
DERECHOS
DIGITALES
América Latina
EL CUERPO COMO DATO
MARIANNE DÍAZ

Este trabajo fue posible gracias al apoyo de Ford Foundation”

Edición: Juliana Guerra
Portada y diagramación: Constanza Figueroa
Junio 2018.

RESUMEN

El acelerado crecimiento en el uso de tecnologías biométricas para la identificación en América Latina plantea una serie de cuestionamientos relativos no solo al impacto de estas tecnologías sobre la libertad de expresión y de acción en espacios públicos, sino a la autonomía y a la identidad del individuo. La creación de estándares mínimos para la implementación de sistemas biométricos en América Latina resulta urgente; sin embargo, incluso en los casos en que existen regulaciones en materia de datos personales, estas pueden resultar insuficientes para enmarcar la relación particular entre la persona y el dato derivado del cuerpo, lo que exige un debate más amplio con respecto a la naturaleza del dato biométrico en su relación con la identidad del individuo.

Palabras clave: *biometría, datos personales, identidad, autonomía, América Latina*

CONTENIDO

1. RESUMEN EJECUTIVO

Esta investigación explora las relaciones entre el cuerpo y el dato biométrico, a través de los diferentes enfoques legislativos que buscan explicar la naturaleza de los datos personales, de los datos derivados del cuerpo y del cuerpo mismo y sus partes. Dado que el dato biométrico surge a través de un proceso de registro o codificación de aspectos materiales (el iris, la huella dactilar, el rostro) o inmateriales (la manera de caminar o el patrón de tecleo) del cuerpo humano, creemos necesario explorar la naturaleza del cuerpo como elemento de la identidad, incorporando perspectivas desde diversas áreas del conocimiento, así como la naturaleza del dato biométrico, ya sea abordándolo como parte o derivado del cuerpo humano, o como elemento constitutivo de una identidad compuesta por múltiples capas.

Partiendo de estas nociones, exploramos los riesgos que presenta la implementación de tecnologías biométricas en sus diferentes formas. Al igual que otros sistemas utilizados para el control social, la biometría plantea potenciales violaciones a las libertades de expresión, asociación e información, a través del efecto de enfriamiento, analizado desde hace décadas como efecto directo de la vigilancia masiva. Menos analizados son, por otra parte, los potenciales efectos de discriminación de poblaciones minoritarias (personas con discapacidad, personas transgénero, miembros de religiones minoritarias) a causa de la naturaleza misma de los sistemas biométricos e identitarios en general, que buscan clasificar al individuo como parte de una taxonomía predefinida, dejando fuera a todo aquel que no encaje correctamente en las categorías establecidas.

Por último, analizamos brevemente diversas formas de implementación de tecnologías biométricas en algunos países de América Latina, sin ánimo exhaustivo y con el interés de analizar las posibles implicancias de estos sistemas en los derechos humanos de las poblaciones afectadas, en el contexto específico de las regulaciones existentes en cada país. Este análisis nos permite identificar ciertas tendencias y, como consecuencia, plantear algunas conclusiones y recomendaciones de cara a la eventual creación de estándares legislativos en torno a las tecnologías biométricas en la región.

2. GENERALIDADES

La biometría funciona sobre la base del supuesto de que ciertos rasgos físicos o conductuales son únicos al individuo, ya sea por sí solos o en combinación con otros; y a partir de estos datos, transformados en una plantilla (la representación digital de este rasgo), se crea la posibilidad de la identificación o la autentificación del individuo (Torrano & Barrionuevo, 2016). La autentificación, o el modelo biométrico de uno contra uno, consiste en comparar uno o más rasgos de un individuo con una plantilla correspondiente a la identidad de ese mismo individuo, es decir, es un proceso mediante el cual se verifica la declaración de identidad hecha por una persona en cuyo poder reside, por ejemplo, un carnet de identidad. La identificación, por su parte, es una comparación de uno a muchos, lo que significa que requiere una base de datos que contiene los rasgos biométricos de un grupo determinado de individuos, almacenados en una base de datos centralizada, con la finalidad de: a) determinar si el individuo en cuestión se encuentra en esa base de datos (por ejemplo, en un modelo de entrega de servicios asistenciales), o b) identificar quién es el individuo dentro del rango de esa base de datos (por ejemplo, en el caso de la búsqueda de un sospechoso en una base de datos de antecedentes penales) (Kindt, 2007).

