Identidad Biométrica en Perú

Estado de la cuestión

hiperderecho

Hiperderecho

Asociación civil peruana sin fines de lucro dedicada a investigar, facilitar el entendimiento público y promover el respeto de los derechos y libertades en entornos digitales. Fundada en el 2013, investiga e interviene en debates de políticas públicas sobre libertad de expresión, derechos de autor, privacidad, ciberseguridad y delitos informáticos.

Investigación:
Carlos Guerrero y Martín Borgioli

Asociación Civil Hiperderecho
Av. Benavides 1180, Piso 6
Miraflores, Lima

hola@hiperderecho.org

Algunos derechos reservados, 2018
Bajo una licencia Creative Commons Reconocimiento 4.0 Internacional. Usted puede copiar, distribuir o modificar esta obra sin permiso de sus autores siempre que reconozca su autoría original. Para ver una copia de esta licencia, visite: https://creativecommons.org/licenses/by/4.0/deed.es

Esta investigación ha sido financiada gracias al apoyo de Privacy International entre noviembre de 2017 y mayo de 2018. Para más información sobre el trabajo de Privacy International en materia de identidad biométrica visitar https://privacyinternational.org/topics/biometrics

Índice

Índice 3
1. Hallazgos 4
2. Metodología de la investigación 5
3. Contexto 5
3.1. Antecedentes de la identificación biométrica en el Perú 6
3.2. El paradigma peruano en las políticas públicas de identificación biométrica 8
4. Ecosistema de identificación biométrica 10
4.1. Entidades públicas 10
4.2. Entidades privadas 12
4.3. Proveedores 14
5. La identificación biométrica a través de sus diversas facetas 15
5.1. Diseño institucional 15
5.2. Estándares y medidas de seguridad 16
5.3. Identificación biométrica y política: Propuestas populistas y de corto plazo 17
5.4. Marco legal de los datos biométricos 18
6. Conclusiones 20
7. Anexos 23
7.1. Ecosistema de identificación biométrica en Perú 23
7.2. Organigrama del AFIS Policial 24
7.3. Modelo de Convenio suscrito entre RENIEC y una entidad privada 25

1. Hallazgos

- En Perú los estudios sobre el desarrollo de los sistemas biométricos de identificación son escasos, siendo la mayoría de ellos informes de operaciones y resultados del Registro Nacional de Identificación y Estado Civil (RENIEC), la entidad pública rectora del sistema de identificación de personas en el país. El esfuerzo principal de este informe es presentar el estado actual de las cosas en relación al uso de identificación biométrica en el país por parte de actores públicos y privados desde un punto de vista más neutral.

- Con la creación de RENIEC en 1995, se da un giro respecto del uso de los sistemas de identificación biométricos, transitando del uso de tecnologías anticuadas a una más moderna de reconocimiento automatizado de huellas dactilares (AFIS) que es la más extendida actualmente. Además, esta entidad centraliza todas las competencias del nuevo sistema de identificación de personas y desarrolla y ejecuta políticas públicas en esta materia, casi de forma exclusiva y limitada sólo por el marco legal vigente.

- Con RENIEC a la cabeza, se ha formado una suerte de ecosistema alrededor del uso de la biometría como sistema de identificación, que comprende no solo a actores públicos sino también privados. A veces estas relaciones son de provisión de servicios de identificación solicitadas voluntariamente, pero también existen casos en donde el uso de sistemas biométricos viene impuesto por ley, como es el caso de la adquisición de líneas de telefonía móvil.

- En apariencia RENIEC es, si se le compara con sus pares dentro de la región, una entidad que ha sabido aprovechar su rol predominante dentro del ecosistema nacional para dotar de coherencia al sistema de identificación que emplea tecnología biométrica. Sin embargo, pese a contar con diferentes estándares y medidas de seguridad en el tratamiento de estos datos, existen muchos ángulos de vulnerabilidad no solo relacionados a su sistema centralizado de operación sino también a los servicios que ofrece y que se otorgan a los privados, quienes no están sujetos a dichos estándares.

- La ausencia de entidades en el sector público o privado que fiscalicen el desarrollo de los sistemas de identificación biométricos en el país es también un problema, en la medida que nuevos actores se han sumado al ecosistema local, y están cambiando la forma cómo los ciudadanos se relacionan con la biometría. Algunos de ellos lo hacen a través de la creación de políticas públicas que incorporan estas tecnologías con diferente fines como la seguridad ciudadana, mientras que otros lo hacen desde el ámbito de la innovación y la soluciones para el sector privado.

- En abril de 2018, Hiperderecho detectó y reportó un filtrado de información en RENIEC que dejaba expuestas las fotografías del documento de identidad de todos los peruanos. Aunque la vulnerabilidad fue resuelta luego de reportada, este tipo de errores cobran mayor magnitud cuando existen bases de datos centralizadas en las que el acceso a una porción de los datos puede permitir la explotación del resto y no existen mecanismos de control claros.

2. Metodología de la investigación

Al considerar que este es un trabajo inicial que busca ofrecer un panorama más o menos completo de la situación de la biometría en el país, hemos decidido emplear una metodología exclusivamente descriptiva. Para ello, hemos acopiado información de fuentes principalmente secundarias y terciarias, entre las que se encuentran estudios sobre el desarrollo del Estado, manuales de operaciones, recortes periodísticos, columnas de opinión, etc. Además, hemos consultado también la legislación aplicable, que se incluye más adelante.

En algunos casos hemos empleado también la comparación de modelos, tomando como puntos de referencia a otros informes sobre el estado de la biometría en Argentina[1] y Chile[2]. Esto nos ha permitido en ciertos momentos situar nuestra realidad fuera o dentro de lo que son consideradas prácticas comunes de biometría, así como medir qué tan eficiente, seguro y resiliente es nuestro sistema biométrico público con respecto a otros que existen en contextos similares.

Finalmente, otra de las herramientas que nutren esta investigación han sido las solicitudes de acceso a la información pública que hemos enviado a diferentes entidades del Estado. Si bien es de conocimiento público el uso de las tecnología biométricas, no lo es tanto cómo estas funcionan o qué impacto tienen en la vida de las comunidades a las que sirven. Estos datos son quizás algunos de los más importantes y reveladores y se encuentran al final de este informe.

3. Contexto

La palabra biometría deriva de los términos griegos *bios* y *metron* que significan "vida" y "medida" respectivamente. En su acepción más amplia, biometría es todo proceso cuyo fin es medir de forma estandarizada características físicas o conductuales de cualquier ser vivo, con el fin de poder identificarlo entre sus semejantes.[3] Sin embargo, hoy en día la palabra biometría se usa principalmente para referirse a los sistemas de identificación y verificación de identidad empleados tanto por estados y empresas con distintos fines, desde la persecución de delitos hasta el otorgamiento de créditos bancarios.

Si bien existe evidencia en la antigüedad sobre prácticas de identificación biométrica, es a partir de finales del siglo XIX que estas empiezan a ser adoptadas en occidente por los estados, sobre todo con fines de orden interno y seguridad nacional. Algunos ejemplos son el sistema antropométrico (1870) desarrollado por primera vez en Francia, el de reconocimiento manual de huellas dactilares (1903) desarrollado y empleado extensivamente en los Estados Unidos, el de reconocimiento automatizado de huellas dactilares "AFIS" (1994), que fue el primero en ser

---

1 Asociación por los Derechos Civiles, "La identidad que no podemos cambiar. Cómo la biometría afecta nuestros derechos humanos," (Abril, 2017), https://perma.cc/A938-7TRT

2 Romina Garrido y Sebastián Becker, "La biometría en Chile y sus riesgos," *Revista Chilena de Derecho y Tecnología* 6, no. 1 (Junio, 2017), https://perma.cc/9YAZ-HE6A

3 Diccionario de la Real Academia Española de la Lengua, 23 ed. (2014), s.v. "biometría", https://goo.gl/LMa3p3

usado por una agenda del gobierno federal también en Estados Unidos y otros desarrollos más recientes como la identificación de iris, voz, entre otros.[4]

En la actualidad, es casi imposible encontrar un lugar en el mundo en donde no se haya desplegado al menos un sistema de identificación biométrica básico. Por ejemplo, en Perú actualmente coexisten varios sistemas de tipo público y privado, los que permiten el acceso a toda clase de servicios. En la mayoría de casos, estos parecen haber representado un cambio positivo en la vida de las poblaciones a las que sirven. Pero su implementación ciertamente ha generado consecuencias perjudiciales, muchas de las cuales pueden pasar desapercibidas a simple vista.

Con el paso del tiempo y los avances tecnológicos, los sistemas biométricos se han ido refinando al punto de ser considerados infalibles, no solo porque su margen de error es mínimo, sino también porque son tan complejos que a veces sus operadores no entienden cómo funcionan, convirtiendo su efectividad en un asunto de fe. Esto se convierte en un problema sobre todo en sociedades hiper tecnificadas en donde el acceso a servicios básicos depende de que un sistema automático "reconozca" si alguien es quien dice ser.

