012, "artículo 5. Datos Sensibles. Para los propósitos de la presente ley, se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición así como los datos relativos a la salud, a la vida sexual y los datos biométricos."

[16] La Delegatura de Protección de Datos de la Superintendencia de Industria y Comercio (SIC) es la autoridad para ejercer la vigilancia, inspección y control sobre el tratamiento de datos personales en Colombia en lo que respecta al sector privado (artículo 19 de la Ley 1581 de 2012).

[17] La Sentencia C-1011 de 2008 contiene un pasaje citado en varias ocasiones por la misma Corte Constitucional y la Delegatura para la Protección de Datos para definir el dato sensible: "la información sensible,[está] relacionada, entre otros aspectos, con la orientación sexual, los hábitos del individuo y el credo religioso y político. En estos eventos, la naturaleza de esos datos pertenece al núcleo esencial del derecho a la intimidad" Cfr. Corte Constitucional, sentencia C-1011 del 16 de octubre de 2008, M.P. Jaime Córdoba Triviño.

[18] Superintendencia de Industria y Comercio, Delegatura para la Protección de Datos, conceptos C-2014-273515 y C-2018-299565

biométricos, la Corte Constitucional y la Delegatura –hasta donde se pudo averiguar– han decidido casos solamente relacionados con huellas dactilares y fotografías o videos.

En lo que respecta a las fotografías del rostro existe una salvedad, pues la Delegatura ha dicho que son datos personales pero no necesariamente biométricos y, por lo tanto, sensibles. En casos en los que la administración de un edificio tomaba fotografías a las personas que ingresaban al sitio o se había implementado un sistema de videovigilancia[19], se entendió que se trataba de un dato personal de tipo privado. Esta clasificación proviene de otra línea jurisprudencial de la Corte Constitucional en la que la información se clasifica de acuerdo con su divulgación.[20]

La Delegatura para la Protección de Datos interpretó que una fotografía o video se clasifica como biométrico y, por lo tanto sensible, solo cuando se implemente alguna técnica para "la extracción de elementos particulares del rostro"[21]. Esta interpretación deja dudas sobre qué tipo de técnica y conexión con otras bases de datos se requeriría para determinar el cambio de clasificación del dato para ser biométrico, ya que sería necesario un repositorio con el cual contrastar el resultado de la medición de las características del rostro, aspectos que no han sido abordados por la Delegatura.

Al indagar en diversas consultas ciudadanas que fueron presentadas ante la Delegatura[22], se encontró que el organismo fue precisando lo que entienden por biometría de acuerdo a si distintos tipos de datos pueden ser catalogados como biométricos. De dichas consultas surge que la Superintendencia ha utilizado la definición de la Unión Internacional de Telecomunicaciones (UIT) al referirse a los dato biométricos como "los métodos automatizados que pueden de manera precisa reconocer a un individuo con base en características físicas o de comportamiento".[23]

Además, la Superintendencia define a la biometría como la "tecnología de seguridad basada en el reconocimiento de una característica física e intransferible de las personas, como la huella digital, que al ser característica única de cada individuo permite distinguir a un ser humano de otro".[24]

En México, el marco regulatorio para la protección de datos personales no contempla los conceptos de "identificación biométrica", "dato biométrico" o "biometría". Sin embargo, el Instituto Nacional

[19] Superintendencia de Industria y Comercio, Delegatura para la Protección de Datos, Resolución N. 60460 de 2017; Resolución N. 43530 de 2018 ; Resolución N. 55405 de 2018.

[20] Cfr. Corte Constitucional, sentencia C-1011 del 16 de octubre de 2008, M.P. Jaime Córdoba Triviño, "Respecto a estos datos personales, la jurisprudencia propone dos modos de clasificación. La primera, relacionada con el nivel de protección del derecho a la intimidad, divide los datos entre información personal e impersonal, definiéndose la segunda como aquella que no reúne los requisitos mencionados anteriormente. (...) La siguiente gran tipología divide los datos personales con base en un carácter cualitativo y según el mayor o menor grado en que pueden ser divulgados. Así, se establece la existencia de información pública, semiprivada, privada y reservada." Estas dos clasificaciones paralelas fueron sostenidas también en la sentencia C-748 de 2011.

[21] Superintendencia de Industria y Comercio, Delegatura para la Protección de Datos, Resolución N. 60460 de 2017, disponible en: http://www.sic.gov.co/sites/default/files/files/Proteccion_Datos/201706046resolucion.pdf

[22] Consultas: N. 13-2733515 de 2014, N. 0171259 de 2018, N. 0297406 de 2018, y N. 0299565 de 2018.

[23] Superintendencia de Industria y Comercio, Oficina Jurídica, consulta N. 13-2733515 de 2014.

[24] Íbid.

de Transparencia, Acceso a la Información y Protección de Datos (INAI) publicó una guía para el tratamiento de datos biométricos en marzo de 2018.[25]

La guía establece un glosario de términos en donde define a la biometría como "método de reconocimiento de personas basado en sus datos biométricos", al dato biométrico como "propiedades físicas, fisiológicas, de comportamiento o rasgos de la personalidad, atribuibles a una sola persona y que son medibles", y al reconocimiento biométrico como "identificación o verificación de la identidad de una persona a partir de la comparación de plantillas biométricas". Además, brinda una mayor precisión al explicar el concepto de plantillas biométricas como la "representación alfanumérica de la información extraída de una o más muestras biométricas".

Para establecer estas definiciones, el INAI cita como fuentes el Dictamen 3/2012 del Grupo de Trabajo del Artículo 29 y el informe Privacy & Biometrics. Building a conceptual foundation (2006) del subcomité sobre biometría perteneciente al Consejo Nacional de Ciencia y Tecnología de los Estados Unidos.

El INAI determina que no siempre puede catalogarse a un dato biométrico como dato personal, pues según la legislación mexicana deben cumplirse dos condiciones: por un lado, el dato debe referir a una persona física, y por otra parte, debe identificar o hacer identificable a su titular. Recién en ese momento se lo considera un dato personal.

De esta manera el INAI sostiene que "si bien existen datos biométricos que por sí mismos identifican a una persona, por ejemplo, el rostro de una persona conocida; la mayoría de ellos requiere de un procesamiento o información adicional para que sea posible reconocer a su titular (...) tal es el caso de la huella dactilar", agregando también que "un dato biométrico aislado, que no pueda ser registrado en un sistema biométrico, ni se pueda vincular con un sujeto en lo particular o comparar con otras muestras, no podría considerarse un dato personal".

Asimismo, la guía establece que no todos los datos biométricos se consideran automáticamente sensibles bajo la legislación de datos personales y deben analizarse las condiciones de cada caso. Específicamente, cuando el dato se refiera a la esfera más íntima de su titular; que su uso en forma indebida pueda dar origen a discriminación; o que su uso ilegítimo conlleve un grave riesgo para su titular. En tal sentido, el INAI ejemplifica con casos de uso del iris y la huella dactilar.

Podemos entonces concluir que, en definitiva, la introducción de la biometría no ha sido correctamente delimitada en los países en estudio. Mientras que solo Brasil y Colombia tienen una mención expresa a los datos biométricos en sus leyes de protección de datos personales, únicamente se incorpora el término en referencia a los datos sensibles, mas no se profundiza sobre un concepto detallado, que determine a qué información biométrica se está haciendo referencia. Esta falta de precisión en

[25] INAI. Guía para el tratamiento de Datos Biométricos. Marzo 2018. Disponible en: http://inicio.ifai.org.mx/DocumentosdeInteres/GuiaDatosBiometricos_Web_Links.pdf

el uso de conceptos repercute en la manera de tratar el uso de la tecnología biométrica y de los datos biométricos, como veremos en las secciones siguientes.

III. Biometría e identidad: custodiando la puerta de entrada a tus derechos

En esta sección nos adentramos en el contexto sociopolítico y las realidades de los cuatro países, poniendo foco en los marcos normativos sobre los cuales se ha basado la introducción de políticas públicas sobre la identidad de las personas y el uso de tecnologías biométricas.

I. Argentina

En junio de 1966, la junta militar, autodenominada "Revolución Argentina", asumió el poder mediante un golpe de Estado. Al asumir, dictó un Estatuto de diez artículos que tenían preeminencia por sobre la Constitución Nacional. En su artículo quinto, el Estatuto arrogaba al presidente de casi todas[26] las facultades legislativas correspondientes al Congreso.

Ante una realidad donde las instituciones no funcionaban de la manera en que habían sido diseñadas y la participación ciudadana era inexistente, en este contexto fue dictado el Decreto-Ley 17.671 "de identificación, registro y clasificación del potencial humano nacional". La ley atribuye las funciones del Registro Nacional de las Personas (RENAPER) respecto del procedimiento para la identificación de todas las personas domiciliadas en territorio argentino y de todos los argentinos cualquiera sea el lugar donde residan.

Desde los avances de Vucetich, la sistematización del uso de huellas dactilares y la introducción del Documento Nacional de Identidad (DNI), los argentinos poco a poco fueron naturalizando su uso. La relación entre los ciudadanos y el Estado se construyó desde esa base, que luego fue ampliada hacia los actores privados. El mismo Registro Nacional de las Personas (RENAPER) promueve la emisión del DNI bajo la consigna de "la puerta de entrada a tus derechos", en referencia a la necesidad de contar con este documento para la realización de trámites ante el Estado, en donde prácticamente una persona no existe si no es por su número de DNI.

[26] "Con excepción de aquellas previstas en los arts. 45, 51 y 52 para los casos de juicio político a los jueces de los tribunales nacionales."

Centro móvil del RENAPER para la emisión del DNI.

La legislación sobre la cual está basado todo el sistema de identificación de la población se encuentra atravesada por una lógica y origen que arrastra la ideología de una dictadura militar, situación que nunca fue cuestionada política o judicialmente.

Si bien es importante resaltar los defectos de forma que tiene el surgimiento de esta norma, aún más revelador es cómo se aborda el tema de fondo, la identidad de las personas. En su mismo título, la ley se refiere a las personas como "potencial humano", lo que pone la lupa sobre la concepción misma del ser humano, visto por las instituciones del Estado como un activo o recurso a disposición para ser controlado y administrado.

En las cinco décadas posteriores a su sanción, el Decreto-Ley 17.671 fue utilizado por los diversos gobiernos democráticos como base para la ampliación de los sistemas de identificación de personas, justificando en el artículo 9 la legalidad de la implementación de tecnologías biométricas y procediendo, prácticamente en forma exclusiva, mediante decretos o resoluciones.

El artículo 9 establece que para proceder a la identificación de las personas, el RENAPER debe recolectar “el testimonio de su nacimiento, fotografías, impresiones dactiloscopia, descripciones de señas físicas, datos individuales, el grupo y factor sanguíneo”.

Así, por el Decreto 1501 de 2009, el RENAPER, organismo descentralizado bajo la órbita del Ministerio del Interior, autorizó el uso de tecnología biométrica para la emisión del DNI.[27] Posteriormente,

[27] Decreto 1501 de 2009, RENAPER, Ministerio del Interior.

con la Resolución 1474 de 2012 se introdujo el pasaporte biométrico.[28] En ambos casos, la principal justificación que se esgrime gira en torno a la autenticidad de los documentos que se emiten.

En noviembre de 2011, a través del Decreto 1766,[29] el gobierno nacional dió vida a SIBIOS, la mayor base de datos biométricos del país, centralizada en el Ministerio de Seguridad. Según el primer artículo del decreto, el objetivo del Sistema es "prestar un servicio centralizado de información respecto de los registros patronímicos y biológicos individuales, a los fines de contribuir a la comprobación idónea y oportuna en materia de identificación de personas y rastros, en procura de optimizar la investigación científica de delitos y el apoyo a la función preventiva de seguridad."