Durante las últimas décadas, países desarrollados y en desarrollo han impulsado la adopción de tecnologías de reconocimiento biométrico para un amplio rango de fines, desde avanzar planes de identificación universal de la población hasta llevar a cabo procesos electorales o facilitar la entrega de servicios básicos y asistenciales (Privacy International, 2013). Los sistemas basados en la identificación biométrica son vistos como un mecanismo más seguro para garantizar la identificación legal de un individuo, y mientras los mecanismos analógicos de reconocimiento –como las huellas digitales convencionales– han sido usados desde mucho antes del desarrollo de las tecnologías digitales, el crecimiento de la adopción de sistemas biométricos se debe a la evolución acelerada del sector tecnológico (Mordini & Massari, 2008).

Cualquier característica, biológica o de comportamiento, puede ser empleada como identificador biométrico, siempre que cumpla con cuatro requisitos básicos: la coleccionabilidad, o la posibilidad de ser medido; la universalidad, o la existencia del elemento en todas las personas; la unicidad, o el hecho de que el elemento sea distintivo a cada persona; y la permanencia del elemento en el tiempo (Mordini & Massari, 2008).

Las preocupaciones relativas a la implementación de tecnologías biométricas son, pues, de diversa índole, y dependerán de las características específicas de la tecnología implementada, las consideraciones relativas a regulaciones y políticas públicas, y la naturaleza del contexto social. De entrada, el uso de tecnologías biométricas con funciones de identificación presenta problemas mucho más urgentes que su uso con fines de autentificación, puesto que la creación de una base de datos centralizada de los rasgos biométricos de un grupo de individuos hace surgir una serie de riesgos de seguridad y privacidad atingentes al hecho de que los datos no se encuentran bajo el control de la persona, sino

de un gobierno o una empresa a cuyo cuidado y administración se somete la base de datos (Kindt, 2007).

Sin embargo, saltar directamente a la discusión meramente legislativa respecto a la administración de los datos biométricos en cuanto datos personales omite una discusión fundamental sobre la naturaleza del dato biométrico en cuanto a su relación con la identidad del individuo y con el cuerpo como elemento del yo. La captura y digitalización del cuerpo para convertirlo en dato, a través del proceso comúnmente denominado 'informatización del cuerpo', nos remite al proceso de desmaterialización analizado por Baudrillard (Higgs & Caplan, 2013), en que el cuerpo progresa de cosa a mercancía, a signo, a mera información; un proceso que algunos argumentan podría deshumanizar el cuerpo y de este modo, ofender el núcleo mismo de la dignidad humana (Mordini, 2008).

Desde la bioética se ha debatido durante décadas la naturaleza del cuerpo y de los derechos que, como individuos, albergamos sobre este. De acuerdo con esta perspectiva, las aproximaciones jurídicas del cuerpo como la propiedad, la integridad y la autonomía, además de ser casi siempre excluyentes, resultan insuficientes por sí solas para definir la relación entre un individuo y su cuerpo (Herring & Chau, 2007).

3. NATURALEZA JURÍDICA DEL DATO BIOMÉTRICO

¿Somos nuestros cuerpos, o son nuestros cuerpos parte de nosotros? Si bien este debate corresponde a la esfera filosófica, es imposible de evadir si intentamos determinar el abordaje jurídico del cuerpo y, como consecuencia, de su digitalización. El enfoque tradicional de las normativas sobre datos personales apunta a reconocer nuestra relación con el dato como parte del ámbito de la protección de nuestra intimidad y autodeterminación informativa (Sanz Salguero, 2016), y a caracterizar el enfoque de la propiedad como problemático, dado que entender el dato personal como propiedad implica aceptar la existencia de un mercado donde los datos personales pueden ser objeto de intercambio y compraventa (Schwartz, 2003).

Respecto a la privacidad en relación con las tecnologías biométricas, es clara la exigencia de que previo a su implementación exista un marco legislativo de protección de datos personales. La ausencia de dicho marco -demasiado frecuente- tiene una incidencia social y ética sobre las libertades individuales (Privacy International, 2013).

No obstante, si bien este enfoque es correcto y lógico cuando se trata de datos personales, es insuficiente para el abordaje legislativo de los datos biométricos. Desde el momento mismo de su recolección, los datos biométricos pueden causar una serie de preocupaciones e incomodidades relacionadas con normas culturales, miedos y circunstancias contextuales y sociales. En ciertas culturas o religiones, los procesos de recabar las huellas digitales o el iris del ojo pueden resultar invasivos, incómodos o humillantes; los niños y adultos mayores pueden sentir temor a las máquinas que deben entrar en contacto con sus cuerpos; las personas discapacitadas y LGBTQI pueden verse excluidas, afectadas o discriminadas a través del proceso de categorización y clasificación de sus cuerpos mediante parámetros de lo que se defina como “normal” (Wickins, 2007). Por otra parte, si bien la implementación a escala colectiva de tecnologías biométricas suele presentarse como una herramienta para incrementar la seguridad y la “confianza” en las relaciones con las estructuras de poder, suele generar el efecto contrario en los colectivos vigilados (Zureik & Hindle, 2004), causando miedo y desconfianza en las instituciones, así como un posible enfriamiento de la participación cívica por parte de segmentos completos de la población (Vagle, 2016).