Pero también trae problemas a sociedades menos tecnificadas, como en el caso del Perú. Esto debido a que incluso los sistemas biométricos más sencillos requieren para su funcionamiento de una infraestructura compuesta por múltiples elementos: bases de datos biométricos, servidores dedicados, entidades acreditadoras, dispositivos de verificación, etc. Mantener niveles de eficiencia y seguridad óptimos en cualquiera de estos elementos supone un alto grado de coordinación e interoperabilidad, que en la mayoría de países en vías de desarrollo es aún deficiente.

La masificación de Internet, el avance de las tendencias del "big data" y de la inteligencia artificial en los años recientes no ha hecho más que expandir el abanico de posibilidades y peligros. En este contexto, el presente informe tiene como objetivo describir el proceso de implementación de sistemas biométricos en el Perú con el fin de dar a conocer su estado actual, identificar a los actores relevantes en su desarrollo y brindar al lector una idea acerca del futuro de estas tecnologías en el país.

3.1. Antecedentes de la identificación biométrica en el Perú

La evidencia histórica indica que la recopilación sistemática de datos biométricos en el Perú se inició en las primeras décadas del siglo XX. Previamente, durante la época colonial, los actos civiles relevantes como los nacimientos, matrimonios, defunciones, contratos sobre inmuebles, etc, eran registrados por las autoridades locales con fines estadísticos y de tributación[5], para los cuales se empleaba casi exclusivamente la firma como método de validación de la identidad. Esta práctica se mantendría luego del nacimiento de la República y no presentaría mayores reformas durante los próximos cien años debido a la inestabilidad producida por las guerras civiles, los golpes de estado y la Guerra del Pacífico.

---

4 Stephen Mayhew, "History of Biometrics," *Biometric Update*, (Febrero, 2018), https://perma.cc/5GFE-Q4L8

5 Superintendencia Nacional de Registros Públicos, "El Rol del Catastro en el Registro del Territorio y la Seguridad Jurídica", *Revista Fuero Registral* 7 (2011), p. 378

Es a partir de 1931 que se crea el primer documento oficial que incorpora formalmente datos biométricos (huellas dactilares) que pueden ser verificados manualmente para controlar el sufragio: la "Libreta Electoral". Durante sus primeros años de existencia, la posesión de estas libretas estuvo restringida a los varones a partir de los 21 años que sabían leer y escribir[6], pero con el tiempo se hizo de uso generalizado, primero con respecto de las mujeres, luego de las personas iletradas (que tenían un registro especial) y finalmente a todos los peruanos mayores de 18 años. Sin embargo, pese a ser el documento de identificación más importante de su época, la manufactura y distribución de las libretas electorales fue durante mucho tiempo responsabilidad de los gobiernos locales, que en la mayoría de casos no contaban con una infraestructura adecuada para satisfacer las demandas de cobertura y fiscalización.

Junto con las libretas electorales, coexistió durante muchos años otro tipo de registros de identidad que recogían también datos biométricos: la "Libreta Militar". Desde el inicio de la República en 1821 y hasta el año 1999, el servicio militar fue obligatorio en el Perú, por lo cual se hizo necesario crear un registro con todos aquellos ciudadanos en edad de servir. Este registro, que se hizo oficial a partir de 1912, incluyó desde sus inicios la consignación de datos biométricos como la estatura, el peso e inclusive la "raza", además de otros datos útiles para identificar a una persona usando el sistema antropométrico. Los encargados de mantener este sistema eran las Fuerzas Armadas. Sin embargo, a partir del año 2008, la inscripción en dicho registro dejó de ser obligatorio.

Los casos mencionados anteriormente constituyen en gran medida los sistemas de registro e identificación biométrica empleados durante gran parte del siglo XX, cuyo uso estaba restringido a la verificación del voto y el reclutamiento militar, para lo cual empleaban los sistemas biométricos de reconocimiento manual de huellas dactilares y el sistema antropométrico. No obstante, la historia indica que la implementación de los mismos fue deficitaria desde el inicio hasta el final. En la década de 1990, el índice de población indocumentada seguía siendo muy alto, no existían recursos para mantener sistemas de identificación óptimos, se seguían empleando sistemas desfasados como el antropométrico, entre otros. ¿Por qué ocurrió esto? En parte debido al bajo nivel de modernización de la Administración Pública,[7] pero también a la falta de una entidad que guíe el desarrollo de los sistemas nacionales de identificación.

Como producto de las reformas emprendidas a partir del año 1990, empieza una etapa nueva para los sistemas de identificación y por ende para la biometría. En 1993 se publica una nueva Constitución Política que establece la creación del RENIEC,[8] la primera entidad de su tipo en el país a la que se asigna las funciones de supervisor, coordinador y ejecutor de los sistemas de identificación de personas a nivel nacional. En 1995 se crea formalmente este organismo y empieza la unificación de todos los sistemas de identificación en el país. En esta etapa, se da la transición al uso de tecnologías más modernas como el sistema de identificación automático de huellas dactilares (también conocido como AFIS, por sus siglas en inglés), que actualmente es el sistema biométrico más utilizado en el país. También se crea un nuevo documento: el

---

6 "Evolución en el tiempo de documento de identidad del Perú". *Quiosco Perú,* 3 de agosto, 2016, https://goo.gl/La9QiH

7 Fernando Straface y Ana Inés Basco, *La Reforma del Estado en el Perú*, Banco Interamericano de Desarrollo, 2006, https://goo.gl/sX88b6

8 Constitución Política del Perú, Art. 177, 183 y disposiciones finales y transitorias.

"Documento Nacional de Identidad (DNI)" que no solo incorpora datos biométricos sino que establece nuevas medidas de seguridad de lectura electrónica. Así mismo, la cobertura sufre un cambio radical en la siguiente década pues entre los años 2005 y 2011 se pasa de un nivel de identificación efectiva del 59% a casi el 99% de la población (aprox. 30 millones de personas)[9], que incluye también a los menores de edad.

La rápida expansión de RENIEC a lo largo del territorio nacional y su papel fundamental en la prestación de otros servicios del Estado (trámites, salud, trabajo, etc.), le permitió la creación de productos cada vez más complejos. Un ejemplo de ello es el Documento Nacional de Identidad Electrónico (DNI-e), una solución reciente que ha incorporado la tecnología de microchip que almacena firmas digitales y datos biométricos, cuya entrega es una de las prioridades de esta institución en la actualidad.[10] En el mismo sentido, al haber concentrado las bases de datos de identificación a nivel nacional, este organismo da soporte de identificación a casi todas las demás entidades del sector público e incluso a algunas del sector privado como bancos, notarías, etc. a través del sistema AFIS, a veces bajo un sistema de oferta de servicios, en otros casos en cumplimiento de mandato legal.

3.2. El paradigma peruano en las políticas públicas de identificación biométrica

Como se desprende de su recorrido histórico, la identificación biométrica en el Perú ha transitado principalmente por dos momentos. El primero es el período que abarca desde el nacimiento de la República hasta el año 1990. En esta etapa se llegaron a implementar dos sistemas que empleaban datos biométricos: (1) el de reconocimiento manual de huellas dactilares, y (2) el antropométrico, que implicó la recolección de medidas corporales de una persona como su estatura o distancia de separación entre ambos hombros. Estos estaban orientados casi exclusivamente a verificar la identidad del ciudadano al momento del sufragio y facilitar el reclutamiento para el servicio militar obligatorio. Por ende, ninguno de estos datos fue empleado extensivamente para cubrir otras necesidades del sector público, menos aún del privado.

Tras una breve etapa de transición, empieza el segundo período en 1993 con la nueva Constitución Política que crea al RENIEC y lo convierte en la entidad máxima del sistema de identificación nacional. Beneficiándose de un diseño institucional moderno y contando con mayores recursos, RENIEC centraliza la mayoría de procesos de identificación, los perfecciona y expande hacia todo el territorio nacional. Debido en parte a su eficiencia en la labor de identificación, esta entidad profundiza en el uso de nuevas tecnologías, entre ellas el AFIS, lo que le permite ofrecer productos a la ciudadanía que habilitan nuevas opciones de servicios por parte del Estado. Asimismo, se consolida en el medio local como el primer proveedor de servicios de verificación de identidad dentro del sector público y de algunas operaciones y procesos en el sector privado.

Podemos decir que la visión imperante en la primera etapa era cortoplacista y estaba orientada a la obtención de resultados muy específicos. Si bien con el avance de la tecnología algunos de los

---

9 RENIEC, "Servicio de verificación biométrica", Febrero, 2012, 38, https://perma.cc/3NQR-DZU7

10 "DNI electrónico: Pasos y Requisitos para obtenerlo", *Diario La República, 5 de febrero, 2018*, https://goo.gl/sgrbpJ

sistemas de identificación biométricos podrían haberse refinado, la falta de una entidad responsable de supervisar su desarrollo hizo imposible que estos experimentaran cambios sustanciales. Sumado a ello, una Administración Pública sumamente burocrática, la inestabilidad política y económica y una falta de visión sobre la importancia de la identificación de la población hicieron imposible el aprovechamiento completo de las tecnologías biométricas.