A partir de solicitudes de acceso a la información pública presentadas por la ADC en 2016 y 2017, el Ministerio de Seguridad estableció que los datos biométricos almacenados por SIBIOS son huellas dactilares, huellas palmares y registros de rostros.

Debido a que las bases de datos 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 RENAPER, como la autoridad de la depende la emisión del DNI y del pasaporte.

La tecnología detrás de este Sistema fue adquirida a dos empresas, por parte del Ministerio de Seguridad a la francesa Morpho Safran (actualmente denominada IDEMIA), y por el lado del Ministerio del Interior a la cubana DATYS.[30]

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 Policía Federal 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.

[28] Resolución 1474 de 2002, RENAPER, Ministerio del Interior.

[29] Decreto 1766 de 2011, Ministerio de Seguridad.

[30] "La identidad que no podemos cambiar", ADC, 2017.

Identificación biométrica por huella dactilar por la Policía Federal Argentina.

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

A comienzos de abril de 2017, mediante el Decreto 243,[31] se establece la ampliación de la invitación para adherirse a SIBIOS extendiéndose 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.

SIBIOS es usado tanto con fines criminales como civiles; el primero para la investigación científica de delitos y el segundo para la identificación de personas, por ejemplo, ante catástrofes naturales o accidentes, aunque sus aplicaciones se encuentran en constante expansión. Para utilizar la base de datos de SIBIOS, los usuarios no requieren de una orden judicial.

Al momento de su lanzamiento, el gobierno nacional produjo una campaña informativa bajo el slogan "Si nos conocemos mejor, nos cuidamos más", destacando cómo ciertos rasgos de las personas sirven para identificarlas indudablemente. El video con la propaganda de SIBIOS subraya la lógica de la prevención del delito y la suplantación de identidad, destacando que gracias a este Sistema "ahora vos, sos vos".[32]

Además de las bases de datos bajo la órbita del Ministerio de Seguridad y del Ministerio del Interior mencionadas previamente, hay otras dos iniciativas estatales que desarrollaron sus propias soluciones, una en el ámbito tributario y la otra en el de seguridad social.

[31] Decreto 243 de 2017, Ministerio de Seguridad.

[32] Video con la propaganda de SIBIOS disponible en: https://youtu.be/Pj6II4eazxE

En 2010, la Administración Federal de Ingresos Públicos (AFIP) emitió la Resolución General 2811 creando el Registro Tributario[33], bajo el cual como parte del proceso de inscripción y otorgamiento de la Clave Única de Identificación Tributaria (CUIT), además de la Clave Fiscal con Nivel de Seguridad 3, las personas deben proceder al registro digital de la fotografía de su rostro, su firma y su huella dactilar.

La Clave Fiscal es necesaria para poder realizar trámites ante la AFIP en forma online, como por ejemplo presentar declaraciones juradas, efectuar pagos, adherirse al Monotributo, solicitar la baja en impuestos o regímenes. Esto implica que un gran porcentaje de la población deba registrarse en su base de datos.

Propaganda de la ANSES sobre el programa Mi Huella.

En diciembre de 2014, la Administración Nacional de la Seguridad Social (ANSES), a través de la Resolución 648, comenzó el proceso de enrolamiento del programa "Mi Huella", mediante el cual estableció que los jubilados, pensionados y sus apoderados debían registrar sus huellas dactilares en el Sistema de Identificación Biométrica. El objetivo del programa es implementar la tecnología biométrica para dar fé de vida y cobrar los haberes previsionales.

La incorporación de tecnología biométrica en el ANSES encuentra su origen en la Resolución DE-N 567 de 2013. Posteriormente, el organismo se encargó de ampliar y perfeccionar la recolección, procesamiento y uso de datos biométricos exclusivamente a través de sus propias resoluciones.

[33] Resolución General 2811, 24 de abril de 2010, Administración Federal de Ingresos Públicos.

II. Brasil

La identificación de un ciudadano es considerada obligatoria para la provisión de beneficios sociales y el reconocimiento de diversos derechos. Debido a que los datos biométricos se encuentran fuertemente asociados al concepto de ciudadanía, esta es una de las razones por las cuales su recolección, para la emisión de documentos de identidad, nunca despertó una fuerte oposición. Las iniciativas de identificación promovidas por el Estado brasileño son vistas tradicionalmente en forma positiva por la mayoría de la población.[34]

Brasil cuenta con varios esquemas de identificación que incluyen más de diez tipos de números distintos y frecuentemente se sobreponen. Tal es el caso de la tarjeta de identificación ("RG"), la licencia de conducir ("CNH"), el registro para votar[35], el número que conecta a los brasileños con los servicios financieros ("CPF") y el pasaporte.

La Ley 7.116 de 1983 instituyó que los estados federales de Brasil ("Unidades Federativas") serían responsables de la emisión de las tarjetas de identificación ("RG") conteniendo la fotografía y huellas dactilares de los ciudadanos.[36] Esta estructura resultó en la descentralización de información dado que las Unidades no comparten los datos entre ellas[37], siendo posible para una persona obtener una identificación distinta en cada uno de los 27 estados del país.[38]

[34] Kanashiro, Marta Mourão. Biometria no Brasil e o Registro de Identidade Civil: novos rumos para identificação. 2011, p. 81.

[35] El voto es obligatorio en Brasil para los ciudadanos entre 18 y 70 años.

[36] El único documento necesario para emitir la tarjeta de identificación es el certificado de nacimiento, pero los procedimientos y el procesamiento de datos para la emisión son establecidos via actos administrativas por la autoridad estatal encargada de la identificación de personas.

[37] Akiyama, Thaís Gualda Carneiro; Almeida, Veronica Eberle de; Godri, Lucina; Guarido Filho, Edson Ronaldo. Organizações e Ambiente Legal: a construção do sistema de identificação civil brasileiro. RAM, Rev. Adm. Mackenzie, 16(6), Edición Especial, SÃO PAULO - SP, Nov./Dec. 2015, p.104.

[38] En un reportaje de investigación para "Folha de São Paulo", un periodista pudo obtener 9 tarjetas de identificación válidas. Debido a la falta de interoperabilidad, el periodista obtuvo una identificación en Belo Horizonte con su foto y huella dactilar pero haciendo uso del nombre de un colega. Disponible en: https://www1.folha.uol.com.br/cotidiano/2013/10/1355762-reporter-tira-carteira-de-identidade-em-9-estados.shtml

Investigación de Folha de São Paulo donde obtuvieron 9 cédulas de identidad en distintas Unidades Federativas de Brasil.

Desde 1997, Brasil viene tratando de implementar una credencial de identidad única. Luego de dos décadas con varios proyectos[39] de diferentes partidos, la Ley 13.444 del 2017 creó la Identificación Civil Nacional. De esta forma se estableció un único documento que concentraría información con datos cívicos, patronímicos y biométricos, incluyendo una fotografía y un chip, con la justificación de la prevención del fraude[40].

En el plan piloto para su implementación participaron funcionarios públicos del Tribunal Superior Electoral, a quienes se entregó una versión digital del documento en julio de 2018, alegando que recién un mes después comenzaría a implementarse a nivel nacional para todos los ciudadanos.[41] Sin embargo, recién en enero de 2019 se reportó la reanudación de las conversaciones sobre esta iniciativa entre los ministros del gobierno del presidente Jair Bolsonaro.[42]

[39] El "Registro de Identidade Civil" creado por el Presidente Fernando Henrique Cardoso, a través de la Ley 9.454 de 1997, intentó unificar la emisión de la tarjeta de identidad a lo largo de Brasil. No fue sino hasta 2010 que las primeras credenciales fueron emitidas durante la administración de la presidencia de Lula, pero luego de solo 14 mil credenciales emitidas por la Casa da Moeda, el proyecto fue abandonado y el contrato con la Casa no fue renovado. En 2015, la presidente Dilma Rousseff anunció el proyecto de ley 1.755/15, con el objetivo de crear el Registro Civil Nacional; el proyecto fue finalmente aprobado en 2017, durante el gobierno del presidente Michel Temer, con la Ley 13.444 y bajo el nombre Identificação Civil Nacional.

[40] Disponible en: http://www.casacivil.gov.br/central-de-conteudos/noticias/2017/maio/temer-sanciona-lei-da-identificacao-civil-nacional

[41] Disponible en: http://www.planejamento.gov.br/assuntos/tecnologia-da-informacao/documento-nacional-de-identidade/dni-1

[42] Disponible en: https://brasil.estadao.com.br/noticias/geral,aposta-de-moro-investigacoes-com-auxilio-de-dna-crescem-28-no-pais,70002668739

Desde 2003, el Tribunal Superior Electoral (TSE) implementó tecnología biométrica en el proceso de emisión de las credenciales de identificación para votar, justificándose en la necesidad de "garantizar un sistema de votación verdaderamente democrático y más seguro", añadiendo que la biometría no deja dudas respecto a la identidad de cada votante.[43]

Es importante resaltar que los datos biométricos recolectados por la Justicia Electoral –necesarios para el ejercicio de la ciudadanía y del voto obligatorio– han sido utilizados y compartidos con otras finalidades, especialmente para investigaciones criminales. Esto viene sucediendo a través de convenios y acuerdos de cooperación técnica, y en los términos del Decreto 8.789/16[44], pero sin transparencia, control público o medidas de seguridad, representando una violación significativa del principio de legalidad.

Urna electrónica usada en el proceso para la verificación de identidad por huella dactilar en las elecciones en Brasil.

Debido a que la Ley 7.444 de 1985 estableció las facultades normativas del Tribunal para determinar las instrucciones sobre el uso y procesamiento de la base de datos de la Justicia Electoral (artículo 9), el TSE se ha encargado de implementar tecnología biométrica en forma gradual mediante resoluciones administrativas.[45] En septiembre de 2018, el Supremo Tribunal Federal declaró válidas las reglas que autorizan la cancelación de las identificaciones de votación para aquellas personas que no hayan cumplido con el llamado obligatorio para el registro de sus datos biométricos.[46]

[43] Disponible en: http://www.tse.jus.br/imprensa/noticias-tse/2014/Fevereiro/recadastramento-biometrico-e-amparado-por-lei

[44] El Decreto 8.789 de 2016 trata del intercambio de bases de datos en la administración pública federal.

[45] Resolução-TSE no. 21.538/2003, no. 22.688/2007, no. 23.061/2009, no. 23.335/2011, no. 23.345/2011 y no. 23.366/2011.

[46] Supremo Tribunal Federal, Arguição de Descumprimento de Preceito Fundamental (ADPF) 541, caso reportado por el juez Luís Roberto Barroso, 26 de septiembre de 2018. Disponible en: http://www.stf.jus.br/portal/cms/verNoticiaDetalhe.asp?idConteudo=390875

Las licencias de conducir, por su parte, también son un documento nacional de identificación válido, pero con una base de datos integrada, mediante el Registro Nacional de Carteiras de Habilitação (RENACH), organismo creado por la Ley 9.503 de 1997 (código de tránsito brasileño). El RENACH mantiene una base de datos para todo el país en el Departamento Nacional de Tránsito y otras ubicadas en las oficinas de cada estado, las cuales se encuentran interconectadas de manera en constante.[47] En 2017, mediante la resolución administrativa 684/17, se estableció que para la emisión y renovación de las licencias se procedería al registro de la fotografía, las huellas dactilares y la firma de las personas solicitantes.