Así, mientras que la ética médica tradicional sostiene el concepto de consentimiento informado sobre la base del derecho a la autonomía y autodeterminación del individuo –al punto que, por ejemplo, tomar muestras de ADN de una persona, inclusive de un recluso, pone en tela de juicio sus derechos a la integridad personal–, el derecho sobre los datos biométricos ha sido sostenido únicamente en la base del derecho a la privacidad y a la protección de datos personales (Gemalto, 2018), incluso al referirse a estándares de consentimiento informado, aunque el carácter automatizado de la mayoría de las prácticas de recolección de datos biométricos excluye por sí misma la posibilidad del consentimiento previo (Bourcha, Deftou, & Koskina, 2017). En este sentido, el

acto de captar una huella digital o un rostro no se considera una violación a la integridad personal (Sutrop, 2010), a pesar de que implica una afectación clara al control sobre el propio cuerpo.

Para Van der Ploeg (2007), esta diferenciación llama a reconceptualizar lo que consideramos cubierto por el concepto de integridad personal y particularmente sobre la arista de la integridad física, señalando que al extraer ADN de un individuo, lo que compromete la integridad no es el acto mismo del contacto con el cuerpo –difícilmente una intromisión por cuanto basta con un cabello tomado de la ropa–, sino la información que se genera sobre el cuerpo, los análisis y procesos que se llevan a cabo sobre esa información, y el conocimiento sobre la persona que se hace posible como consecuencia de ello. La informatización del cuerpo reconstruye y transforma la identidad del individuo, por cuanto la lectura del cuerpo a través de máquinas y procesos tecnológicos revela una cantidad de información sobre la persona que anteriormente era desconocida, posiblemente incluso para ella misma.

De este modo, la biometría 'filtra' el cuerpo y lo inscribe en un espacio de poder (Foessel & Garapon, 2006). El 'individuo' se convierte en 'persona' solo cuando posee una identidad reconocible, cuando se convierte en una realidad abstracta, en un signo.

Refiriéndose a los datos biométricos, Anton Alterman (2003) señala que la privacidad es el control sobre cómo y cuándo se comunican a otros las representaciones sobre nuestra identidad, y que cuando la "parte de nosotros" que es utilizada para preservar nuestra identidad –es decir, entregada a otros para su autenticación– sale de nuestro control y es digitalizada, es difícil recapturarla y recuperar ese control.

Afirmar que el uso de los datos extraídos del cuerpo solo afecta a la información y no al cuerpo mismo niega la relación inextricable entre esas piezas de información y la dignidad del cuerpo al que se refieren. Por ende, entender los datos biométricos en la misma extensión y sentido que los datos personales (como la dirección, o el número telefónico de un individuo) niega la importancia central de la corporalidad en cuanto a la identidad del individuo.

3.1. IDENTIDAD, AUTONOMÍA E INTEGRIDAD

Como argumenta Alterman, los derechos centrados en el cuerpo como una parte integral del yo existen para crear una zona personal inviolable que proteja los aspectos emocionales y físicos del individuo: las libertades de movimiento, integridad personal, privacidad, intimidad y autonomía. En consecuencia, existe un interés moral en evitar la alienación entre el yo psicológico y el yo biológico, dado que la integración entre ambos es una precondición de nuestra capacidad de estar en el mundo y experimentarlo a través de nuestra agencia como individuos.

Este interés moral lleva a la creación de garantías que buscan proveernos de

cierto grado de control sobre la manera en que nos representamos ante otros, tanto en nuestra apariencia física como en representaciones proyectadas, icónicas o simbólicas. Así, la necesidad de tener control sobre nuestro yo, como característica del derecho a la integridad (en su dimensión corporal tanto como en sus dimensiones psíquica y moral), es también la necesidad de poder evitar ser representados en formas que puedan causarnos algún daño -físico o psicológico-, que afecten nuestra autonomía o nuestra dignidad.

Así, Van der Ploeg (2002) señala que la ontología del cuerpo en la cual los aspectos fisiológicos y anatómicos constituyen un límite o frontera para la delimitación conceptual, no es otra cosa que una construcción histórica y, como tal, una noción obsoleta que se encuentra continuamente con dificultades de aplicación a medida que la realidad avanza y se ve mediada por el uso de tecnología. Pero los datos acumulados a través del rastreo, el registro y la vigilancia del individuo crean una entidad -nueva, si bien no separada- que refleja, media e interactúa con el individuo, y en el contexto de dicha relación, el yo digital, también llamado "data döppelganger" y "sombra digital", modifica la identidad percibida y proyectada (Ruyg, 2016). Sin embargo, al definir el cuerpo como una entidad que remite únicamente a la realidad biológica, dividimos el yo y la representación del yo: mientras el cuerpo se considera una realidad material, la información sobre este se considera un asunto socio-cultural (van der Ploeg, 2007).