Por el contrario, con la creación de RENIEC, la visión desde el sector público cambia. Esta entidad se percibe a sí misma no solo como una mera facilitadora de procesos, sino como un centro de desarrollo de políticas públicas en materia de identificación. Así mismo, al ser una instancia de dirección, pero también de ejecución, y que no depende de ningún poder del Estado, al ser organismo constitucionalmente autónomo, pudo sortear la valla impuesta por la burocracia, lo que le ha permitido convertirse en un organismo medular dentro de la Administración Pública. Esto no solo por la utilidad de la identificación para las relaciones entre los ciudadanos y el Estado sino porque también esto ha permitido la viabilidad de diferentes planes en otros sectores y la eficiencia de la ejecución de servicios como las asistencias sociales o la mejora de procesos productivos. En este contexto, el uso intensivo de sistemas de identificación biométricos más modernos como el AFIS en los procedimientos de registro e identificación actuales es una consecuencia de estos cambios.

En la última década, las políticas públicas relacionadas a la identificación de personas partieron casi exclusivamente desde RENIEC, incluyendo las que tenían que ver con el uso de sistemas biométricos. Sin embargo, en los años recientes existen múltiples iniciativas, principalmente desde el Congreso de la República, que han aprovechado los productos de esta entidad en materia de identificación para proponer políticas pensadas en otros temas como seguridad, salud y trabajo. Es decir, hemos visto aparecer propuestas legislativas y leyes que buscan solucionar nuevos problemas como fraude, criminalidad o estafa mediante el uso de la base de datos biométrica ya construída por RENIEC. Si bien esto parece ser un proceso natural y el reconocimiento final de la importancia del trabajo de RENIEC, muchas veces estas propuestas suponen rupturas con la coherencia normativa existente en temas de identificación o presentan nuevos desafíos para el ejercicio de otros derechos humanos.

Por ejemplo, en los últimos años se han aprobado leyes en materia de seguridad ciudadana que establecen la obligación de ciertas empresas de incorporar procesos de identificación biométrica para realizar transacciones como adquirir una línea de teléfono móvil. También desde la misma preocupación se aprobó una Ley para exigir la colocación obligatoria de cámaras de vigilancia en todos los establecimientos con acceso al público.[11] Estas nuevas interacciones, que salen del ámbito ciudadano-Estado, en algunos casos no solo suponen cargas administrativas sino también nuevas responsabilidades para los particulares de cara al respeto de garantías y derechos que tienen que asumir por mandato directo de la ley.

Más allá de la conveniencia de estas reformas en materia de seguridad ciudadana, es de esperar que en los próximos años el uso de información biométrica en diversos ámbitos de la vida diaria del ciudadano peruano continúe ampliándose. Además del interés de los actores locales, hay que tener en cuenta también la aparición de empresas transnacionales que emplean sistemas de identificación biométricos para ofrecer sus servicios. Así pues, si en un primer momento el

[11] Martín Borgioli, "Decreto Legislativo 1218: Un país bajo videovigilancia," Hiperderecho (blog), 2015, https://goo.gl/qkDGfW

paradigma dependía única y exclusivamente de las entidades del sector público, actualmente esta realidad se ve afectada también por la forma cómo esta tecnología evoluciona y se emplea en manos del sector privado. Un claro ejemplo de ello son los teléfonos inteligentes (*smartphones*), algunos de los cuales incorporan tecnologías de autenticación biométricas tipo AFIS desde hace algunos años.

4. Ecosistema de identificación biométrica

Hemos decidido llamar "ecosistema de identificación biométrica" al conjunto de actores relevantes que intervienen en la creación, uso o desarrollo de esta tecnología en el país. Eso incluye a entidades públicas y privadas que interactúan con la biometría, ya sea en relaciones de pares, de dependencia, de prestación de servicios, entre otros. Esta no es una lista exhaustiva, pero sí ejemplificadora, por lo que es posible que no estén registrados todos los actores de ciertos sectores.

4.1. Entidades públicas

Aquí se encuentran prácticamente todas las entidades de la Administración Pública que, en la mayoría de casos, hacen uso del sistema de identificación y verificación AFIS en calidad de "clientes internos" de RENIEC. Para la obtención de este servicio, las entidades solicitantes deben suscribir convenios de cooperación interinstitucional con RENIEC para tener acceso a sus bases de datos con el fin de verificar la identidad de las personas, ya sea empleando datos personales como el nombre o registrando sus huellas dactilares. El acceso a esta base de datos está limitado a ciertas entidades públicas y privadas que hayan suscrito un Convenio de Suministro de Información con RENIEC. Desde hace pocos años, el uso de esta base de datos es gratuita para las entidades públicas mientras que las instituciones privadas que deseen hacerlo deben de pagar aproximadamente 0.50 centavos de dólar por cada verificación.

Por otro lado, también existen otras entidades que hacen uso del AFIS o del Sistema de Verificación Biométrico (un desarrollo original de RENIEC), empleando sus propias bases de datos biométricos, que no son compartidos con otras entidades públicas. Este es el caso de la Policía Nacional del Perú, que tiene actualmente operando un sistema propio, el "AFIS Policial". El uso del AFIS Policial consiste básicamente en la contrastación de la información proporcionada por RENIEC con las bases de datos biométricos que posee la Policía (construida a partir de los registros de delincuentes reincidentes). Sin embargo, el empleo de este método no parece ser muy beneficioso para el trabajo de dicha institución, no solo en términos de eficiencia sino también porque el marco legal aplicable es limitado.[12]

Cabe resaltar que el servicio de identificación y verificación es realizado siempre por RENIEC y requiere el empleo de su software. Sin embargo, los terminales desde los cuales se recopilan los datos biométricos no son comercializados por esta institución sino por diferentes proveedores.

---

[12] Oscar Mabel Llatas Soraluz, *El registro biométrico dactilar con el sistema AFIS y el control del delito*, Pontificia Universidad Católica del Perú, Tesis para optar el Grado de Magíster en Ciencia Política (Abril, 2016), 22-30, https://perma.cc/9HR2-P5U3

Aunque depende de cada entidad seleccionar el proveedor de este hardware, RENIEC señala los siguientes requerimientos técnicos para usar el sistema de identificación biométrica:[13]

- Una PC con sistema operativo Windows 7 u 8, con 512 MB de memoria RAM, al menos 4GB de espacio de almacenamiento libre y con Java instalado.
- Una conexión a Internet de al menos 512 Mbps
- Un equipo biométrico certificado por el Federal Bureau of Investigations de Estados Unidos como dispositivo "PIV SINGLE FINGER CAPTURE DEVICES" que cumpla con las siguientes características:
    - Tipo de Sensor: Óptico (CCD o CMOS)
    - Tipo de Lector: Monodactilar para captura plana de huellas dactilares.
    - Tamaño de Captura del sensor: ≥ 12.8 mm (ancho), ≥ 16.5 mm (alto)
    - Tamaño de imagen de 512 pixels de ancho por 512 pixels de alto.
    - Resolución de 500 dpi.
    - Posibilidad de enviar imágenes en formato WSQ con un ratio de compresión de 2.0
    - Generación de imágenes en Escala de Grises de 256 tonos (8 bits), formato Mapa de Bits (BMP).
    - Conexión a PC por cable USB.
    - Compatibilidad con sistema operativo Windows 7/8 (32 bits y 64 bits)
    - USB 2.0 o superior

Adicionalmente, la propia página web de RENIEC pone a disposición del público para descarga el software controlador (driver) para los siguientes modelos de lectores biométricos:

- Crossmatch Verifier 300 LC 2.0
- nBioScan D-Plus
- nBioScan F
- Futronic FS10/FS50/FS88/FS88H
- Sagem MSO 300/350/1300/1350
- Suprema RealScan D y G1
- Suprema BioMini Slim S20 y Combo S20

[13] Registro Nacional de Identificación y Estado Civil, Gerencia de Tecnologías de la Información, "Especificaciones técnicas mínimas del lector biométrico para el acceso al servicio de verificación biométrica del RENIEC," (Julio, 2016), https://perma.cc/RWN2-LYSM

- VIRDL V-FOH04
- Dermalog F1/ZF1/ZF1+
- GreenBit DactyScan26i y DactyID20
- Secugen Hamster Pro 20 y Hamster Pro DUO SC PIV
- RTE U.are.U 5160/5300
- EikonTouch

Entidades del sector público (listadas por categoría)
Ministerios y sus dependencias
Gobiernos regionales
Organismos autónomos
Fuerzas Armadas
Policía Nacional del Perú
Embajadas
Entidades privadas que proveen servicios públicos

4.2. Entidades privadas

En el caso de las entidades privadas, identificamos dos grandes grupos. Aquellas entidades que emplean sistemas de identificación biométricos dentro de sus procesos de venta de bienes y/o servicios y las que los emplean con fines de control interno.