En definitiva, la recolección y procesamiento de datos biométricos en Brasil es regulada por resoluciones, provisiones y ordenanzas, así como también acuerdos de cooperación y contratos. Al innovar el orden legal, creando derechos, obligaciones, castigos y prohibiciones, estos actos regulatorios parecen desafiar el principio de legalidad, establecido en el artículo 5 apartado II de la Constitución.

III. Colombia

"La biometría es el método ideal de identificación humana", sostiene la Registraduría Nacional del Estado Civil (RNEC)[48]. Esta afirmación sobre la certeza de métodos científicos y técnicos para configurar la identidad de una persona a partir de sus características físicas, está atravesada por la forma en la que entendemos al Estado y en la que la ciudadanía puede acceder a servicios públicos.

Colombia inició el proceso de recolección de datos biométricos de la ciudadanía en dos esfuerzos diferenciados, que terminaron confluyendo en el siglo XXI. Por un lado se encuentra la base de datos criminal que, al igual que otros países del mundo, se introdujo a principios del siglo XX, tomando huellas dactilares, medidas antropométricas y fotografías de los criminales.[49] Por otro lado, el Departamento Nacional de Identificación, en un intento por luchar contra los fraudes electorales, empezó a proveer Cédulas de Ciudadanía que incluían datos antropométricos, una fotografía y la huella del índice derecho en 1934.[50]

En 1948, en medio de una crisis de institucionalidad y violencia partidista, se expidió la Ley 89 para reformar el sistema electoral, creando un organismo independiente de los partidos que administrara las elecciones. En esta ley se incluyó el requerimiento de contratar una misión extranjera de países del Norte global para que ayudara a "dictaminar acerca de los sistemas que deban emplearse en la

[47] Más información disponible en la web del RENACH.

[48] Registraduría Nacional del Estado Civil, "La biometría: método ideal de identificación humana". Disponible en: https://www.registraduria.gov.co/La-biometria-metodo-ideal-de.html

[49] Alzate, Juan David, Entre rostros y huellas. Una aproximación a los procedimientos aplicados a la investigación judicial por homicidio en Medellín-Colombia (1900-1930). TRASHUMANTE | Revista Americana de Historial Social, (2013): 32-55.

[50] Decreto 944 de 1934.

identificación y cedulación"[51].

Dos años después, llegó al país una misión canadiense que hizo una serie de recomendaciones que incluían la adopción del sistema dactiloscópico "Henry" y la puesta en marcha de un archivo centralizado microfilmado de las huellas dactilares.[52] A partir del informe de dicha misión, en 1951 se adoptó el Decreto 2628 para iniciar la impresión de las nuevas cédulas.[53] El proceso de consolidación de la base de datos de identidad nacional se dio con la Ley 39 de 1961, que convirtió a la Cédula en un requerimiento para "todos los actos civiles, políticos, administrativos y judiciales"[54]. Con esta Ley se inició un proceso que mezcló el registro de la ciudadanía para reclamar sus derechos con la recolección y clasificación de sus datos biométricos.

En 1970, con el Decreto 1260, la RNEC quedó a cargo de la producción de las cédulas y la recolección de datos.[55] El cambio del archivo a formato digital inició en 1997 con el Proyecto de Modernización Tecnológica que trató de aumentar los estándares de seguridad de las cédulas anteriores y buscó digitalizar los datos de la Registraduría y las bases de datos biométricas. El procedimiento se realizó en dos fases y la RNEC lo hizo con el apoyo de la multinacional francesa Morpho SAFRAN (actualmente denominada IDEMIA[56]).[57]

La primera fase, desarrollada entre 1997 y 2005, implicó la preparación de los datos de la Registraduría para instalar un Sistema Automatizado de Identificación Dactilar (AFIS, por sus siglas en inglés). En tanto que en la segunda fase (2005 - 2010) se extendió la base de datos a las personas que tenían los anteriores modelos de la cédula y se terminó el sistema AFIS con un servicio web que permitía su implementación en los sectores público y privado.[58] Igualmente, en 2008 comenzó la emisión de la tarjeta de identidad biométrica a menores de edad, para incluirlos en las bases de datos de la Registraduría[59]. En 2010, los antiguos formatos perdieron validez y se completó la transferencia del sistema, consolidando la base de datos biométricos más grande del país con un índice de indocumentación del 10 por ciento[60].

[51] Ley 89 de 1948.

[52] Es curioso señalar que Canadá no contaba en su momento, ni en la actualidad, con un sistema de credenciales nacionales de identificación.

[53] Decreto 2628 de 1951.

[54] Ley 39 de 1961.

[55] Decreto 1260 de 1970.

[56] https://en.wikipedia.org/wiki/IDEMIA

[57] Martins, Alexandre, The Colombian Identification System Implementation and technological advancement of the civil identification and registration systems. Keesing Journal of Documents & Identity, (2013): 25-28.

[58] Ibídem.

[59] Registraduría Nacional del Estado Civil. «Historia de nuestra cédula de ciudadanía.» Nuestra huella - Revista Electrónica Mensual, (2012)

[60] Banco Interamericano de Desarrollo, Inventario de los registros civiles e identificación de América Latina y el Caribe. (Washington: BID, 2010), 14.

Cédulas de ciudadanía emitidas por la RNEC en Colombia.

En 2011, con el Decreto 4057, se suprimió el Departamento Administrativo de Seguridad (DAS) y se transfirieron sus funciones de registro a la Policía Nacional.[61] Finalmente, ese mismo año, por medio del convenio interadministrativo No. 3, se suscribió un acuerdo de cooperación entre la RNEC y la Policía que permitiría el uso del servicio web para reducir el tiempo de consulta. De esta forma, los registros criminales terminaron confluyendo con los registros civiles en la base de datos biométrica de la Registraduría.

Después de la consolidación de la base de datos biométricos de la Registraduría, se inició un proceso de automatización e interoperabilidad de la identidad digital en el Estado. Así, con el Decreto 19 de 2012, con el fin de hacer más eficiente al Estado, se permitió el uso de la verificación electrónica de la huella dactilar para los trámites y actuaciones frente a entidades y particulares en actividades administrativas.[62] Este decreto abrió la posibilidad de utilizar la base de datos biométrica de la Registraduría para identificar a una persona en cualquier relación con el Estado.

Posteriormente, con la Ley 1753 de 2015, se ampliaron los espacios en que se requeriría la verificación biométrica y se consolidó el camino para interoperar la base de datos biométrica de la RNEC y asentarla como un requisito básico de la vida ciudadana. Por un lado, convirtió en obligatoria la verificación biométrica de las personas dentro del sistema de seguridad social (salud, pensión y riesgos laborales). Además, la Ley instó a cualquier entidad pública y a privados con funciones

[61] Decreto 4057 de 2011.

[62] Decreto 019 de 2012, artículo 18.

públicas a verificar la identidad ya fuese por medio de su propia infraestructura o utilizando uno de los operadores seleccionados por la Registraduría para este fin.[63] Por otro lado, la Ley abrió la posibilidad de que las instituciones financieras y aseguradoras utilizaran la base de datos para identificar a las personas, pagando un monto determinado por la Registraduría.[64]

Las tendencias que dejó esta ley se institucionalizaron con la Resolución 5633 de 2016, que reglamentó las condiciones y procedimientos para el acceso a las bases de datos de la Registraduría. En primer lugar, cualquier entidad y particular que cumpla funciones públicas puede pedir acceso a la base de datos por medio de una solicitud y cumpliendo con los requerimientos técnicos para utilizarla. En segundo lugar, se reguló la posibilidad de que los privados suscriban acuerdos con la Registraduría para acceder a la autenticación biométrica por medio de pagos a la RNEC.[65] Y por último, se determinaron los requisitos técnicos que habilitaron a que los operadores pueden cobrar para ofrecer los servicios tecnológicos a entidades o particulares interesados en la autenticación de las personas.[66]

Policía Nacional de Colombia utilizando identificación biométrica por huellas dactilares.

Verificar la identidad de una persona en las bases de datos de la RNEC, a través de la biometría, es una forma de tratamiento de datos biométricos. Sin embargo, en los casos donde por mandato legal la biometría sirve para establecer la identidad, se puede producir una situación en la que solo pueden

[63] Ley 1753 de 2015.

[64] Íbid, artículo 159.

[65] Resolución N. 5633 de 2016, artículo 33.

[66] Íbid.

negarse a entregar estos datos bajo la condición de renunciar al servicio o beneficio, haciéndose inaplicable lo establecido en el Decreto 1377 de 2013, en el sentido de que ninguna actividad estará condicionada a la entrega de datos sensibles.

Los casos de uso de biometría para verificar la identidad de una persona muestran, por lo tanto, un contraste entre el régimen de protección de datos y la creación y uso de bases de datos biométricas estatales.

La Corte Constitucional se ha pronunciado en varios casos en donde la huella digital se usa para suplir la falta del documento de identidad. En uno de ellos, una persona solicitó la protección del derecho a la vida y la salud frente a la decisión de su empresa prestadora de salud de negarse a entregar los medicamentos que necesitaba para la enfermedad de Parkinson. Para reclamar el medicamento, la empresa de salud exigía que se verifique la identidad del beneficiario con su huella digital. En la práctica, esto resulta en la negación del acceso al servicio de salud porque la persona no podía desplazarse hasta el lugar donde entregaban el medicamento por el estado avanzado de la enfermedad y, en su lugar, enviaba a una persona de confianza para reclamarlo. En esa ocasión, dijo la Corte:

> Para la Sala es factible que SaludCoop E.P.S. exija que fármacos como los relacionados en el presente caso, sean reclamados por la persona directamente afectada, pues así se evitan fraudes, malos usos o destinación indebida. Sin embargo, dichas reglas de cuidado no pueden aplicarse desconociendo las circunstancias del caso concreto, como quiera que en ocasiones como la actual, la persona aún necesitando los medicamentos no puede reclamarlos personalmente viéndose impelida a autorizar a un tercero para que, en su representación, exija su entrega a la E.P.S. respectiva.[67]

En una decisión que sintetiza las relaciones entre identidad y biometría frente a distintos registros estatales, la Corte Constitucional consideró que ser titular de un derecho es distinto a la forma de acreditar la identidad. Por esto, se deben flexibilizar las formas para realizar esa acreditación en el marco de la modernización, simplificación y eliminación de trámites y también considerando los "avances científicos y tecnológicos" en relación con la identidad. Concretamente, la Corte afirmó que "los medios de identificación personal no son sistemas estáticos. Por el contrario, estos deben actualizarse en consonancia con los avances científicos y tecnológicos sobre la materia para lograr mayor seguridad, fiabilidad y eficacia en los procesos de individualización, guardando siempre respeto por la dignidad humana y demás garantías constitucionales."[68]

Con los movimientos recientes de la RNEC, es claro que la concepción de la identidad está cambiando. Por una parte, en un intento por hacer más seguro y moderno el proceso de identificación, se están

[67] Corte Constitucional, sentencia T-312 del 4 de abril de 2008, M.P. Rodrigo Escobar Gil.

[68] Corte Constitucional, sentencia T-1000 del 26 de noviembre de 2012, M.P. Jorge Iván Palacio Palacio.

recolectando datos biométricos de la población cada vez más sensibles, a la vez que se contratan costosos sistemas que buscan automatizar los procesos. Así, la relación de la ciudadanía con el Estado se vuelve más dependiente de la plena identificación, obligando a todas las instituciones públicas a implementar costosas tecnologías o una contratación con un tercero, inclusive, en zonas sin infraestructura para su funcionamiento.