Pero en el caso de los datos biométricos, la información no es más que la representación digital de la realidad física, y esta diferencia es tan tenue como la que existe entre la huella digital en la punta de los dedos de un individuo, y la representación de la misma huella digital en una base de datos. Así, la traducción del cuerpo en información debilita esa división precisa entre el cuerpo en sí mismo, perteneciente a la realidad material, y los datos derivados de ese cuerpo, como "representaciones". La noción de identidad no puede estar restringida a un concepto estático, ni la ontología del cuerpo delimitada a los aspectos anatómicos de lo que se define como visible, en cuanto la identidad es, en sí misma, un constructo compuesto por múltiples capas de significado: nuestra identidad es, en realidad, el resultado de la superposición de una serie de identidades que se solapan, interactúan y se modifican mutuamente (Phillips, 2002).

Si el control sobre nuestros cuerpos es crucial para la autonomía individual, la pérdida del control sobre los datos derivados de los mismos afecta también nuestra autonomía (Herring & Chau, 2007). La característica misma que define al rasgo biométrico -su permanencia- constituye su principal riesgo a la autonomía del individuo. En los términos de Foessel & Garapon (2006), la digitalización del rasgo biométrico "nos condena a vivir en un mundo inmóvil y sin refugio", es decir, resume nuestra identidad a un conjunto de parámetros constantes y objetivos que, una vez fijados y sancionados por la autoridad, nos inmoviliza. Al reducir el cuerpo a su elemento inalterable más mínimo (el rasgo), la identidad se establece a partir del cuerpo codificado, convirtiendo el cuerpo en el indicador de la legalidad o ilegalidad de una persona, y creando una noción estática de la identidad (Ceyhan, 2006).

3.2. RIESGOS DE LAS TECNOLOGÍAS BIOMÉTRICAS

3.2.1. PRIVACIDAD O PROPIEDAD

Como hemos visto, un enfoque de datos personales para la regulación de los datos biométricos resulta insuficiente, pero en el ámbito de la privacidad de la información, carecemos de marcos teóricos y legislativos para abordar comprehensivamente el fenómeno.

Una alternativa es volcarnos hacia la bioética en busca de una respuesta, y analizar los parámetros bajo los cuales se regulan los elementos o partes que son removidos del cuerpo: los órganos extirpados, los fluidos personales o las partes amputadas.

En el ámbito de la medicina, se discute igualmente la idoneidad de un modelo basado en la propiedad (que permitiría a los individuos retener el control sobre las partes de sus cuerpos que han sido removidas) o de un modelo basado en la privacidad y la integridad (que, mientras puede proteger a una persona del acto de remover partes de su cuerpo en contra de sus deseos, no provee protecciones sobre estas una vez que han sido removidas) (Herring & Chau, 2007).

Si bien la propiedad es una herramienta jurídica poderosa para el control de un bien, lleva consigo la carga semántica del comercio y del mercado. Un bien que puede ser poseído es un bien que está dentro del comercio, y esto plantea un conflicto moral (De Witte & Ten Have, 1997): para algunos, es irrespetuoso tratar al cuerpo humano como propiedad que puede ser intercambiada, y equivaldría a asimilar el cuerpo, considerado como "sagrado", a un automóvil o un televisor, una visión degradante y demasiado cercana a la noción de esclavitud (Herring & Chau, 2007). Esto solo revela que la noción de propiedad, una vez más, resulta insuficiente; no tenemos un cuerpo, señala Toombs (1999) sino que somos un cuerpo, existimos en este y desde dentro de este, lo que en sí mismo constituye una diferencia sustancial frente a cualquier otro bien que podamos poseer. El concepto de propiedad requiere una separación entre el que posee y lo poseído; mientras que no existe una distinción clara entre "nosotros" y "nuestros cuerpos" (Herring & Chau, 2007).