En el primer caso además podemos dividirlas entre las que han adoptado estos sistemas de forma voluntaria y las que lo han hecho en cumplimiento de las leyes peruanas. Entre las entidades que han adoptado la biometría de forma voluntaria se encuentran casi todas aquellas que conforman el sector financiero y sus industrias complementarias. Dada la naturaleza de los servicios que ofrecen, el poder contar con sistemas de identificación confiables es un factor crítico y por lo tanto han adoptado estas tecnologías como forma de obtener ventajas dentro del mercado. Aquí se ubican los bancos, las cajas de ahorro, las financieras entre otros. En todos los casos, estas entidades utilizan el Servicio de Verificación Biométrico, que es un sistema desarrollado por RENIEC diferente del AFIS, pero que funciona de forma similar. Para hacer uso del mismo, estos deben pagar una tarifa establecida previamente que es de aproximadamente 0.50 centavos de dólar por cada verificación. Sin embargo, a partir de la Ley N° 30693, “Ley del Presupuesto para el Sector Público del Año Fiscal 2018”, expedida a finales del año 2017, se determinó que el uso del

Sistema de Verificación Biométrica para consultas sea gratuito con motivo de contribuir a la seguridad ciudadana, para todas las entidades del sector público y privado en general.[14]

Del otro lado, existen entidades privadas que se han visto obligadas a implementar o adquirir servicios de verificación biométricos con RENIEC por disposición legal. Este es el caso de las Notarías cuando se trata de la inscripción de ciertos actos en registros públicos[15] y, más recientemente, de las compañías que comercializan líneas de teléfono móvil. Como habíamos indicado anteriormente, desde 2017 cualquier persona que quiera adquirir una línea móvil o realice cambios en la misma deberá identificarse haciendo uso de sus huellas dactilares, para lo cual las empresas que ofrecen estos servicios deben contar con terminales compatibles con el software de RENIEC.

Finalmente, encontramos el caso de las entidades privadas que emplean sistemas biométricos "internos" para cubrir necesidades como el registro y control de su personal, la asistencia, la seguridad de sus procesos y activos, etc. No hemos profundizado demasiado en esta categoría pues su impacto actualmente no es significativo, no solo porque el universo de personas afectadas por el mismo es muy reducido, sino porque los datos biométricos almacenados en estas terminales por regla general no se comparten con terceros ni forman parte de registros de uso público. En cualquier caso, esta información está protegida por las reglas generales de la Ley de Protección de Datos Personales y su compartición necesita de consentimiento expreso del titular de estos datos.

En todos los casos salvo el último, las entidades del sector privado también tienen una relación de cliente-proveedor respecto de RENIEC, en la medida en que sus sistemas de identificación y verificación requieren del software de esta entidad. De la misma forma que sus pares en el sector público, deben firmar un Convenio de Suministro de Información y pagar las cuotas establecidas por las consultadas realizadas. Cabe señalar aquí que bajo la legislación y actual y en función de las resoluciones jefaturales de RENIEC, cualquier empresa debidamente constituida puede realizar el trámite correspondiente para suscribir el Convenio, pues los únicos requisitos para hacerlo son:

- Enviar una solicitud dirigida al Jefe Nacional del RENIEC, con atención a la Oficina de Convenios, consignando nombre completo de la entidad o institución, giro de la entidad, número del Registro Único de Contribuyentes, domicilio, nombre, dirección de correo electrónico y número de documento de identidad del representante legal, justificando detalladamente de la necesidad de contar con el servicio de acuerdo al giro de la empresa, adjuntar copia del RUC, adjuntar copia del DNI del representante legal, copia legalizada de la Constitución de la entidad.

- Adjuntar a la solicitud una copia simple del testimonio de la escritura pública de constitución de la empresa, y original de la vigencia de poder otorgado por la oficina registral correspondiente con antigüedad no mayor de 30 días, adjuntar copia del RUC.

---

[14] Al momento de la edición final de este reporte, la Comisión de Presupuesto y Cuenta General de la República aprobó por unanimidad el martes 5 de junio derogar esta disposición. Entre algunos de los motivos citados están las quejas de RENIEC, que indicó haber dejado de percibir 12 millones de soles por estos servicios.

[15] Decreto Legislativo No. 1049, artículo 55.

Entidades del sector privado
Entidades bancarias y financieras
Notarías
Empresas de telecomunicaciones
Empresas en general con interés en realizar verificaciones biométricas
Empresas con equipos de verificación biométrica instalados para uso interno

4.3. Proveedores

En este apartado se encuentran entidades privadas que ofrecen básicamente dos productos: La puesta en funcionamiento de un servicio de identificación biométrico y la venta de terminales de captura de datos biométricos. Ambos se ofrecen tanto al sector público como al privado bajo diferentes tipos de contratación: licitación, venta directa, etc.

En el primer caso, la empresa más importante es Idemia (anteriormente conocida como Morpho), que soporta el servicio AFIS que ofrece RENIEC. A esta le siguen otras que ofrecen soluciones específicas a otras entidades, como ocurre en el caso del pasaporte biométrico.

Respecto de las que comercializan terminales, el mercado local es bastante diverso y ofrece todo tipo de soluciones, desde las que usan las entidades del Estado, hasta otras menos complejas o que hacen uso de otros datos biométricos como el iris, las venas de la mano, etc.

Entidades Proveedoras de sistemas de identificación
Idemia (AFIS RENIEC)
In Continue Et Services – Gemalto México S.A. (Pasaportes biométricos)
X Infotech (Pasaportes biométricos)

Entidades Proveedoras de terminales y hardware doméstico
Bionix System
IP Solutions
Sylcomtel Data Peru S.A.C
Biotronic
Otros

5. La identificación biométrica a través de sus diversas facetas

En esta sección hemos analizado la actuación de los diferentes actores del ecosistema de la identificación biométrica para ver cómo se comportan frente al cumplimiento de diferentes medidas de orden técnico y legal. Con esto queremos descubrir cuáles son los puntos fuertes y débiles de la aplicación de la biometría en el país y a quiénes corresponde su éxito o fracaso. De igual forma, hemos empleado la comparación con los modelos de biometría en Chile y Argentina para conocer nuestra situación de cara a las prácticas regionales en esta materia.

5.1. Diseño institucional

En el Perú, todos los sistemas de registro y verificación de identidad públicos se encuentran actualmente bajo el control de RENIEC, lo que incluye el sistema biométrico AFIS. Al ser la entidad que custodia la base de datos personales más completa del país, ofrece servicios de identificación al sector público y también al privado, que los contrata casi siempre de forma voluntaria, pero en ciertos casos lo hacen también obligados por la ley.

Desde su creación en 1995, RENIEC fue una entidad pensada para ser un organismo público autónomo con personería jurídica de derecho público interno y atribuciones exclusivas y excluyentes en materia registral, técnica, administrativa, económica y financiera.[16] En ese sentido, al ser un ente rector, pero también ejecutor de sus propias políticas de identificación, tuvo que expandir su presencia por todo el territorio y estructurar adecuadamente sus niveles jerárquicos y su línea de procesos.

A diferencia del desarrollo de la biometría en Argentina, en donde los sistemas de identificación incluyen a varios actores que no suelen interactuar entre sí y que tienen procesos diferenciados y no uniformes (reflejo de su sistema de gestión federal), el hecho de que RENIEC asumiera desde el inicio el control total sobre los registros de personas parece haber tenido un impacto positivo en su nivel de eficiencia y cobertura. Un indicador de ello es el bajo índice de indocumentación del país, que llegaba hasta el 1.1%, el más bajo de toda la región, según indicaba en 2016 el jefe de RENIEC, Jorge Luis Yrivarren.[17]

En el caso específico de la biometría, que en el Perú es básicamente el uso del sistema AFIS, este parece funcionar sin inconvenientes e inclusive existen plataformas especiales para las solicitudes provenientes del sector privado, especialmente de bancos y notarías. Estas solicitudes de identificación y verificación constituyen actualmente gran parte del volumen de trabajo del sistema biométrico que mantiene RENIEC y a lo largo de su existencia no se han documentado complicaciones o fallos graves en su uso. Es más, sistemas paralelos de identificación como el AFIS Policial, que es un desarrollo parecido al SIBIOS argentino, sí ha presentado muchos problemas en términos de funcionamiento y resultados.

---

16 RENIEC, "Servicio de verificación biométrica", 2012: 18-19, https://goo.gl/8E6T4p

17 Entrevista a José Luis Yrivarren, jefe de RENIEC, *El Peruano*, Junio 1, 2016, https://goo.gl/gs1yu2

5.2. Estándares y medidas de seguridad

Decíamos que RENIEC posee oficinas en todo el país con el fin de acercar sus productos y servicios a todos los ciudadanos. Sin embargo, respecto del uso de sus sistemas biométricos, la calidad no solo debería medirse en función del cumplimiento de sus cuotas de registro y verificación de datos biométricos, sino también del respeto de los estándares de seguridad para recoger y almacenar dicha información. En ese aspecto, ¿cumple esta entidad con las buenas prácticas que se aplican en la región?

En términos de estándares, existen dos gerencias que poseen certificación bajo la norma ISO 9001:2008: La Gerencia de Registros de Identificación y la Gerencia de Procesamiento de Registros Civiles. Ambas oficinas y sus dependencias están, al menos en teoría, capacitadas para procesar información biométrica de forma eficiente y segura en los procesos de: Trámites de Identificación (emisión de DNI), Depuración de Registros de Identificación, Identificación Biométrica, Administración de Documentación Registral y Atención de Información Registral.[18]

Cómo es lógico, el seguimiento de la norma ISO por parte del personal de RENIEC en estas oficinas hace suponer (y ningún hecho actual hace pensar lo contrario) que un trámite como la expedición del DNI Electrónico cumple, en todos los tramos, con medidas de seguridad de la información previamente establecidas y permanentemente evaluadas. Sin embargo, esto no se extiende a aquellas interacciones que tiene RENIEC con otras entidades del Estado y con el sector privado en donde se tratan datos biométricos.