Por otra parte, la RNEC se está convirtiendo en un administrador de la identidad biométrica de la población, al cobrar a los privados, interesados en tener la certeza de individualidad (en su mayoría compañías financieras), por los datos personales sensibles de la ciudadanía.

En primer lugar, una base de datos biométricos, pensada para la identificación de votantes solo para las elecciones, se convirtió en un registro civil requerido para que la ciudadanía se relacione con el Estado al reclamar sus derechos, ampliando la base de sujetos susceptibles al proceso de recolección de datos biométricos. En segundo lugar, la base de datos biométricos que, a principios del siglo, estaba reservada para "poblaciones indeseadas" como las personas con procesos criminales se terminó uniendo con los registros civiles. En tercer lugar, la base de datos destinada para el registro civil frente al Estado se convirtió en un prerrequisito para acceder a los derechos básicos de la ciudadanía, una herramienta de la fuerza pública y un mecanismo de individualización e identificación frente a los privados.

IV. México

La reforma a la Ley de Población, realizada en 1992, obligaba a los ciudadanos mexicanos a registrarse ante el Registro Nacional de Población (RENAPO), manejado por la Secretaría de Gobernación, para obtener una cédula de identificación que contenía, además de los datos patronímicos, la huella dactilar del titular. Toda la información correspondiente a los titulares serían ligada a la Clave Única del Registro de la Población (CURP) y alojada en una base de datos centralizada.

En 2011, mediante un decreto presidencial, la Secretaría de Gobernación modificó el Reglamento de la Ley de Población para agregar la recolección de más información biométrica. A los datos ya existentes –huella dactilar y firma[69]–, se añadió el iris de los dos ojos, las diez huellas digitales y la fotografía biométrica.[70] El Instituto Federal de Acceso a la Información (ahora Instituto Nacional de Acceso a la Información o INAI) criticó la ampliación en el tratamiento de datos biométricos por ir en contra del principio de finalidad, alegando que con la verificación de las huellas digitales el proceso de identificación contaba con el 99 % de confiabilidad.[71] Además, la Comisión Nacional de Derechos

[69] Artículo 107 de la Ley General de Población.

[70] Decreto Presidencial por el que se reforman y adicionan diversas disposiciones del Reglamento de la Ley General de Población publicado en el Diario Oficial de la Federación el 19 de enero de 2011. Disponible en: http://dof.gob.mx/nota_detalle.php?codigo=5174983&fecha=19/01/2011

[71] IFAI. RDA 310/12.

Humanos (CNDH) solicitó la adopción de medidas precautorias que protegieran los derechos de los menores de edad registrados.[72]

A pesar de las críticas, el programa de registro continuó como se había estipulado, logrando recolectar los datos biométricos de alrededor de 6 millones de menores de edad. Entre tropiezos y asignaciones opacas de presupuesto,[73] el programa fue suspendido después de que se invirtieron más de cuatro mil millones de pesos mexicanos entre los mandatos de los expresidentes Felipe Calderón y Enrique Peña Nieto, entre 2006 y 2018.[74] La actual administración no tiene planes para darle continuidad al programa de la cédula de identidad del RENAPO.[75]

Centro de registro del Instituto Nacional Electoral en México.

Como lo determina el transitorio cuarto de la reforma a la Ley de Población, ante la falta de una cédula de identidad ciudadana (como a la que apuntaba RENAPO) la credencial emitida por

[72] El Informador. "Acepta Segob recomendaciones de la CNDH para la cédula". Informador.mx. 12 de febrero de 2011. Disponible en: https://www.informador.mx/Mexico/Acepta-Segob-recomendaciones-de-la-CNDH-para-la-cedula-20110212-0124.html

[73] Sánchez, Eduardo. "Armenta, uno de los responsables del fracaso del Renapo". Exclusivas Puebla. 7 de junio de 2018. Disponible en: http://exclusivaspuebla.com.mx/armenta-uno-de-los-responsables-del-fracaso-del-renapo/

[74] Redacción Quehacer Político. "Calderón y Peña tiraron más de 4 mil millones en una credencial única... que nunca se concretó". Quehacer Político. 8 de diciembre de 2018. Disponible en: http://quehacerpolitico.mx/calderon-y-pena-tiraron-mas-de-4-mil-millones-en-una-credencial-unica-que-nunca-se-concreto/

[75] Sánchez, Enrique. "Descartan continuidad de Cédula de Identidad Ciudadana", Excelsior, 22 de enero de 2019. Disponible en: https://www.excelsior.com.mx/nacional/descartan-continuidad-de-cedula-de-identidad-ciudadana/1291866

el Instituto Nacional Electoral (INE), utilizada en procesos electorales para evitar fraudes, puede funcionar como medio de identificación personal en aquellos trámites administrativos en los que exista un convenio entre la autoridad electoral y las demás autoridades y actores del sector privado.[76]

Entre 1992 y 2016, el INE celebró 102 convenios de apoyo y colaboración con diversas autoridades locales, federales y con entidades públicas, con el fin de habilitar el uso de la credencial electoral como medio de verificación de identidad.[77] En 2013, se firmó un convenio "piloto" de este tipo con Banamex, uno de los mayores bancos de México. Dos años después, por solicitud del INE, el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI) emitió una opinión sobre la aplicación del Servicio de Verificación de datos de la Credencial para Votar.[78]

v. Tendencias

El recorrido realizado a lo largo de los marcos normativos de los países en estudio nos permiten brindar claridad a los puntos en común que surgen de la manera en que se ha introducido el uso de tecnologías biométricas y de los datos biométricos.

La inserción de derechos, obligaciones, castigos y prohibiciones mediante decretos y resoluciones desafían el principio de legalidad. En donde debería existir un debate legislativo, abierto y transparente, que incluya la voz de la ciudadanía y las preocupaciones de los expertos, encontramos políticas promovidas sin estudios ni análisis previos, bajo lógicas poco democráticas.

El vínculo entre la identidad y las personas, como algo de lo que el Estado se encuentra en su derecho para disponer y administrar, vislumbra una lógica de control, en la que las instituciones públicas pueden gobernar a la población como recursos. Esto se vuelve más evidente cuando el otorgamiento de beneficios o servicios sociales está condicionado a la entrega de datos biométricos, sin posibles alternativas, profundizando a su vez la desigualdad social.

IV. Aplicaciones de la biometría en la vida diaria

Teniendo en cuenta los marcos normativos analizados previamente, en esta sección exploramos distintos casos de estudio que resultan claros para evidenciar cómo se van consolidando las narrativas sobre la identidad de las personas y el uso de los datos biométricos para los más diversos fines.

[76] https://www.ine.mx/credencial/

[77] Consejo General del Instituto Nacional Electoral. INE/CG92/2016. 12 de abril de 2016. Diario Oficial de la Federación. Disponible en: http://dof.gob.mx/nota_detalle.php?codigo=5432730&fecha=12/04/2016

[78] IFAI/CPDP/0022/15.

I. Argentina

Como expusimos en la sección anterior, la introducción de tecnología que utiliza datos biométricos fue permeando la vida civil de manera exponencial. Actualmente, los argentinos se ven obligados al uso de sus huellas dactilares y rostro en diversos ámbitos con múltiples fines. En seguridad pública, bajo la excusa de la lucha contra el delito y el fraude. En seguridad social, por motivos de evitar la suplantación de identidad y publicitado como un sistema ágil, seguro, efectivo, confiable y sencillo. En el sistema tributario. En el ámbito educativo, para controlar el presentismo del cuerpo docente. En el ámbito electoral, para validar la identidad de votantes bajo la justificación del combate a la "migración electoral transfronteriza"[79]. En los eventos deportivos, para controlar el ingreso a los estadios de fútbol.[80]

Hacia mediados de 2018, el Ministerio del Interior y la Secretaría de Modernización (en su momento conformada como ministerio) anunciaron la puesta en funcionamiento de un proyecto conjunto denominado Sistema de Identidad Digital (SID), con el objetivo de simplificar y agilizar los trámites que realizan las personas con el Estado, permitiendo validar la identidad mediante el uso de reconocimiento facial.

Propaganda del Ministerio del Interior y la Secretaría de Modernización sobre el Sistema de Identidad Digital.

[79] Ver: "Prueba biométrica en las PASO: la Cámara Electoral respondió a ADC", 18 de octubre de 2017, disponible en: https://adcdigital.org.ar/2017/10/18/prueba-biometrica-las-paso-la-camara-electoral-respondio-adc/ y "¿Es necesario un sistema de identificación biométrica electoral?", 7 de noviembre de 2017, disponible en: https://adcdigital.org.ar/2017/11/07/es-necesario-un-sistema-de-identificacion-biometrica-electoral/

[80] Para mayor información sobre cada ámbito referirse al informe "Cuantificando identidades en América Latina", ADC, 2017.

El SID se ubica dentro del marco de acción de la actual administración nacional que busca promover la digitalización y actualización tecnológica del Estado, poniendo a las entidades públicas al servicio del ciudadano. En este contexto, en diciembre de 2017, Interior y Modernización firmaron el acuerdo de cooperación que luego daría vida al SID.

El marco jurídico esgrimido por el Estado para justificar al SID y la introducción de la biometría como un modo de identificación legalmente válido, son los artículos 9 y 11 de la Ley 17.671 y su reglamentación con el artículo 1 del Decreto 1501/09, que según vimos en las secciones anteriores de este informe entendemos que son insuficientes bajo un análisis de legalidad y derechos humanos.

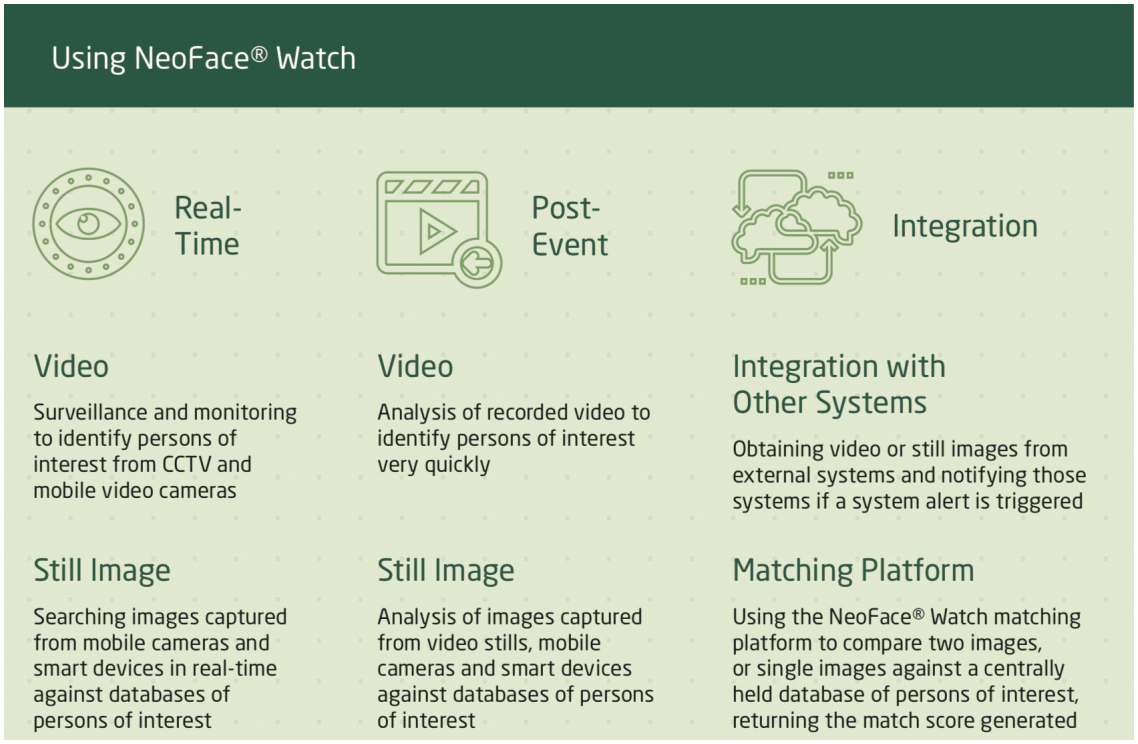
En marzo de 2018, la Secretaría de Gobierno Digital, bajo la órbita de Modernización, efectuó la adjudicación directa para la adquisición del software de reconocimiento facial a la empresa NEC Argentina S.A., filial de la multinacional de origen japonés con base en Tokio, por un total de 834.403,90 dólares estadounidenses, según surge del acta de negociación a la cual accedió la ADC tras una solicitud de acceso a la información pública.