Sin embargo, el enfoque legislativo sobre la regulación del cuerpo es mixto, y sería incorrecto decir que todos los elementos del cuerpo están fuera del comercio. Si bien vender un órgano no es legal, vender semen, cabello o sangre está permitido en la gran mayoría de las legislaciones (Rao, 2000). Nos interesa, pues, principalmente la distinción entre el material genético y la información genética, por cuanto podemos trazar un paralelismo que relaciona al material biométrico y los datos biométricos en cuanto respecta a la digitalización, a la creación de una representación digital de la materialidad del cuerpo. Aunque suele considerarse que la concepción de propiedad es aplicable al material genético en la medida que es parte del cuerpo, y si se permite concebir la

propiedad de partes del propio cuerpo mientras la integridad de este último no esté en riesgo, el estatus de la información genética sigue estando menos claro. Muchos países prohíben la propiedad de la información genética por razones de protección del progreso científico, pero desde el punto de vista de la investigación científica hay poca o ninguna distinción entre el material genético y la información genética (De Witte & Ten Have, 1997). La información genética se hace disponible una vez que el material genético ha sido analizado y los resultados han sido almacenados en un archivo o base de datos, del mismo modo que el dato biométrico surge del análisis del rasgo biométrico y su transformación en una plantilla (Mordini & Massari, 2008).

Los enfoques legislativos que buscan proteger los datos personales en general prescinden de la noción de propiedad, al resultar riesgoso para la privacidad admitir que los individuos puedan comerciar con su información personal. Sin embargo, y si bien la alienabilidad parece ser el obstáculo fundamental para permitir un modelo de propiedad aplicable a los datos personales, lo cierto es que el mercado de datos personales existe y alcanza dimensiones multimillonarias. Tal como está definido en la actualidad, el límite a la alienabilidad de los datos personales existe solo para los usuarios de quienes estos datos son extraídos, pero no para las compañías que se dedican a extraerlos (Schwartz, 2003). La noción de los datos personales como moneda de intercambio y como bien que posee un valor económico específico no es nueva: las compañías tienden a ver los datos acumulados como un activo en cuya extracción han invertido, empleando software especializado, y la noción de "pagar" por servicios gratuitos a cambio de la entrega de información sobre nuestras actividades de navegación y uso de las tecnologías tampoco resulta ya extraña (Schwartz, 2003). A pesar de la ya mencionada resistencia histórica, de acuerdo con Douilhet & Karanasiou (2016), el auge del big data está causando un movimiento en la academia, que se traslada del enfoque tradicional de protección de la privacidad hacia un régimen de propiedad, considerado más amplio y, en todo caso, más proteccionista.

3.2.2. RIESGOS DE LA BASE DE DATOS

La función de identificación de las tecnologías biométricas ("uno a muchos", usada para comparar los rasgos de una persona contra los de una población, como por ejemplo las bases de datos de ADN criminal) plantea las principales preocupaciones y riesgos, por cuanto los datos deben salir del control de la persona y almacenarse en una base de datos centralizada (Kindt, 2007).

Los sistemas de identificación biométricos también incrementan los riesgos de falsos positivos y de irrupciones a bases de datos, en relación con los riesgos de seguridad asociados a sistemas de identificación tradicionales, como carnets de identificación. Dado que los datos biométricos son únicos e irremplazables, la posibilidad de pérdida o robo de estos significa que la identidad legal del individuo se ve comprometida sin posibilidad de que se le provea de una nueva

identidad, creando un contexto en el cual, de no existir salvaguardas legales, una persona podría verse privada de su identidad sin recursos para recuperarla ni indemnización a los daños (Privacy International, 2013).

Aunado a esto, existen investigaciones que señalan que casi todos los datos biométricos crudos contienen una cantidad importante de información adicional no requerida, en particular información relativa a la salud del individuo. Si bien en teoría esta información debería ser eliminada al crear la plantilla, la ausencia de marcos regulatorios claros respecto a los estándares de procesamiento de estos datos podría multiplicar por varias veces la cantidad de datos almacenados sobre el cuerpo de una persona (Kindt, 2007).

3.2.3. DESVIACIÓN DE USO

El tema de la desviación de uso, o function creep, es una de las preocupaciones recurrentes en torno a la implementación de tecnologías biométricas. Se denomina desviación de uso a la expansión del uso de una tecnología, un sistema más allá de los propósitos para los cuales fue originalmente creado, en especial cuando esta expansión lleva a una invasión potencial de la privacidad. Según Mordini & Massari (2008), la desviación de uso por lo general involucra al menos tres elementos: 1) un vacío de políticas públicas; 2) una demanda insatisfecha por una función determinada; y 3) un efecto de pendiente resbaladiza. En el ámbito del reconocimiento personal automatizado la desviación de uso puede verse motivada por un rango de intereses que van desde la vigilancia estatal con fines de inteligencia, a propósitos comerciales de intereses privados. La desviación de uso, si bien no siempre es igualmente dañina, erosiona la confianza pública en el uso de un sistema.