En lo que respecta a las medidas de seguridad acerca de la recolección y almacenamiento, RENIEC afirma seguir los estándares impuestos por los proveedores de los servicios que contrata (en el caso del AFIS son los que maneja la empresa Idemia), así como la normativa peruana vigente. Si bien en el primer caso no queda claro cuáles son esos estándares pues se trata de un particular, respecto de la norma peruana, debe entenderse que se refiere a la "Norma Técnica Peruana NTP-ISO/IEC 17799:2004 EDI Tecnología de la Información", que establece buenas prácticas para la gestión de la seguridad de la información en el sector público. Esta norma, que es de obligatorio cumplimiento en todas las entidades de la Administración Pública, hace prever que, cuando menos, es exigible cierto estándar de seguridad en el tratamiento de datos biométricos. No obstante, como en el caso anterior, esto no se extiende al sector privado.

Dicho esto, al menos en el papel, el Perú parece cumplir con las prácticas regionales en el mismo sentido que Chile y Argentina, que también cuentan con certificaciones ISO 9001:2008 en las agencias que operan sus sistemas biométricos, además de normativa propia para asegurar la calidad de sus servicios. Sin embargo, pese a que no se conoce el nivel de cumplimiento de estos estándares, han existido algunos casos en donde estos claramente han sido incumplidos[19], pero sin que se tenga claro si esto ha ocurrido por fallos de seguridad o debido al error humano.

Pese a que en otras entidades del Estado se han detectado múltiples fallos de seguridad[20], producto casi siempre de la incompetencia de los funcionarios encargados del mantenimiento de

---

18 RENIEC, "Sistema de la calidad de los procesos de registros civiles," 2012, https://goo.gl/wYiNM8

19 "Revelan errores en los pasaportes biométricos", *Panorama*, 2016, https://goo.gl/T6oad2

20 Carlos Guerrero, *La encuesta virtual LGBTI 2017 pone en riesgo a todos,* Hiperderecho (blog), 2017, https://goo.gl/wzGmyb

las plataformas virtuales,[21] esto no necesariamente puede extrapolarse a RENIEC. En todo caso, no se ha registrado a la fecha ningún caso en donde se haya comprometido la integridad de los datos biométricos, se hayan producido fugas o intrusiones en las mismas. Esto no quiere decir necesariamente que estos incidentes no hayan ocurrido, pero han sido resueltos o sencillamente no son de conocimiento público.

Adicionalmente, sí tenemos noticia de al menos un caso en el que la información de las fotografías de la base de datos de RENIEC estuvo expuesta por un número no determinado de días. En abril de 2018, Hiperderecho detectó y reportó una vulnerabilidad en los sistemas informáticos de RENIEC que permitía el acceso indiscriminado a las fotografías del documento de identidad de todos los ciudadanos peruanos. El error se encontraba en la aplicación web Padrón Nominal, desarrollado por RENIEC a pedido del Ministerio de Salud, que permite la consulta del historial de salud de los menores de edad de todo el país. La vulnerabilidad consistía en que una ruta web del sistema había quedado expuesta al público y podía ser cambiada manualmente con el número de Documento de Identidad de cualquier persona para obtener su fotografía. De esta manera, no solo podían obtenerse las fotografías del documento de identidad de cualquier persona sino que la base de datos de millones de fotografías podía ser descargada total o parcialmente.

Hiperderecho reportó esta vulnerabilidad a través de la Coordinadora de Emergencias de Redes Teleinformáticas de la Presidencia del Consejo de Ministros (PeCERT). En menos de 48 horas, la vulnerabilidad había sido mitigada bloqueando el acceso completo al sistema y luego solo habilitando para ciertas IPs asociadas a los centros de salud que usaban el aplicativo. Sin embargo, no obtuvimos mayor información sobre cualquier otra medida de mitigación o corrección implementada.

5.3. Identificación biométrica y política: Propuestas populistas y de corto plazo

Quizás una de las pocas brechas en el aparentemente sólido sistema biométrico que opera RENIEC es la aparición reciente de otros actores interesados en proponer políticas públicas relacionadas al uso de la biometría. Estos actores son públicos y privados, pero la mayoría de ellos tienen diferentes propuestas sobre un tema recurrente: la seguridad ciudadana. El Perú al igual que otros países de la región ha experimentado un crecimiento del crimen en los últimos años, lo que ha disparado la sensación de inseguridad en la población, que exige medidas cada vez más drásticas.

Una respuesta desde el Estado contra este problema ha sido la expedición de todo tipo de normas con un gran efecto en la opinión pública, pero con poco sustento técnico y que no atacan el origen de la delincuencia. Por ejemplo, entre los años 2015 y 2017 se publicaron más de una decena de leyes para aumentar las penas en diferentes delitos,[22] hacer obligatorio el uso de

---

[21] Diego Escalante, *SUNEDU expuso la información personal de miles de estudiantes peruanos,* Hiperderecho (blog), 2017: https://goo.gl/zAVLpP

[22] "Poder ejecutivo modificó normas que aumentan penas contra el crimen organizado", *Diario Perú 21, 29 de octubre, 2016,* https://goo.gl/Y69Afd

cámaras de videovigilancia,[23] autorizar el acceso de datos de geolocalización de sospechosos,[24] y obligar a los usuarios de telefonía móvil a registrar sus datos biométricos para adquirir líneas nuevas o modificar las que ya tenían con el fin de prevenir la extorsión y la reventa de equipos robados.[25]

Prácticamente en todas las normas mencionadas anteriormente, la biometría juega un rol particularmente importante, lo que significa en muchos casos su uso en escenarios no contemplados por RENIEC. Por ejemplo, en el caso de la identificación biométrica para adquirir líneas móviles, no existe ningún fundamento para afirmar que esto es útil para el sistema nacional de identificación. El único motivo por el cual se creó este proceso fue para facilitar la persecución contra los delitos de extorsión, contra el cual el Estado ha probado diferentes estrategias a lo largo del tiempo, sin que ninguna sea particularmente exitosa.[26]

Del mismo modo ocurre en el caso de la norma que crea la obligación de instalar cámaras de videovigilancia con el fin de que luego sus registros puedan ser revisados para combatir la delincuencia. Pese a que no se ha dicho de forma directa, el siguiente paso de este tipo de sistemas es habilitar la identificación biométrica en vivo, algo para lo cual un sistema tan robusto como el de RENIEC pareciera estar preparado, pese a que esta entidad nunca ha contemplado este uso dentro de sus planes de trabajo. Ya ha ocurrido un caso similar en Colombia, que pone de relieve el peligro intrínseco de este tipo de políticas efectistas y de corto plazo.[27]

En este ámbito, tanto Perú como Chile y Argentina enfrentan situaciones similares. El aumento de la inseguridad sumada a la búsqueda por crédito político ha impulsado todo tipo de iniciativas que emplean la biometría como si se tratara de un arma contra la delincuencia. Por ello no es extraño ver proyectos sin ningún sustento técnico y totalmente ignorantes de las consecuencias negativas que puede tener el uso de esta tecnología para los ciudadanos. Si bien en nuestro país, estas ideas no han ido más allá de los sistemas AFIS actuales, es de suponer que con el tiempo podrían abarcar la inclusión de otros sistemas o proponer medidas aún más intrusivas y onerosas para los derechos de los ciudadanos.

5.4. Marco legal de los datos biométricos

Dentro del ámbito de uso de la biometría en el país, las normas relacionadas a derechos humanos de cumplimiento son aquellas que protegen la privacidad de la información (en este caso de los datos biométricos) y la seguridad de que esta no van a ser compartida con terceros sin el consentimiento de sus titulares. En ese sentido, la norma más importante es la Ley N° 29733, Ley

---

23 "Será obligatorio para las empresas usar videocámaras de vigilancia", *Diario Gestión,* 28 de setiembre, 2015, https://goo.gl/6CLLWw

24 "Cinco claves para entender la ley de geolocalización", *Diario La República,* 30 de julio de 2015, https://goo.gl/MfzD8u

25 "Móviles prepago se venderán solo con identificación biométrica", *Diario El Comercio,* 27 de diciembre de 2017, https://goo.gl/fbnTku

26 Carlos Guerrero, "Celulares, policías y ladrones," *Hiperderecho* (blog), 7 de julio de 2016, https://goo.gl/kTpvpc

27 Carolina Botero, "Cámaras biométricas en Transmilenio: Casi recreamos 1984," *Diario El Espectador*, 1 de febrero de 2018, https://goo.gl/dGKgNi

de Protección de Datos Personales (LPDP)", su Reglamento y las leyes conexas. La encargada de velar por su cumplimiento es, en primera instancia, la Autoridad de Transparencia, Acceso a la Información y Protección de Datos Personales.