La solución adquirida a NEC fue NeoFace Watch[81], la cual se implementó directamente en el RENAPER para utilizar la base de datos de rostros ya existente.

De acuerdo con la información provista por su fabricante, NeoFace Watch funciona de la siguiente manera: Una vez que obtiene las imágenes faciales provenientes de videos, fotografías o sistemas de terceros integrados, el algoritmo analiza los cuadros individuales de los videos o las imágenes para detectar rostros e individualizar los rasgos faciales de cada persona. Luego crea una pequeña plantilla para cada cara y la compara con los registros disponibles en la base de datos sobre la cual se implementó, hasta que encuentra una coincidencia. El sistema puede almacenar un historial de las coincidencias encontradas y admite ser configurado para emitir alertas en tiempo real.[82]

[81] https://www.nec.com/en/global/solutions/safety/face_recognition/NeoFaceWatch.html

[82] Folleto publicitario de NEC sobre el software NeoFace Watch.



Descripción de la empresa NEC sobre las facultades de su software de reconocimiento facial NeoFace Watch.

NEC declara tener una alta tasa de coincidencia, incluso con imágenes de muy baja resolución o que tengan cambios en las variables ambientales (como la luz, la posición del rostro, accesorios que use la persona, etc.).

En principio, el SID es un servicio a disposición de las entidades estatales y las empresas del sector privado, que se formaliza con el alta desde la plataforma de Trámites a Distancia[83], pudiendo elegir entre tres tipos de paquetes para validar distinto tipo de información que tiene el RENAPER.

El primer paquete del servicio le va a solicitar una foto del frente y dorso del DNI, además de la foto de su rostro con fé de vida[84]; el segundo paquete le va a solicitar a la persona que ingrese los números del DNI y su género, luego le va a solicitar la foto de su rostro[85]; por último, el tercer paquete solo solicita el número del DNI, género y número del trámite en cuestión[86]. Las tarifas para la verificación de estos datos son establecidas por el RENAPER y fue actualizado por última vez en julio de 2018 con la Resolución 430.[87]

La empresa u organismo puede implementar el SID de tres maneras[88]:

[83] https://www.argentina.gob.ar/sid/adherir
[84] https://www.argentina.gob.ar/sid/modalidades-y-productos/paquete1
[85] https://www.argentina.gob.ar/sid/modalidades-y-productos/paquete2
[86] https://www.argentina.gob.ar/sid/modalidades-y-productos/paquete3
[87] Resolución 430/18, Ministerio del Interior.
[88] https://www.argentina.gob.ar/sid/tecnologias-soportadas

1. Utilizando la interfaz de programación de aplicaciones (API[89], por sus siglas en inglés) desde una página web o app móvil.

2. Integrarla directo en su app mediante el kit de desarrollo de software (SDK[90], por sus siglas en inglés) provisto, disponible para Android y iOS.

3. Vincular el proceso a la app del RENAPER mediante un código QR o link, la cual luego realiza el proceso de identificación biométrica por separado.

Desde el lado de las personas que utilizarán los servicios que implementen el SID, al momento de comenzar a hacer un trámite desde su smartphone o tablet se les solicita una foto de su rostro, esta información es enviada al RENAPER para contrastarlo con su base de datos y devolver a la empresa u organismo de esa app un resultado de "hit" o "no hit", es decir si hubo o no coincidencia en los datos. Es por esto que, ante el cuestionamiento de la ADC, el RENAPER argumenta que no existe una transmisión de los datos biométricos de su parte.

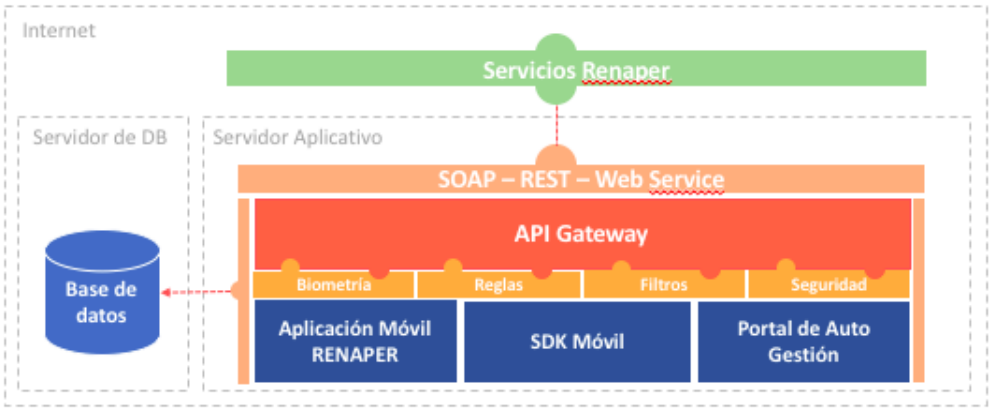


Gráfico elaborado por el Ministerio del Interior y la Secretaría de Modernización sobre la arquitectura del SID.

A septiembre de 2018, el RENAPER registró 116 entidades públicas y privadas interesadas en el uso del SID, según surge del pedido de acceso a la información pública presentado por la ADC. De ellas, 47 entidades realizaron un total de 14.452 pruebas de su funcionamiento en un ambiente de desarrollo (no productivo), sumado a las 10535 pruebas llevadas a cabo por RENAPER.

En la respuesta brindada por Modernización al pedido de información presentado por la ADC, se aclara que sostuvieron una reunión en abril de 2018 con los representantes de la Agencia de Acceso a la Información Pública y la Dirección General de Tecnología de la Información del RENAPER, con el objetivo de recibir sus consideraciones sobre la compatibilidad del SID con la ley vigente de protección de datos personales.

[89] https://es.wikipedia.org/wiki/Interfaz_de_programaci%C3%B3n_de_aplicaciones
[90] https://es.wikipedia.org/wiki/Kit_de_desarrollo_de_software

El principal sector que busca promover la implementación del SID es el de los servicios financieros, específicamente las empresas catalogadas como fintech, donde se destacan las plataformas de pagos móviles y los bancos digitales. A través de la Mesa de Innovación del Banco Central, que reúne a los principales actores públicos y privados en la materia, se permitió a los miembros implementar un proceso de prueba.

A pesar de esto, el mismo discurso del Estado Argentino apunta a la expansión del Sistema de Identidad Digital hacia una multiplicidad de sectores, servicios y ámbitos, posicionándolo como la nueva herramienta en la interacción de las personas con organismos públicos y privados.

II. Brasil

En años recientes, argumentos en torno a la seguridad pública comenzaron a permear el debate, a medida que se incrementó la adopción de tecnologías de vigilancia en servicios públicos y políticas afines.

En marzo de 2015, el gobierno del Estado de Rio de Janeiro anunció medidas para la implementación de una tarjeta de transporte que registre las huellas dactilares de las personas usuarias.[91] Al mismo tiempo, mediante la Asamblea Legislativa de Río de Janeiro aprobó el uso de identificación biométrica mediante reconocimiento facial en los autobuses.[92] La implementación tecnología biométrica en el sistema de transporte es producto de colaboraciones público-privadas.[93]

[91] Disponible en: http://www.rj.gov.br/web/setrans/exibeconteudo?article-id=2383637

[92] Ley 7.123 del 8 de diciembre de 2015. Disponible en: https://chupadados.codingrights.org/wp-content/uploads/2016/11/Lei_7123_Controlebiometrico.pdf

[93] Más información en "RioCard: concentración de datos y dinero en el transporte público", disponible en: https://chupadados.codingrights.org/es/com-o-riocard-seus-dados-passeiam-pelo-rj-e-ninguem-sabe-onde-vao-descer-2/

En 2016, el Instituto Nacional de Estudios e Investigación Educativa (Instituto Nacional de Estudos e Pesquisas Educacionais Anísio Teixeira, o Inep), una agencia federal vinculada al Ministerio de Educación, anunció la recolección de las huellas dactilares de estudiantes que tomaran el Examen Nacional de la Enseñanza Media (ENEM)[94]. En la última década, su relevancia se fue incrementando debido a que múltiples universidades federales e institutos educativos utilizan el ENEM como una prueba de admisión.

El Inep el comunicado Edital ENEM 2016 en el Boletín Oficial, estableciendo que empezaría la recolección de datos biométricos de los participantes en el día de los exámenes.[95] Al año siguiente, mediante el Edital ENEM 2017, el Inep estableció que "el participante que se niegue, injustificadamente, a la recolección del dato biométrico será eliminado del Examen"[96]. Las mismas medidas fueron impuestas para la edición 2018.[97]

La lógica seguida por el Inep para justificar esta iniciativa es revestir de mayor seguridad al proceso del Examen. Según la presidente del Inep, Maria Inês Fini, gracias a la base de datos de huellas dactilares de la Policía Federal, pueden asegurarse si los participantes son quienes dicen ser. Sin embargo, no se brindaron mayores detalles sobre el procesamiento de los datos biométricos, qué sería considerado como una negativa justificada a otorgar la huella dactilar, o cómo se procedería a la recolección de dichos datos.

Desde el 2010, han habido frecuentes reportes sobre casos de fraude y filtración de información sobre el ENEM.[98] Sin embargo, los casos de fraude se han relacionado a trampas y a la transmisión electrónica de respuestas a los participantes[99], los casos en donde otras personas se hacen pasar por los estudiantes que toman el examen son extremadamente raros.

En noviembre de 2018, el Consejo Nacional de Justicia (CNJ) anunció un programa que implementa tecnología biométrica para el registro de las personas en prisión, además de la actualización y emisión de documentos personales como el número de seguridad social ("CPF") o el certificado de nacimiento.

[94] "MEC fará cadastramento biométrico surpresa no Enem", O Globo, 14 de abril de 2016, disponible en: https://oglobo.globo.com/sociedade/educacao/enem-e-vestibular/mec-fara-cadastramento-biometrico-surpresa-no-enem-19085113

[95] Diário Oficial da União (DOU), 15 de abril de 2016.

[96] Diário Oficial da União (DOU), 10 de abril de 2017.

[97] Diário Oficial da União (DOU), 21 de marzo de 2018.