El debate en torno al uso potencial de los datos biométricos más allá de sus fines originales suele verse articulado en torno al incremento de las prácticas de vigilancia y a la noción de “interoperabilidad” (Ajana, 2013). Como hemos mencionado, dependiendo de la manera en que se implemente un determinado sistema biométrico, la base de datos puede contener estrictamente la información indispensable para conformar la plantilla (con los cuales es imposible hacer ingeniería inversa de los datos), o una gran cantidad de información de otra índole que, no siendo necesaria para el propósito original, puede potencialmente ser utilizada con otros fines. Un sistema biométrico ideal solamente debería recabar los datos mínimos indispensables para el propósito de identificar a la persona, sin embargo, de acuerdo con Mordini & Massari (2008) esto es una quimera, en razón de la forma en que los sistemas biométricos modernos funcionan. Usualmente, un sistema biométrico moderno consiste de seis factores:

- sensores, dispositivos que capturan propiedades físicas, fisiológicas o de comportamiento del cuerpo humano,
- detectores de vitalidad, que detectan los signos fisiológicos de una persona con la finalidad de evitar ser engañados por signos falsos,

- detectores de calidad, que indican si las características verificadas poseen la calidad suficiente o si deben ser verificadas de nuevo,
- módulo generador de características, que extrae información de las características de la muestra biométrica y genera una representación digital de éstas, que se transforma en una plantilla,
- módulo de emparejamiento, que compara la plantilla obtenida a partir de las características con la plantilla previamente almacenada,
- y por último, el módulo de decisión, que decide si la comparación realizada es suficiente y acepta o rechaza la identificación de la persona.

Varios de estos elementos generan datos redundantes, tanto por su propia naturaleza como por la naturaleza "comunicacional" del cuerpo. Por un lado, el sensor genera toda clase de información respecto a la hora, la fecha, la ubicación en que la muestra fue tomada, pero además genera información respecto al cuerpo, como la edad, el género, la etnicidad o el estado de salud (Mordini, 2008). Por su parte, el detector de vitalidad recaba datos como la presión sanguínea, el reflejo pupilar, el pulso o la respiración, datos que pueden arrojar información adicional como el estado emocional o médico de una persona. Así, al intentar emular de la manera más cercana posible la verdadera interacción y reconocimiento humano, los sistemas de biometría modernos emplean el reconocimiento multimodal, y al hacerlo, recaban y transmiten una enorme cantidad de información sobre cada individuo, del modo que las tecnologías implementadas actualmente van más allá de la mera verificación de identidad y permiten, por ejemplo, estimar el género o la edad de un sujeto determinado (Ricanek Jr & Barbour, 2011).

3.2.4. DISCRIMINACIÓN

Antes de considerar los posibles casos indeseados de exclusión a causa de las tecnologías biométricas, debemos establecer que la exclusión no solo es natural sino que es central, no solo al uso de tecnologías biométricas con fines de identificación, sino a los sistemas de identificación en general. La biometría busca delimitar un espacio de legalidad e ilegalidad, permitir al Estado establecer el límite entre los cuerpos "deseados" e "indeseados", ya sea al momento de vigilar los controles migratorios, proveer un beneficio social o poner en práctica sistemas de seguridad ciudadana (Foessel & Garapon, 2006). La implementación de un sistema de este tipo tiene por finalidad principal la creación de límites de exclusión para conceder o negar un derecho.

Ahora bien, existe además un margen de exclusión indeseada, comprendido por los individuos que se ven discriminados por el uso de tecnologías biométricas a causa de características que no han sido consideradas en el diseño de los sistemas. Las personas con discapacidades de aprendizaje o discapacidades físicas, las personas con enfermedades mentales y las personas en situación de calle son solo algunos de estos grupos. Diversos estudios han comprobado que

los sistemas de identificación biométrica presentan dificultades en el registro de personas de piel oscura, o de quienes por razones religiosas deben cubrirse la cabeza (Wickins, 2007).

Por otra parte, la permanencia del cuerpo como un objeto material estático no es una noción realista, pues aún cuando datos biométricos como el iris o la huella dactilar son únicos e irremplazables, factores ligados a la identidad del cuerpo –como el género, las extremidades, o las características del rostro– pueden variar por acciones del propio individuo o externas a este, como la ocurrencia de accidentes, enfermedades o el simple paso del tiempo. Sin la exigencia legal de que la base de datos permanezca actualizada –y permita a la persona mecanismos para causar su actualización– el individuo estará siempre sujeto a decisiones falsas que pueden afectar sus derechos (Kindt, 2007). Esto afecta especialmente a sistemas de identificación que incluyen a infantes o adolescentes, pero también afecta a cualquier sistema cuyo grupo poblacional comprenda individuos que caigan fuera de los parámetros considerados como "normales": las tecnologías biométricas actuales pueden verse confundidas por variaciones tan pequeñas como el uso de anteojos o asimetrías del rostro (Wickins, 2007).