A diferencia de Chile, en donde no es explícito ni existe una autoridad semejante, en la sección de Disposiciones Generales de la LPDP peruana se dice específicamente que los datos biométricos están considerados como "datos sensibles" y por lo tanto se encuentran en el máximo grado de protección. Además, que dicha norma aplica tanto para los bancos de datos administrados por entidades públicas y privadas. Sin embargo, también se citan algunas excepciones, entre las cuales se encuentra una que indica que la Ley no aplica en los casos en que estos datos son tratados (sin autorización) en cumplimiento de los objetivos de las entidades públicas, para la defensa nacional, seguridad pública, y para el desarrollo de actividades en materia penal para la investigación y represión del delito.

De lo anterior se desprende que siempre que los datos (biométricos o no) sean recogidos, almacenados y tratados por entidades privadas, estas están obligadas sin excepción a seguir lo que la Ley de Protección de Datos Personales ordena, la cual posee diferentes mecanismos para asegurar el respeto del derecho a la privacidad y a la autodeterminación informativa. Esto significa que entidades como los bancos, las notarías o las empresas de telecomunicación que emplean terminales para registrar datos biométricos, están obligados a mantener niveles de seguridad óptimos y a disponibilizar medios para que los usuarios puedan saber cómo se tratan sus datos y puedan ejercer los derechos ARCO.[28]

Diferente es el caso de las entidades públicas en donde, si bien el cumplimiento también es obligatorio, este puede dejar de observarse en las situaciones arriba mencionadas. Lamentablemente no existe suficiente material normativo que desarrolle de forma más amplia el contenido de estas excepciones, salvo un pronunciamiento reciente de la Autoridad de Protección de Datos personales que reafirma que, en principio las entidades del sector público deben cumplir con los mismos estándares de la LPDP, lo que incluye crear y mantener medidas de seguridad para evitar la vulneración de los datos personales recopilados y ser pasibles de sanciones administrativas si no lo hacen.[29]

En definitiva, el nivel de cumplimiento de las normas que protegen derechos humanos que podrían estar comprometidos por las prácticas de biometría del sector público no es claro. Si bien no existen precedentes de abuso o casos públicos en donde se haya probado la violación del consentimiento en el uso de los datos personales de algún ciudadano, eso no significa que no estén ocurriendo y no sean de conocimiento público. Además hay que tener en cuenta los peligros inherentes al uso intrusivo de algunas iniciativas que buscan fortalecer la seguridad ciudadana a costa de la inseguridad de la privacidad.

---

[28] Ministerio de Justicia y Derechos Humanos, "El derecho fundamental a la protección de datos personales" (2013), https://goo.gl/pRkSqv

[29] Dirección General de Transparencia, Acceso a la Información Pública, y Protección de Datos Personales, Informe N° 27-2017 -JUS/DGTAIPD-DPDP, Noviembre 17, 2017, https://goo.gl/gJFo8M

6. Conclusiones

Tenemos un sistema de identidad biométrica centralizado por diseño

RENIEC es un organismo bien consolidado en el país con capacidad operativa suficiente para el mantenimiento del actual sistema biométrico AFIS, así como para la expansión de su catálogo de servicios de identificación orientados al sector público y privado. Es de prever que con el paso de los años, el nivel de dependencia que tiene la mayoría de entidades del sector público crezca y se incrementa la demanda en el sector privado.

No obstante, el ser el organismo más importante para el funcionamiento de los sistemas biométricos actuales también tiene un problema. Si en algún momento y por cualquier motivo (ataque, catástrofe natural, captura política, etc.) RENIEC no puede asegurar la continuidad de sus operaciones o a veracidad de su información, todo el sistema colapsará. Esto nos hace pensar que debería existir alguna clase de respaldo o un sistema de identificación alternativo para este tipo de contingencias. De la misma manera, al funcionar como un sistema centralizado también se convierte en un solo punto de ataque de agentes maliciosos. Es decir, un error o vulnerabilidad en este sistema puede abrir el acceso a todos los datos que contiene y comprometer la integridad de la base de datos en su totalidad. De momento en la región no hay ejemplos de este tipo, pero no se puede perder de vista lo ocurrido en Corea del Sur, uno de los países con sistemas de identificación más avanzados del mundo, en donde un ataque expuso la información de casi la totalidad de su población.[30] Una alternativa a este modelo centralizado podría ser un sistema de bases de datos modulares que se articulen entre sí pero que por diseño sean independientes.

No existe suficiente competencia en el mercado local de los sistemas biométricos

Además de Idema y Gemalto, responsables por la puesta en funcionamiento del AFIS de RENIEC y el pasaporte biométrico respectivamente, no existen otras empresas que generen un ambiente de mayor competencia en el país. Esto se debe probablemente a que la usuaria más grande de los sistemas biométricos es RENIEC y que los demás actores no necesitan soluciones tan complejas. Si bien esto no tendría por qué significar un problema, sería conveniente que en futuros desarrollos, RENIEC decida contratar con diferentes empresas (internacionales y locales), especialmente de aquellas que ofrezcan un mayor grado de transparencia respecto de sus operaciones. Al mismo tiempo, otro elemento que limita la competencia en el mercado son las restricciones impuestas por la plataforma misma de RENIEC que hace imposible que se usen los equipos que no son compatibles con su sistema.

El ecosistema de identificación biométrica necesita fiscalizadores

Notamos una gran ausencia de actores de los sectores público y privado que vigilen de forma sostenida el desarrollo e implementación de las políticas de identificación biométrica de RENIEC. Pese al papel que algunas entidades como la Autoridad de Transparencia y Protección de Datos Personales y la Defensoría del Pueblo podrían jugar en este esquema, su acción en este ámbito es incierta y no existen pronunciamientos públicos al respecto.

---

[30] Iain Thompson, "South Korea faces $1bn bill after hackers raid national ID database," *The Register*, Octubre 14, 2014, https://goo.gl/3mDp7u

En cuanto a las empresas y los emprendimientos, estos parecen divididos entre aquellos que muestran interés en las posibilidades que ofrece la identificación biométrica o ya han empezado a utilizarla dentro de sus procesos; y aquellos a las que su uso les ha sido impuesto por la ley. Sin embargo, aún en el caso del último grupo, no se percibe una intención de vigilancia que vaya más allá de denuncias puntuales para evadir responsabilidades y costos de estas operaciones.

Finalmente, en lo que respecta a las organizaciones de sociedad civil, no existe un entendimiento suficiente sobre lo que implica el uso de la biometría y por lo tanto es muy poco el nivel de incidencia en estos temas, aún dentro de los grupos de activismo de derechos humanos. Si bien es cierto que la situación actual no permite pensar que hacen falta grandes movimientos sociales para impedir situaciones de abuso de datos biométricos o vigilancia masiva, el tener actores enfocados en el bienestar de los ciudadanos parece algo importante. Inclusive, pensamos que esta tarea no solo podría ser asumida en estricto por organizaciones de derechos humanos sino también por asociaciones de defensa del consumidor, desde que existen muchos usos de la biometría vinculados a la compra de bienes y servicios.

Los nuevos actores están desnaturalizando el uso de la biometría

Cuando iniciamos esta investigación, nuestra hipótesis inicial era que la amenaza que supone el uso de la biometría para ciertos derechos era inherente a la forma en que esta había sido implementada en el país. Por el contrario, todo el desarrollo llevado a cabo por RENIEC en materia de biometría pareciera, al menos en teoría, respetuoso de estándares internacionales de protección de la privacidad y con una clara vocación de habilitador de servicios para el ciudadano.

En cambio, han sido las recientes políticas que hacen un uso de la biometría las que pueden constituirse en peligrosos para el ejercicio de los derechos humanos. En general, estas provienen de entidades ajenas al ecosistema de la biometría y que simplemente han empleado esta herramienta para mejorar sus propios procesos o para obtener créditos políticos, especialmente cuando se trata de actuar por la seguridad ciudadana. Prueba de ello son las normas mencionadas en el punto anterior, respecto del marco regulatorio.

La sociedad civil organizada debe empezar a cuestionar los caminos que está tomando la biometría

Ante la situación descrita en el punto anterior, es imperioso que las organizaciones de sociedad civil y otros actores interesados hagan causa común para alertar a la población sobre los riesgos que reviste el uso de la biometría que proponen estos nuevos actores. Para ello también pueden involucrarse entidades del sector privado que también son afectadas por estas iniciativas. Parece ingenuo pensar que es posible desandar todo el camino y regresar a sistemas de identificación no biométricos, pero en cambio es factible asegurarnos de que los actuales cumplan funciones muy específicas orientadas al bienestar y no a fomentar estados de vigilancia.