[98] Luego de la investigación sobre la filtración de información no se han publicado conclusiones al respecto ni impuesto sanciones a los responsables. http://g1.globo.com/educacao/noticia/2010/08/vazamento-de-dados-de-estudantes-do-enem-sera-apurado-diz-inep.html

[99] Disponible en: https://www1.folha.uol.com.br/educacao/2018/04/estudo-inedito-indica-alta-chance-de-fraude-em-mil-provas-do-enem.shtml

El presidente del CNJ y el juez de la Corte Suprema, Dias Toffoli, remarcaron la importancia de asegurar la ciudadanía a las personas encarceladas, estableciendo que "la mayoría no tienen siquiera un certificado de nacimiento", lo que conecta la narrativa entre ciudadanía y la seguridad pública.[100] La Procuradora General de Brasil, Raquel Dodge, justificó el programa bajo una cuestión de debido proceso, argumentando que "las personas bajo custodia deben ser identificadas y el Estado debe conocer su delito, si son reincidentes, dónde se encuentran, y cómo están cumpliendo sus condenas".[101]

En enero de 2019, la oficina de prensa de la ciudad de Río de Janeiro publicó un comunicado anunciando la implementación de software de reconocimiento facial para vigilar las multitudes durante el Carnaval en el mes de marzo, comenzando en la ciudad de Copacabana[102]. Según el Secretario de Estado del Departamento de Policía Militar, coronel Rogério Figueredo de Lacerda, el objetivo fue permitir que las autoridades vigilen las festividades de forma remota e identifiquen a las personas con órdenes de detención, registros policiales y personas desaparecidas.[103]

III. Colombia

Los principales organismos estatales que operan bases de datos biométricos son la RNEC, la Policía Nacional y Migración Colombia.

Como se mencionó en la sección anterior, a partir de la publicación del Plan Nacional de Desarrollo (2010 - 2014), se abrió la posibilidad de utilizar las bases de datos generadas por entidades públicas, y particulares en ejercicio de funciones públicas, de forma "permanente y gratuita" por otras entidades que lo requieran para los programas y proyectos de ese Gobierno.[104]

[100] Disponible en: http://www.cnj.jus.br/noticias/cnj/87773-biometria-e-digitalizacao-vao-melhorar-justica-criminal

[101] Además, el ministro de Justicia y Seguridad Pública, Sérgio Moro, presentó al plenario de la Cámara de Diputados el Proyecto de Ley 882/2019, parte de su propuesta de medidas anticrimen. Entre las medidas contenidas en el proyecto se encuentra la creación de un Banco Nacional Multibiométrico y de Impresiones Digitales, con datos cosechados "en investigaciones criminales o con ocasión de la identificación criminal" para subsidiar investigaciones criminales.

[102] Disponible en: http://www.pmerj.rj.gov.br/2019/01/policia-militar-vai-implantar-programa-de-reconhecimento-facial-e-de-placa-de-veiculos/

Según un portavoz, el proyecto no tendrá ningún costo inicial, ya que la empresa de telecomunicaciones responsable del software tiene un contrato vigente con las agencias de seguridad para instalar programas de comunicación en los vehículos de la policía. "La empresa Oi ya es un contratista estatal. Este costo ya se agregó a los servicios que Oi proporciona al estado. Esto es en realidad el tráfico de datos". Si se aprueba, el proyecto piloto servirá de base para un futuro acuerdo de licitación, con la posibilidad de participación de otras empresas. Disponible en: http://agenciabrasil.ebc.com.br/geral/noticia/2019-01/rio-programa-de-reconhecimento-facial-entra-em-operacao-no-carnaval

[103] "PM anuncia que vai começar a usar programa de reconhecimento facial e de placas de veículos no carnaval", Globo, 30 de enero de 2019, disponible en: https://g1.globo.com/rj/rio-de-janeiro/carnaval/2019/noticia/2019/01/30/pm-anuncia-que-vai-comecar-a-usar-programa-de-reconhecimento-facial-e-de-placas-de-veiculos-no-carnaval.ghtml

[104] Ley 1450 de 2011, artículo 227.

El proceso que cambió la lógica del uso de las bases de datos biométricas de la Registraduría se dió dió recién con la publicación del Decreto 019 de 2012, que introdujo el uso de medios electrónicos para autenticar a la ciudadanía en procedimientos que llevan a cabo entidades públicas o quien ejerza funciones públicas de diversa índole, como ser por motivos financieros, pensionales, registros públicos, la expedición de pasaportes y visas, entre otros.[105] Las siguientes regulaciones de la Registraduría pusieron a disposición de las entidades públicas y los particulares que prestan servicios públicos la base de datos biométricos de la RNEC[106].

Las siguientes regulaciones de la Registraduría pusieron a disposición de las entidades públicas y los particulares que prestan servicios públicos la base de datos biométricos de la RNEC[107], bajo la lógica de la lucha contra la suplantación de identidad y la prevención del fraude.

Luego de la puesta en marcha de esta política, aparecieron los denominados "aliados tecnológicos", los operadores de la infraestructura tecnológica que le permite a las entidades y a los particulares acceder a la base de datos de la RNEC, luego de cumplir los requisitos[108] que esta determina. En la práctica, esto implica que los actores que quieran utilizar la base biométrica de la Registraduría dependen de los aliados tecnológicos para ejercer sus funciones. En definitiva, la RNEC convirtió el uso de su base de datos biométricos en un negocio para que las empresas privadas presten servicios tecnológicos al Estado y que los particulares cumplan funciones públicas.[109]

En 2016, la Policía Nacional comenzó el proceso de adquisición e implementación del sistema Appolo, para utilizar dispositivos de verificación biométrica móvil, con un costo de 895 millones de pesos (287 mil dólares estadounidenses, aproximadamente).[110] Para su funcionamiento, fue necesario un convenio con la RNEC para tener un acceso directo a las bases de datos biométricas, basados en la Resolución 3341 de 2013.

De acuerdo con la Policía, este sistema parte de tres preocupaciones. Primero, una necesidad de innovación en la investigación criminal. Segundo, una preocupación por la seguridad nacional, pues la identificación plena de las personas permitiría tomar acciones más efectivas y confiables para la seguridad nacional.[111] En tercer lugar, el dispositivo permitiría facilitar la validación de la identidad en cualquier momento para luchar contra la falsificación de documentos y la suplantación de

[105] Íbid, artículo 17 y 18.

[106] Resolución N. 3341 de 2013 y Resolución N. 5633 de 2016.

[107] Íbid.

[108] Entre los requisitos está la experiencia certificada en autenticación biométrica de al menos tres años, infraestructura tecnológica, capacidad financiera y superar la prueba técnica realizada por la Registraduría.

[109] La RNEC ha publicado una lista de las entidades públicas o que prestan funciones públicas con las cuales hay un convenio vigente para la consulta del Archivo Nacional de Identificación que está disponible en: https://www.registraduria.gov.co/-Consultas-ANI-.html

[110] Oficina de Telemática de la Policía Nacional, «Estudios previos para Contrato de Compraventa 06-7-10081-16: Sistema de Biometría Móvil.» (2016), disponible en: https://www.contratos.gov.co/consultas/detalleProceso.do?numConstancia=16-1-157976

[111] Ibídem.

identidad.[112]

A partir de 2018, la Policía Nacional comenzó a utilizar un dispositivo fabricado por la empresa Olimpia para acceder, via Internet, a la base de datos de la Registraduría, con el fin de verificar la identidad de una persona y cotejar si existen órdenes nacionales o internacionales de captura. El dispositivo permite además cotejar los datos de la Cédula de Ciudadanía (presentes en el código de barras) con los de la base de datos de la RNEC, lo que asegura que el documento es original.[113] La Policía espera que estos dispositivos puedan ser utilizados con nuevas características como reconocimiento facial y de iris.[114]

Las políticas impulsadas por la RNEC también despertaron el interés de las instituciones financieras y bancarias. Mediante el Contrato 27 de 2016, la Registraduría suscribió un solo convenio con la Asociación Bancaria y de Entidades Financieras de Colombia (Asobancaria)[115], permitiéndole a todas las instituciones miembro que acceden a las bases de datos de la RNEC mediante el pago del servicio.

[112] Ibídem.

[113] El País, «Los nuevos gadgets de la Policía con los que verifican identidad y antecedentes en segundos.» El País.com.co, (9 de Mayo de 2018), disponible en: https://www.elpais.com.co/judicial/los-nuevos-gadgets-de-la-policia-con-los-que-verifican-identidad-y-antecedentes-en-segundos.html

[114] Camacho, Laura, «La Policía ahora revisará sus antecedentes judiciales con la huella.» El Tiempo, (21 de Mayo de 2018), disponible en: https://www.eltiempo.com/tecnosfera/tutoriales-tecnologia/policia-implementa-la-identificacion-biometrica-en-sus-procedimientos-214926

[115] Asobancaria . «Autenticación biométrica para usuarios del sistema financiero colombiano.» (2016), disponible en: https://www.asobancaria.com/biometria/

Máquina de identificación biométrica por huellas dactilares utilizada en Colombia.

De acuerdo con Asobancaria, la autenticación biométrica en el sistema financiero colombiano trae beneficios tanto para las personas como para las entidades financieras. En el primer caso, el uso de esta tecnología representa una modernización que hace más rápida las transacciones, mitiga el riesgo de suplantación y hace una transformación digital aplicando la política de "cero papel". En el segundo caso, la autenticación biométrica representa una posibilidad para las entidades de ofrecer servicios de forma automatizada y asegurar la identificación de los datos financieros de cada cliente.[116]

Hace diez años, la RNEC utilizó por primera vez la autenticación biométrica en procesos electorales atípicos. Según la Registraduría, se planeaba implementar tres nuevos controles en el proceso de votación: la identificación del votante en la base de datos del censo electoral, la entrega del documento de identidad y la autenticación mediante su huella dactilar. Dichos procedimientos permitirían evitar la suplantación o la doble votación en las elecciones atípicas.[117] De hecho, la RNEC argumentó que los nuevos procedimientos eran una respuesta al fallo del Consejo de Estado en 2005, que constató que había más votos que votantes para las elecciones al Congreso de la República de 2002.[118] A partir de ahí, la Registraduría ha masificado gradualmente el uso de la biometría en los procesos electorales, llegando a utilizarlo en cerca de 33 comicios.[119]

A fines de 2017, la Autoridad de Control Migratorio y de Extranjería del Estado Colombiano empezó a utilizar el sistema de Migración Biométrica (BIOMIG). Un sistema identificación automática fronteriza que utiliza datos biométricos del iris para identificar a las personas nacionales mayores de 12 años en su ingreso al país a través del aeropuerto más importante del país, el Dorado de Bogotá. El sistema en la actualidad cuenta con 10 terminales y la inscripción es voluntaria, presentando la cédula de ciudadanía, el pasaporte y un análisis de las treinta terminales para recolectar la información biométrica de las personas.[120]

[116] Asobancaria, «Biometría: conveniente y segura.» Semana Económica 2018 (2018).

[117] Registraduría Nacional del Estado Civil, «Suplantación de electores: un fraude más recurrente en el mapa de riesgo electoral.» Nuestra Huella, (2009), disponible en: https://www.registraduria.gov.co/Edicion-No-34-Ano-V-diciembre-de.html#01

[118] Registraduría Nacional del Estado Civil, "Este domingo los habitantes de Salazar de las Palmas (Norte de Santander) y Belén de los Andaquíes (Caquetá) eligirán sus nuevos alcaldes", 2009, disponible en: https://www.registraduria.gov.co/ESTE-DOMINGO-LOS-HABITANTES-DE,1563.html

[119] Registraduría Nacional del Estado Civil, «La huella dactilar: la base del sistema de identificación en Colombia.» Nuestra Huella, (2012), disponible en: https://www.registraduria.gov.co/rev_electro/2012/rev_elec_noviembre/revista_noviembre2012.html#10

[120] Presidencia de Colombia, «Migración Colombia empezó a usar sistema de inmigración de colombianos por medio de reconocimiento del iris.» (25 de Febrero de 2018).

Propaganda de Migración Colombia sobre el sistema de reconocimiento de iris.