Del mismo modo, los cuerpos que por circunstancias sociales se encuentran marginados sufren discriminación al ser escudriñados y categorizados por un sistema que no posee categorías para clasificarlos. Así, el identificador de "género", por siglos considerado un factor inmutable en las prácticas de verificación de actores públicos y privados, no es capaz de traducir la realidad a la taxonomía cerrada de un sistema biométrico estatal: una mujer transgénero que se presenta como tal en un aeropuerto puede tener una M (de "hombre") en su pasaporte, y encontrarse con un sistema que al no saber cómo clasificarla, se paraliza (Currah & Mulqueen, 2009). Retomando a Foessel & Garapon, la codificación del cuerpo pretende volverlo estático, congelarlo en el tiempo, y así, cualquier alteración o evolución del cuerpo biológico lo aleja de la representación almacenada en el sistema.

3.2.5. LA TOTALIZACIÓN DE LA VIGILANCIA

La combinación de sistemas de identificación biométrica con otras tecnologías, por ejemplo, en el uso de reconocimiento facial en sistemas de videovigilancia en espacios públicos o semipúblicos, resulta en la pérdida del anonimato público: la posibilidad de moverse libremente en espacios públicos sin que todos nuestros movimientos se vean registrados y vinculados a nuestra identidad jurídica. Un sinnúmero de filósofos y sociólogos han estudiado el efecto inhibitorio de la vigilancia masiva, efecto que se vuelve más grave cuando la vigilancia no es solo observación sino también registro (Slobogin, 2002).

Al implementar sistemas biométricos en fronteras y pasaportes, el Estado establece un monopolio sobre el movimiento de los individuos. La biometrización de los controles de flujo migratorio y de los controles identitarios establece un

mundo de vigilancia al cual el individuo no es libre de escapar (Ceyhan, 2006). Incluso dentro de las fronteras, al inscribir el cuerpo en un sistema biopolítico imbuido de relaciones de poder, la aprehensión del rasgo que "resume" al individuo puede equipararse a la aprehensión del cuerpo físico, lo que nos traslada al equivalente del panóptico benthamiano donde el cuerpo, si bien en movimiento, ha sido aprisionado: aunque fuera de la cárcel, el panóptico es la ciudad y el mundo entero (Torrano & Barrionuevo, 2016).

Por otra parte, la recolección de datos personales, metadatos y datos biométricos en las actividades cotidianas de los ciudadanos –en los sistemas de transporte, bancarios, comerciales, etcétera– crea un entorno general donde la confianza social se ve minada y a su vez, altera la sensación de libertad del individuo en su comportamiento diario. Las personas que ingresan a un espacio vigilado se sienten menos confiadas y más ansiosas, y a su vez confían menos en el espacio y en las personas que le rodean (Slobogin, 2002). Así, la vigilancia no solo afecta a nuestras libertades de expresión y comunicación, sino que también interfiere con el libre desenvolvimiento de nuestra personalidad y con nuestro derecho a la autonomía individual.

3.2.6. TECNOLOGÍAS BIOMÉTRICAS Y ACTORES PRIVADOS

La acumulación de datos biométricos (y de datos personales en general) por parte de actores privados presenta asimismo preocupaciones relativas a la seguridad en el almacenamiento y manejo de estos datos, así como a las políticas de intercambio y eliminación. Retomando a Kindt, la utilización de sistemas biométricos con fines universales –como es el caso de los sistemas de identidad nacional– crea bases de datos centralizadas y masivas cuyo control está fuera del ámbito de acción del individuo, y a esto se suma la tendencia de desviar estos datos de su uso original a través de su intercambio entre diferentes entidades u organismos. La creciente implementación de tecnologías biométricas por parte de actores privados exacerba los riesgos asociados con el manejo de estos datos, al tiempo que mercantiliza características y rasgos del cuerpo humano (Walker, 2015).

Al examinar las prácticas referidas al uso de tecnologías biométricas por parte de privados, nos encontramos con un rango de usos que van desde el desbloqueo de dispositivos móviles a través de la huella dactilar, los lectores de huella, iris y rostro en sistemas bancarios, hasta el empleo de algoritmos de reconocimiento facial en las fotos publicadas en redes sociales. Dada la extrema facilidad para recabar el dato biométrico, debida a la naturaleza comunicacional del cuerpo humano (Mordini y Massari, 2008), las empresas privadas suelen recopilar estos datos sin el conocimiento y consentimiento informado del usuario, o mediante prácticas de intercambio en relaciones desiguales de poder, en las que el usuario entrega sus datos a cambio de un producto o servicio. Así (argumenta Walker), si se deja a un individuo la opción binaria de proveer sus datos biométricos o abstenerse de usar un producto, quien recaba

los datos es quien tiene el poder en la transacción.