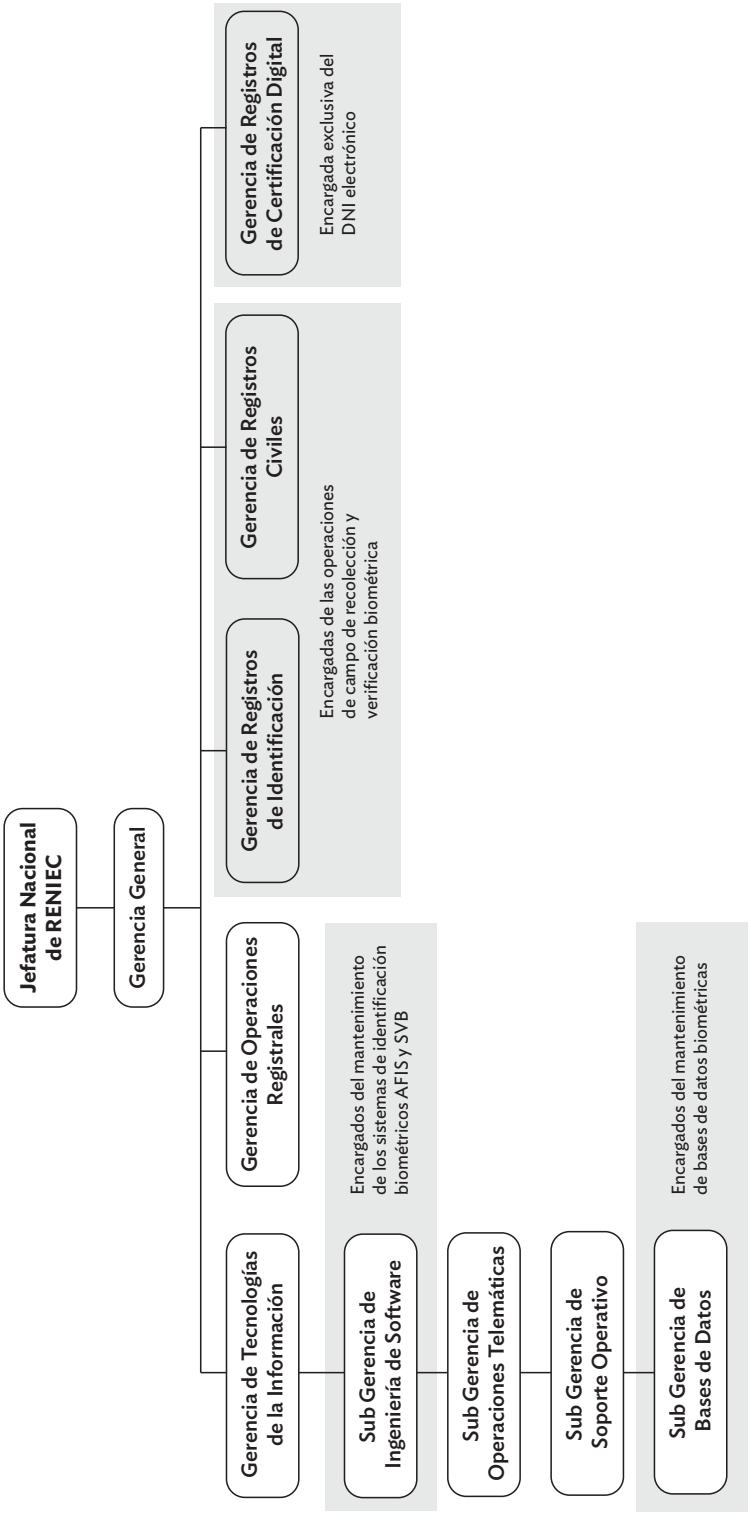
Existe una amplia agenda pendiente de investigación sobre identidad biométrica en Perú

A lo largo de esta investigación, hemos identificado la necesidad de abordar a profundidad sobre diversos aspectos específicos de la identidad biométrica en Perú. La agenda pendiente de investigación incluye una mejor comprensión de cómo resulta aplicable o no la Ley de Protección de Datos a casos específicos de compartición de información en el Estado, el funcionamiento y la seguridad de los documentos de identidad electrónicos peruanos como el Pasaporte Electrónico o

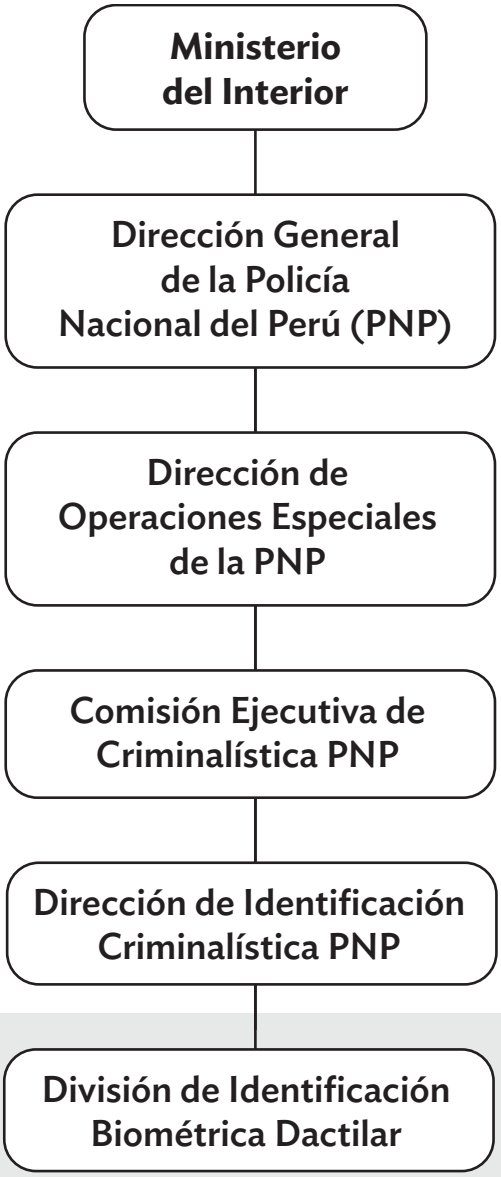
el DNI Electrónico, una mirada completa a los registros alternativos de datos biométricos como el AFIS policial, una auditoría independiente de seguridad informática a estos sistemas, entre otros. En muchos casos, estas investigaciones no solo requieren de una investigación legal sino también técnica que pueda entender los requerimientos y diseños técnicos del sistema desde una mirada crítica.

7. Anexos

7.1. Ecosistema de identificación biométrica en Perú



7.2. Organigrama del AFIS Policial



Gestiona el AFIS Policial que usa el servicio AFIS de RENIEC pero se apoya en bases de datos propias de la PNP

7.3. Modelo de Convenio suscrito entre RENIEC y una entidad privada

CONVENIO DE CONSULTAS EN LÍNEA DE VERIFICACIÓN BIOMÉTRICA ENTRE EI REGISTRO NACIONAL DE IDENTIFICACIÓN Y ESTADO CIVIL Y [EMPRESA …]

Conste por el presente documento, el Convenio que celebran de una parte el REGISTRO NACIONAL DE IDENTIFICACIÓN Y ESTADO CIVIL, con RUC No 20295613620, con domicilio en Av. Bolivia 109 Centro Cívico Piso 30, Lima debidamente representado por su Gerente General, señor Luis Alberto, Bullon Salazar identificado con DNI No. 07837877, autorizado mediante Resolución Jefatura! No 94-2016/JNAC/RENIEC de. fecha 18 de julio de 2016, en adelante El RENIEC; y, de la otra parte [EMPRESA ….] con RUC No […], con domicilio en […], representada por […] en adelante EL USUARIO; en los términos y condiciones siguientes:

CLÁUSULA PRIMERA.- ANTECEDENTES

EL RENIEC es un organismo autónomo creado por mandato de la Constitución Política de 1993, regulado por las Leyes No 26497 y 26859, y el Decreto Supremo N° 015-98-PCM, como Registro Público encargado, entre otras funciones, de organizar y mantener el Registro Único de Identificación de las Personas Naturales.

EL USUARIO es una entidad dedicada a […].

CLÁUSULA SEGUNDA.- DEL USO DE LA INFORMACIÓN

EL USUARIO requiere que EL RENIEC, le suministre información relativa a la identidad de las personas que obran en el Registro Único de Identificación de las Personas Naturales. para verificar la identidad de los ciudadanos.

Se deja expresa constancia que EL USUARIO no cuenta con autorización de ninguna de las formas para almacenar, transferir electrónicamente, entregar de manera gratuita o vender la base de datos que EL RENIEC suministra en virtud de este convenio, pudiendo tan solo emplear la información suministrada como medio de consulta.

EL USUARIO, se compromete a dar estricto cumplimiento a las condiciones expuestas en el párrafo anterior, de verificarse su incumplimiento a través de las acciones de fiscalización que realizará EL RENIEC de manera selectiva, será sujeto a una penalidad por incumplimiento ascendente a trescientas (300) Unidades Impositivas Tributarias (UIT) vigentes a la fecha de incumplimiento.

CLÁUSULA TERCERA.- OBJETO DEL CONVENIO

Por el presente convenio, EL RENIEC brindará a EL USUARIO los siguientes servicios:

1) Servicio de Verificación Biométrica

Este servicio permitirá la verificación de las impresiones dactilares de los ciudadanos que requiera consultar en forma directa con la base de datos de EL RENIEC; para tal efecto EL RENIEC entregará a EL USUARIO una(s) cuenta(s) con su(s) correspondiente(s) clave(s) personal(es).