Según informó el Director de Migración Colombia a la prensa, durante el proceso migratorio, el terminal "se conecta automáticamente con diferentes bases de datos tanto nacionales como internacionales [INTERPOL] para poder verificar si esta persona tiene algún impedimento u orden de captura"[121].

La compra de los equipos se realizó a través del contrato número 117 de 2017 con la Unión Temporal de Control Fronterizo INCOMELEC-GEMALTO. La primera fase del contrato costó más de dos mil cien millones de pesos colombianos (675 mil dólares aproximadamente). A pesar de la Unión, la empresa encargada del sistema es la multinacional holandesa Gemalto, desarrolladora del software que usan las terminales EF-45 de reconocimiento biométrico facial y de iris de la empresa CMI Tech[122]. El contratista tiene amplio historial y relaciones con el Gobierno colombiano y Migración Colombia[123]. En la actualidad, el sistema ya cuenta con terminales en cuatro aeropuertos de Colombia y hay planes de implementarlo en unidades móviles migratorias por conexión satelital[124].

[121] Caracol Televisión, «Con solo una mirada, colombianos podrán ingresar en segundos al país.» Caracol Televisión, (27 de Febrero de 2018): https://noticias.caracoltv.com/colombia/con-solo-una-mirada-colombianos-podran-ingresar-en-segundos-al-pais

[122] Migración Colombia, Contrato No 117 de 2017 con la Unión Temporal de Control Fronterizo INCOMELEC-GEMALTO, (2017).

[123] GEMALTO, "Los ojos son la solución".

[124] Becerra, Laura, «Cuatro aeropuertos del país ya cuentan con sistema de migración automática.» La República, (5 de Abril de 2018).

Según Migración Colombia, el sistema tiene varias justificaciones como la mejora de la percepción de seguridad a nivel internacional, la optimización de los procesos migratorios, la eficiencia financiera, la modernización de la entidad y la seguridad nacional[125]. En ese sentido, el sistema BIOMIG se presenta como una solución para todos los problemas de la entidad en términos de seguridad nacional y eficiencia en la atención al viajero. Igualmente, la idea inicial del sistema es centrarse en la población nacional colombiana para ampliarse a otros tipos de personas[126].

Máquina de reconocimiento de iris usada en el proceso migratorio con el sistema BioMig.

A pesar de que Migración Colombia reconoce que los datos biométricos son sensibles y que deben mantenerse en reserva bajo la Ley 1581 de 2012, su tratamiento no requiere de una autorización previa dada la naturaleza misional de sus funciones. Considerando que Migración Colombia es una autoridad civil de seguridad del Estado, la Ley les permite hacer tratamiento de datos biométricos, a pesar de su naturaleza sensible, por razones de seguridad y defensa nacional[127].

IV. México

La implementación de tecnología biométrica se ha dado con mayor preponderancia desde el sector privado, particularmente en el ámbito financiero. Sin embargo, en años recientes, desde el Estado

[125] Migración Colombia, Estudios Previos para el Contrato No 117 de 2017 con la Unión Temporal de Control Fronterizo INCOMELEC-GEMALTO, (2017), 1-4.

[126] Ibídem, 6.

[127] Oficina de Asesoría Jurídica de Migración Colombia, "Memorando Concepto Jurídico".

comenzaron a concretarse iniciativas que promueven el uso de datos biométricos como soluciones infalibles para solucionar viejos problemas. A continuación, se destacan dos casos correspondientes a ambos sectores. Por un lado, el uso de datos biométricos registrados de los votantes para la verificación de identidad en entidades financieras y, por el otro, la recolección de datos biométricos de las personas migrantes.

Sector financiero

En 2016 se firmaron las Bases de colaboración para inhibir la suplantación de identidad a través del sistema financiero en México, mediante las cuales se acordó que las instituciones bancarias pueden hacer uso del Servicio de Verificación del INE. A partir de esta colaboración, las instituciones bancarias en México recabarán información de sus clientes para compararla con los datos contenidos en el padrón electoral del Instituto Nacional Electoral, con el fin de determinar la identidad de sus clientes.

En 2017, la Comisión Nacional Bancaria y de Valores (CNBV) modificó las disposiciones de carácter general aplicables a las instituciones de crédito, obligando a las entidades bancarias a verificar la información biométrica de las personas que utilicen la identificación expedida por el INE. En caso de que se utilice el pasaporte o documentos migratorios como medio de identificación, no existe la obligación de realizar el proceso de verificación.

La CNBV volvió a modificar, un año más tarde, las disposiciones de carácter general aplicables a las instituciones de crédito para permitir a los bancos la captura de al menos seis huellas digitales, con el fin de verificar la identidad de las personas. También se amplió hasta 2020 el periodo con el que cuentan las instituciones bancarias para utilizar biometría en el proceso de verificación de las personas que contraten o realicen operaciones bancarias. Se espera que el tratamiento de datos biométricos en este rubro se convierta en norma sustituyendo contraseñas y otros medios de verificación.

Migraciones

En el informe de modernización del Instituto Nacional de Migración (INM) de la gestión 2006 - 2012, el organismo declaró contar con una base de datos biométricos centralizada, compuesta por datos biométricos (huella, iris y fotografía del rostro). Según el sexto informe de labores del INM publicado en 2012[128], en diciembre de 2011 se recibió en las instalaciones del Instituto el Motor Biométrico Central, el cual tiene la "capacidad de intercambio de información [biométrica] con dependencias mexicanas y trabajo conjunto con agencias del gobierno de EUA"[129].

Hasta 2012 se habían instalado 84 kioscos con equipamiento para el registro de datos biométrico, dentro del territorio nacional, en 24 de las 32 entidades federativas de la república, y se efectuó la

[128] Secretaría de Gobernación. "Sexto Informe de labores, Instituto Nacional de Migración". pg. 15. Disponible en: http://www.inm.gob.mx/static/transparencia/pdf/Informe_de_labores_2012.pdf

[129] Instituto Nacional de Migración. "Modernización tecnológica del INM: Gestión 2006 - 2012". pg. 10. Disponible en: http://www.inm.gob.mx/static/transparencia/rendicion_de_cuentas/MD_DGTIC_05OCT12.pdf

recepción de 167 kioscos más, entregados por la Oficina de Asuntos Antinarcóticos de la Embajada de Estados Unidos en México (NAS)[130]. El tratamiento de datos biométricos ocurre en cinco casos[131], entre los que se encuentran el registro de personas migrantes que entran y salen de las estaciones migratorias y la resolución de los casos de identidades duplicadas y otras anomalías.

Kioscos instalados para el registro de datos biométricos en el proceso migratorio en México.

Según el periodista Jesús Esquivel, al menos desde 2014, el INM comparte con el gobierno de Estados Unidos los datos biométricos de las personas migrantes detenidas[132], sin que de esto tengan conocimiento siquiera los agentes de inmigración que toman los datos de los migrantes detenidos[133]. Una vez en posesión de Estados Unidos, los datos biométricos son utilizados para identificar a "personas no deseadas" a partir de la bases de datos con las que cuenta el gobierno norteamericano.

En respuesta a una solicitud de acceso a la información realizada por la R3D al INM en 2017[134], el Instituto respondió que únicamente realizaba el tratamiento de datos biométricos de extranjeros como parte del Programa Viajero Confiable, el cual permite a ciudadanos mexicanos, canadienses y estadounidenses reducir el tiempo para ingresar a México cuando llegan al territorio mexicano por

[130] Íbid, página 22.

[131] Los otros tres casos comprenden el enrolamiento, expedición y verificación de las Formas Migratorias de Visitante Regional y la Forma Migratoria para Trabajador Fronterizo. Íbid, página 28.

[132] Aristegui noticias. "México entrega a EU datos biométricos de migrantes y mexicanos: Jesús Esquivel". 7 de mayo de 2018. Disponible en: https://aristeguinoticias.com/0705/mundo/mexico-entrega-a-eu-datos-biometricos-de-migrantes-y-mexicanos-jesus-esquivel/

[133] Íbid.

[134] Solicitud de acceso a la información número 0041110022117, disponible en: https://r3d.mx/wp-content/uploads/Respuesta-Instiuto-Nacional-de-Migraci%C3%B3n-Biom%C3%A9tricos.pdf

vía aérea. En una solicitud de acceso a la información posterior, específicamente sobre el tratamiento de datos biométricos de personas migrantes[135], el Instituto negó realizar dicho tratamiento.

Irazú Gómez, coordinadora de vinculación e incidencia en Sin Fronteras[136], declaró en una entrevista concedida a R3D, haber presenciado desde 2012 el registro por parte del Instituto Nacional de Migración del rostro y el iris de personas migrantes a su ingreso a estaciones migratorias. El sistema de registro de datos biométricos de personas migrantes llamado SICATEN[137] compartía datos con los gobiernos de algunos países de Centroamérica y de Estados Unidos. La transferencia de datos biométricos tenía el objetivo de identificar personas que estuvieran boletinadas por dichos países como terroristas y negar su acceso al país, comentó Gómez.

En relación a la forma como se obtenía el consentimiento de los migrantes para realizar el tratamiento de sus datos biométricos Gómez explicó:

"Al entrar a la estación migratoria los migrantes debían de llenar un registro a mano y luego pasaban por una máquina que registraba su iris y rostro. Por lo que pude ver no les otorgaban información sobre el procedimiento a menos que los migrantes preguntaran. En general sólo les daban un paquete de hojas para que firmaran que les habían leído sus derechos y que habían recibido la información necesaria. Eran formatos de facto que mucha gente no leía y firmaban sin realmente enterarse." Según Gómez el registro biométrico de personas migrantes detenidas continúa en operación.

Según el INM, el fundamento legal para realizar el tratamiento de datos biométricos se encuentra contenido en los artículos 18, 19, 20 y 63 de la Ley de Migración. Los mismos otorgan, entre otras, atribuciones en materia de política migratoria para establecer requisitos para el ingreso al territorio mexicano, para vigilar la entrada y salida de personas del territorio mexicano y revisar sus documentos, así como para mantener el Registro Nacional de Extranjeros[138]. Además el artículo 60 del Reglamento de dicha norma, expedido por el poder ejecutivo, establece explícitamente que la autoridad migratoria podrá corroborar, entre otras cosas, información y datos personales de migrantes.

La Ley es ambigua y amplia respecto de las prácticas que el INM puede perseguir para llevar a cabo la política en materia migratoria y no establece de manera explícita la posibilidad de tratar datos biométricos, sino que mediante la definición de estos como datos personales.

[135] Solicitud de acceso a la información número 0411100139918, disponible en: https://r3d.mx/wp-content/uploads/0411100139918.pdf

[136] Sin Fronteras es una organización de la sociedad civil mexicana, laica, apartidista y sin fines de lucro que contribuye a la promoción, protección y defensa de los Derechos Humanos de las personas migrantes y sujetas de protección internacional para dignificar sus condiciones de vida a través de la atención directa e incidencia en la agenda pública. https://sinfronteras.org.mx

[137] Sistema de Control de Aseguramientos y Traslados en Estaciones Migratorias.

[138] Según el artículo 63 de la Ley de Migración el Registro Nacional de Extranjeros está conformado por la información relativa a todos aquellos extranjeros que adquieren la condición de estancia de residente temporal o de residente permanente en México.

V. Conclusiones

A partir de los países estudiados y los casos de estudio detallados, se ha evidenciado el efecto expansivo en las narrativas de identidad junto a la incorporación de tecnología biométrica. Resulta alarmante que los Estados partan de la tecnología específica para la solución de sus problemas, sin plantear métodos alternativos, encontrando así usos de todo tipo para introducir la biometría en políticas públicas.

La construcción de las narrativas de identidad que promueven el uso incremental de los datos biométricos se ha basado en normas que desafían el principio de legalidad al ser, en su mayoría, decretos del poder ejecutivo y resoluciones ministeriales. Además, las reglas, lineamientos y protocolos que delimitan la recolección y proceso de los datos biométricos son elaborados por las mismas entidades que llevan a cabo estos programas.

La introducción de la biometría no ha sido delineada, de manera precisa, expresa y por ley, en ninguno de los países en estudio. En general, las normativas incorporan los conceptos sin brindar definiciones, dejando la interpretación –en muchos casos– al libre entendimiento de las entidades que implementan la tecnología biométrica y realizan el tratamiento de los datos. Esto presenta diversos problemas vinculados a la delimitación, uso y procesamiento de los distintos tipos de datos biométricos que pueden ser recolectados, pues ante la generalidad, los Estados pueden apuntar a una interpretación más abierta en los datos que pueden utilizar para variados fines.

En Brasil y Colombia, la legislación clasifica al dato biométrico como uno de tipo sensible, mientras que en Argentina y México esa misma elaboración ha sido producto, en cada caso, de la interpretación de la autoridad de protección de datos, antes que de una prescripción legal. Aún así, es evidente la falta de poder con el que cuentan las autoridades de protección de datos en cada país para ejercitar el cumplimiento de la ley y evitar abusos en la utilización de los datos biométricos por el Estado y el sector privado.

De los casos de estudio abordados en esta investigación, se evidencia cómo los países con Estados unitarios, como el caso de Colombia, tienen mayor facilidad en la implementación de políticas públicas bajo iniciativas centrales desde una única entidad. Sin embargo, aún en los países federales –como son Argentina, Brasil y México– las administraciones públicas han logrado promover y unificar narrativas vinculadas a la necesidad de la tecnología biométrica para el reconocimiento infalible de la identidad de las personas, y por ende, del ejercicio de determinados derechos.

Los países en estudio han dado una mirada hacia las justificaciones que esbozan los Estados para incorporar cada vez más tecnologías biométricas en la vida diaria de las personas. La narrativa que prima posiciona a la seguridad pública y a la biometría como la pareja definitiva para solucionar los mayores problemas de inseguridad, siendo utilizada para la investigación y la lucha contra el delito. Además, el otorgamiento de beneficios y servicios sociales se ven condicionados por la entrega de

datos biométricos. El control migratorio, las actividades impositivas (como el pago de impuestos o requisitos obligatorios para el ejercicio de profesiones independientes), el sector financiero, los procesos electorales y el transporte público, también se han visto permeados por la incorporación de tecnologías biométricas.

El impacto que las tecnologías biométricas presentan para el ejercicio de derechos fundamentales depende del tipo de dato en uso y diversos factores como su implementación, por lo que debe analizarse cada caso en particular. Sin embargo, podemos remarcar determinadas consideraciones sobre lo que implica el uso de esta tecnología.

La recolección y procesamiento en las bases de datos biométricos para la identificación de personas (1:N), con fines de investigación y prevención del delito, desafía las garantías del debido proceso y el principio de inocencia, al convertir a todas las personas que tienen sus datos biométricos almacenados en potenciales sospechosos, revirtiendo así la carga de la prueba, pues las personas deben "demostrar" que no son a quien buscan (lo que se produce en el momento en que se descartan sus plantillas biométricas al no encontrar una similitud).

En el caso del reconocimiento facial, los algoritmos encargados de encontrar las similitudes entre las plantillas con los rasgos faciales pueden contener sesgos derivados de su programación y/o entrenamiento. Esto implica que el sistema puede ser propenso a discriminar contra determinados grupos de personas, dada la alta tasa de falsos positivos, como ha sido demostrado en el caso de afroamericanos en Estados Unidos[139].

El desarrollo de sistemas biométricos por parte del Estado, bajo una lógica de control de la población, excede al impacto en el derecho a la privacidad y las libertades individuales como la expresión, reunión y asociación. Su uso como herramienta de vigilancia de las personas o mecanismo de ordenamiento para la provisión de beneficios esenciales por parte del mismo Estado, implica que debemos considerar su aspecto colectivo.

En este sentido, podemos identificar tres factores en los cuales la biometría afecta al conjunto de las personas.

1. Dimensión colectiva de los derechos individuales: Si bien el derecho a la privacidad es un ejemplo clásico de los derechos de primera generación, el poder de las tecnologías de vigilancia ha demostrado la necesidad de pensar en formas colectivas en que se afecta este derecho. La biometría implica un accionar determinado que puede afectar a una multitud o grupo de personas al mismo tiempo. Así, la privacidad deja su faz individual para transformarse en un bien colectivo que involucra a la sociedad en su conjunto. Al respecto, no debe olvidarse que

[139] Jacob Snow, "Amazon's Face Recognition Falsely Matched 28 Members of Congress With Mugshots", ACLU, 26 de julio de 2018, disponible en: https://www.aclu.org/blog/privacy-technology/surveillance-technologies/amazons-face-recognition-falsely-matched-28

en Argentina el nacimiento de las acciones colectivas se dio a través de un caso de violación al derecho de la privacidad.[140]

2. Afectación a derechos sociales: La tecnología biométrica también puede ser utilizada para restringir derechos que ya son considerados de índole colectiva desde su propia esencia, como los derechos sociales. Como fue narrado a lo largo del informe, la provisión de servicios de salud, educación o seguridad social, se encuentran cada vez más condicionados a la entrega obligatoria de datos biométricos. De esta manera, todo intento de resistencia tiene como consecuencia el impedimento del goce de derechos sociales.

3. Impacto particular en grupos desaventajados: El uso de datos biométricos tiene efectos perjudiciales específicos para ciertos grupos étnicos o religiosos. En este caso, el carácter colectivo no está dado tanto por la naturaleza del derecho en juego, sino por los daños que la tecnología biométrica genera en particular en un subconjunto de la población. Así, la biometría presenta el riesgo de mantener o fomentar la reproducción de desigualdades o injusticias en sectores que han atravesado un largo historial de vulnerabilidades.

VI. Recomendaciones

Por defecto, el enrolamiento de los datos biométricos debe ser voluntario, sin condicionar la provisión de servicios y beneficios estatales (como en el caso de la seguridad social) a su entrega. Asimismo, los Estados deben dar la opción de medios alternativos que no impliquen la entrega de datos biométricos.

Previo a la implementación de sistemas y tecnologías que utilicen datos biométricos, los Estados deben llevar a cabo diversas evaluaciones:

1. En primer lugar, estudios que produzcan evidencia científica para establecer en forma fundada la magnitud y realidad del problema que se pretende solucionar mediante el uso de biometría y los diversos caminos que se pueden tomar para solucionarlo. Los Estados deben siempre optar por probar primero la medida que sea menos invasiva y limitante de derechos fundamentales; hasta que no hayan sido todas las anteriores descartadas, no deberían optar por la que sea más restrictiva de derechos civiles y libertades individuales.

2. En segundo lugar, debe analizarse el impacto en derechos humanos que pueden producir la puesta en marcha de dichos sistemas y tecnologías. Esto permite identificar de antemano los riesgos para el ejercicio y goce de derechos como la privacidad, la libertad de expresión, la libertad de asociación, la libertad de reunión, el trato igual ante la ley y la no discriminación. Con el objetivo de tomar las acciones concretas para prevenir y mitigar dichos riesgos.

[140] Halabi, Ernesto c/ P.E.N. - Ley 25.783 - dto. 1563/04 s/ amparo Ley 16.986, 24 de febrero de 2009.

3. Finalmente, debe realizarse un análisis de riesgo basado en la seguridad de los datos personales que se recolectan, almacenan y procesan, con el objetivo de identificar e implementar las mejores prácticas en la protección de la información, prevenir incidentes y articular protocolos ante fallas de seguridad de la información. Incluyendo la incorporación de auditorías técnicas independientes que sean realizadas en forma periódica. Esto debe encontrarse en línea con las estrategias nacionales de ciberseguridad en cada país.

Los órganos legislativos deben plantearse la actualización de los marcos normativos vigentes para reflejar los estándares internacionales de derechos humanos, promoviendo debates abiertos, inclusivos y transparentes, particularmente en lo que respecta a las definiciones sobre "biometría", "tecnología biométrica" y "datos biométricos". La recolección y procesamiento de datos biométricos, con la consecuente conformación de enormes bases de datos, debe realizarse teniendo en cuenta los principios de necesidad y proporcionalidad, acorde a los estándares del Sistema Interamericano de Derechos Humanos. Justificando su origen en una finalidad legítima perseguida que haya sido establecida por una ley sancionada por el órgano legislativo.

Toda legislación sobre biometría debe incorporar previsiones sobre los mecanismos de supervisión y de rendición de cuentas. En tal sentido, un primer paso sería contar con autoridades independientes que puedan detectar y sancionar el mal uso de los datos biométricos o la implementación de sistemas desproporcionados e ilegales acorde a los estándares internacionales de derechos humanos. Establecer controles específicos para el acceso a las bases de datos y su uso para la identificación de personas, por ejemplo bajo autorización judicial en causas criminales, que a su vez deben fundarse en determinados delitos de mayor gravedad.

En lo que respecta a los datos biométricos como datos personales, la legislación de todos los países en estudio –sobre la protección de los datos personales– debe actualizarse para brindar precisión en las finalidades sobre el uso de los datos y mejorar los niveles de protección a su tratamiento. Ello implica también revisar los roles y facultades de las autoridades de protección de datos en lo que respecta a la implementación de la tecnología biométrica por el Estado y el sector privado, junto a su poder de sanción ante el incumplimiento de la ley. Esto va de la mano con dotar a dichas autoridades de plena independencia de los poderes de Estado, asignándole los recursos financieros y el personal capacitado necesario para tal fin.

Dada la inminente construcción y expansión de sistemas de identificación, alimentados por datos biométricos, cada vez más complejos y entramados entre múltiples organismos públicos, debemos replantear lo que entendemos por "consentimiento informado". En especial a la luz de las tecnologías biométricas y la justificación de su implementación en razones de seguridad pública, además del factor de libertad cuando del otorgamiento de los datos biométricos depende el acceso a servicios esenciales para los grupos sociales más vulnerables.

Asimismo, el hecho de que varias iniciativas en los países en estudio implementen tecnología biométrica para la provisión de servicios y beneficios sociales, pone de manifiesto el valor de la libertad al prestar el consentimiento. Difícilmente el consentimiento sea libre cuando la ciudadanía depende del Estado para acceso a servicios esenciales.

Sin embargo, más allá del consentimiento libre e informado, que siempre debe ser exigido, esto no implica que el mismo sea usado como carta blanca o excusa para que estas tecnologías vulneren otros principios claves en el tratamiento de los datos, como es el caso de la finalidad. Es por ello que los estándares mínimos son irrenunciables para el titular de los datos, no pudiendo ser revocados ni cedidos al momento de prestar su consentimiento, siguiendo el principio *in dubio pro titular del dato*, teniendo en cuenta que siempre hay una relación desigual de poder entre quien trata el dato y su titular.

Finalmente, dependiendo del sistema biométrico en cuestión, algunas consideraciones mínimas que deben tenerse en cuenta para mitigar el impacto adverso en la privacidad son: limitar el tipo de datos biométricos que son almacenados en una misma base de datos; priorizar la verificación (1:1) por sobre la identificación (1:N) de las personas; y no almacenar la información patronímica con los datos biométricos en la misma base de datos.


por los Derechos Civiles