Asimismo, EL USUARIO deberá adquirir los equipos de captura de huellas dactilares, de acuerdo a las especificaciones técnicas proporcionadas por EL RENIEC.

CLÁUSULA CUARTA.- DE LA INFORMACIÓN RELATIVA A LA INTIMIDAD DE LA PERSONA

EL RENIEC no proporcionará información alguna que afecte la intimidad de las personas, salvo que medie mandato judicial expreso.

CLÁUSULA QUINTA.- DEL COSTO DEL SERVICIO

EL USUARIO se obliga a pagar el costo del servicio objeto del presente convenio, que se fija mensualmente de acuerdo al básico mensual y al consumo adicional efectuado en base a la tasa fijada por el TUPA/RENIEC, vigente al momento de la prestación del servicio.

CLÁUSULA SEXTA.- DEL PAGO DEL SERVICIO

Dentro de los siete (07) días hábiles siguientes al cierre de cada mes, EL RENIEC presentará a EL USUARIO un reporte (liquidación) de las consultas realizadas por este último durante ese periodo, de conformidad con lo previsto en el TUPAIRENIEC, vigente a la fecha de la prestación del servicio.

Dicho importe deberá ser pagado en su totalidad por EL USUARIO ante la entidad bancaria y en la forma que se detalla en la declaración que forma parte integrante del presente convenio dentro de los siete (07) días calendario siguientes a la fecha de recepción del reporte antes referido.

Si vencida la fecha de pago, EL USUARIO se encuentra moroso, EL RENIEC suspenderá el servicio automáticamente.

Queda expresamente convenido que los reclamos de EL USUARIO respecto del servicio prestado por EL RENIEC durante el mes sujeto a cobro, se resolverán entre el funcionario designado en el presente documento como coordinador interinstitucional, previo pago del importe señalado en el reporte de consultas realizadas.

En caso que EL RENIEC considere que el reclamo de EL USUARIO es irrefutable, el cobro indebidamente efectuado será devuelto a EL USUARIO dentro de los siete (07) días útiles siguientes.

CLÁUSULA SÉTIMA.- DE LA DURACIÓN DEL CONVENIO Y MODIFICACIONES

El presente convenio tiene un plazo de duración indeterminada, a partir de la fecha de suscripción de este documento.

La modificación o ampliación de este convenio necesariamente requerirá acuerdo escrito de ambas partes, mediante Addendum.

CLÁUSULA OCTAVA.- DE LA COORDINACIÓN INTERINSTITUCIONAL

Las partes acuerdan que para el adecuado cumplimiento de lo previsto en el presente Convenio, EL USUARIO establece como **funcionario encargado de la coordinación interinstitucional** a la siguiente persona: […]

EL RENIEC, por su parte, designa para iguales efectos, a los siguientes funcionarios

- OFICINA DE CONVENIOS
- EL GERENTE DE TECNOLOGIA DE LA INFORMACIÓN

CLÁUSULA NOVENA.- DE LAS PERSONAS AUTORIZADAS AL USO DE CLAVES O PASSWORDS

Se deja expresa constancia que EL RENIEC entregará en sobre cerrado las claves de acceso sólo a las personas designadas por EL USUARIO en la declaración que forma parte integrante del presente convenio. quienes quedan obligadas a utilizar dichos passwords de manera personalísima, sin posibilidad de divulgarlos y guardando la confidencialidad necesaria por cuanto han sido designados como los únicos funcionarios autorizados para el uso de dichas claves.

Queda expresamente establecido que ningún funcionario de EL USUARIO encargado del uso de las claves de acceso podrá delegar tal facultad en otro funcionario. Todo cambio o adición de funcionarios autorizados para el uso de claves deberá ser comunicado ante la Gerencia General. por el Coordinador Interinstitucional de EL USUARIO, a efecto de modificar la declaración de personas autorizadas y generar nuevos passwords, los que igualmente serán entregados en sobre cerrado.

CLÁUSULA DÉCIMA.· DE LA RESPONSABILIDAD DE EL RENIEC

EL RENIEC no se hará responsable por la suspensión o retraso en el suministro de información objeto de este convenio. derivado de un caso fortuito o fuerza mayor. o cuando se haya originado de un pedido de EL USUARIO, omitiendo o contraviniendo lo previsto en el presente convenio y/o addendum que formen parte del mismo.

La información contenida en el Registro Único de Identificación de las Personas Naturales se encuentra sujeta a la Ley del Procedimiento Administrativo General No 27444, por lo que, cualquier inexactitud o irregularidad derivada de la captura de datos realizada al amparo de las mismos no será imputable a EL RENIEC.

CLÁUSULA DÉCIMO PRIMERA.· DE LA RESPONSABILIDAD DE EL USUARIO

EL USUARIO se obliga de manera expresa, sin que se admita excepción alguna, a guardar estricta reserva de toda información o datos que se le suministre y/o en general a que tenga acceso en la ejecución de este convenio.

Queda igualmente prohibido que EL USUARIO haga uso de la información proporcionada por EL RENIEC para fines distintos a las funciones administrativas e internas que le son propias, así como a aquellos previstos en este documento.

EL USUARIO se compromete a mantener en reserva las claves, códigos y otros elementos lógicos que EL RENIEC ponga a su disposición o en su conocimiento para que se pueda concretar la prestación del servicio, aplicando todas las medidas de custodia y protección que estuvieran a su alcance. En el improbable caso que EL USUARIO tomara conocimiento de que la reserva de tal información o elementos pudieran haber llegado a verse comprometida lo comunicará de inmediato a través de su coordinador intennstitucional mediante carta notarial dirigida a la Gerencia de Tecnología de la información de EL RENIEC para que se apliquen las medidas de seguridad que la situación requiera y se adopten las acciones que el caso amerite.

Se de¡a expresa constancia que EL USUARIO es responsable de la totalidad de consultas realizadas mediante el password asignado por EL RENIEC, antes de la recepción de la carta notarial precitada, salvo que EL USUARIO acredite lo contrario mediante prueba irrefutable

CLÁUSULA DÉCIMO SEGUNDA.- DE LA RESOLUCIÓN DE CONVENIO

Cualquiera de las partes podrá resolver el presente convenio Para tal efecto EL USUARIO deberá cursar carta notarial a EL RENIEC. con una anticipación no menor de treinta (30) días calendario anterior a la fecha en que se desea deja sin efecto el convenio EL USUARIO asumirá el costo del servicio hasta 30 días después de la recepción de la Carta Notarial mencionada por EL RENIEC.

CLÁUSULA DÉCIMO TERCERA.- DE LAS FACULTADES DE EL RENIEC

EL RENIEC se reserva el derecho de fiscalizar y verificar el adecuado cumplimiento de este convenio. así como la facultad de resolverlo de pleno derecho y sin que medie comunicación previa ni posteriores reclamos indemnizatorios de EL USUARIO, en los siguientes casos:

A.Estado de Insolvencia.

B.Uso inadecuado de la información a que tiene acceso mediante este convenio y/o divulgación de dicha información mediante venta, distribución. transferencia electrónica o entrega gratuita a terceros. entre otras modalidades.

C.Incumplimiento en el pago por dos (02) meses consecutivos.

D.Negativa de EL USUARIO a presentar documentación; impedir inspecciones y demás requerimientos de EL RENIEC destinados a fiscalizar el adecuado uso del servicio, así como de la información a que EL USUARIO tiene acceso

E.Otros que previa comprobación de los hechos, irroguen daños y/o afecten los intereses de EL RENIEC

CLÁUSULA DÉCIMO CUARTA.- DEL LÍMITE EN EL CONSUMO DE CONSULTAS EN LINEA

EL USUARIO autoriza a EL RENIEC a establecer un limite en el consumo diario del servicio de las consultas en linea, de verificación biométrica, consistente en _____ consultas diarias por usuario.

Se deja expresa constancia que cuando EL USUARIO requiera un consumo diario adicional, deberá solicitarlo por escrito presentado por el Coordinador Interinstitucional ante la Gerencia General de EL RENIEC. EL USUARIO será responsable de los costos que genere el consumo adicional solicitado.

CLÁUSULA DÉCIMO QUINTA.- DE LA JURISDICCIÓN

Queda expresamente convenido que las partes se someten a las leyes peruanas. Asimismo. las partes se someten expresamente a la jurisdicción de los Jueces y Cortes del distrito judicial del Cercado de Lima, en caso de cualquier controversia derivada de la aplicación y/o interpretación del presente convenio, para lo cual ratifican como sus domicilios. los consignados en la introducción del presente documento.

Asimismo, declaran que sus domicilios son los indicados en este convenio, en donde válidamente se enviarán comunicaciones, requerimientos extrajudiciales y/o notificaciones que resulten necesarios. Cualquier cambio de domicilio deberá ser comunicado dentro de los cinco (05) días hábiles de ocurrido el hecho.

Ambas partes declaran estar de acuerdo con el contenido de todas y cada una de las cláusulas que forman el presente convenio, en virtud de lo cual lo suscriben por duplicado del mismo tenor, en la ciudad de Lima, a los _____.

[FIRMAS]

Esta investigación ha sido financiada gracias al apoyo de Privacy International.