Los usos de tecnologías biométricas en el sector privado se expanden aceleradamente, siendo utilizados en la actualidad para un amplísimo rango de fines, desde la publicidad dirigida hasta los servicios de asistentes inteligentes (Siri, Cortana, Google Now y Alexa emplean reconocimiento de patrones de voz para identificar al usuario). Este es un modo más en que los datos personales han sido mercantilizados para convertirse en un bien que puede ser intercambiado por otros bienes y servicios (Walker, 2015).

Los aspectos económicos y de mercado derivados del uso de tecnologías biométricas por parte de actores privados ameritan un análisis separado de mucha mayor profundidad; sin embargo, cabe puntualizar que es imposible efectuar una separación precisa entre los manejos privados y públicos de los datos biométricos, por cuanto la implementación estatal de estas tecnologías, en casi todos los casos, pasa a través de procesos de contratación con actores privados cuyos intereses en la implementación pública de estas tecnologías deriva de motivaciones de índole económica.

4. BIOMETRÍA EN AMÉRICA LATINA

En América Latina, como en la mayor parte del mundo, el uso de características biométricas como mecanismos de identificación y autenticación es de larga data; tradicionalmente los documentos de identidad contienen imágenes fotográficas del rostro e impresiones de las huellas dactilares (y en ocasiones, plantares) como factores mínimos de reconocimiento. De acuerdo con Berry & Stoney (2001) uno de los primeros sistemas de identificación por huella digital data de fines del siglo XVII en Argentina, cuando el doctor Ivan Vucetich fue empleado en La Plata para instalar un sistema de identificación antropométrico de origen europeo que empleaba un conjunto de rasgos físicos como mecanismo de autenticación, y luego de convencer a las autoridades de las ventajas de un sistema basado en huellas digitales, inicia lo que se considera el primer sistema de estas características.

La vertiente de la expansión tecnológica de estos usos, que ha ganado impulso en especial durante la última década, pareciera ser la extensión natural de los usos promovidos por los Estados con la justificación de garantizar la identidad de los ciudadanos por razones de seguridad y para garantizar la entrega de beneficios asistenciales. Sin embargo, de manera general, la puesta en marcha de estos sistemas se ha caracterizado por la carencia de marcos jurídicos suficientes para la fijación de garantías en el tratamiento de los datos, y por la escasa transparencia en los procesos de decisión, adquisición e implementación (Asociación por los Derechos Civiles, 2017a). En este sentido, los siguientes párrafos no pretenden servir de registro exhaustivo de los casos de uso de tecnologías biométricas en América Latina, sino apenas como análisis de algunos ejemplos relevantes en lo que respecta a sus implicancias para la privacidad, la autonomía y la integridad de los individuos.

La implementación de sistemas nacionales de carnet de identidad biométrico en países latinoamericanos se ha visto marcada por el discurso de "eliminar la exclusión". Así, en países como Argentina, el uso de biometría para la identificación ha sido naturalizado a partir de un discurso de modernización del Estado (Asociación por los Derechos Civiles, 2017b). Con una historia convulsa de dictaduras, exclusión social y económica, y de desapariciones forzadas, América Latina resulta especialmente susceptible a favorecer el uso de tecnologías que prometan la seguridad de una identidad inmutable frente al Estado (Ajana, 2013).

En el caso argentino, el Sistema Federal de Identificación Biométrica para la Seguridad (SIBIOS) se introdujo en 2011 a través de un decreto ejecutivo, con la justificación de la seguridad ciudadana y la lucha contra el delito. Así, la identificación biométrica nacional sorteó el proceso legislativo ordinario, saltándose el debate parlamentario y ciudadano que ordinariamente forma parte de la formación de normativas de esta índole.

SIBIOS almacena las huellas dactilares, las huellas palmares y los rasgos faciales de todos los ciudadanos argentinos tanto como de los extranjeros que ingresen o egresen a Argentina. Es un sistema interoperativo desde su

concepción, en el cual participan la Policía Federal, las policías provinciales, el Registro Nacional de las Personas, la Dirección Nacional de Migraciones, así como organismos dependientes de los poderes ejecutivo, legislativo nacional y judicial, ninguno de los cuales requiere de una autorización judicial para acceder a los datos almacenados en el sistema. Según ADC (Asociación por los Derechos Civiles, 2017b), los parámetros de uso, resguardo y almacenamiento de esta información, así como las lógicas y procedimientos para la adquisición y adopción de la tecnología empleada para esto no son transparentes y por ende, impiden el ejercicio del control ciudadano sobre el sistema y sobre los datos albergados en este. Aunado a ello, no existe desarrollo legislativo en Argentina sobre los datos biométricos como datos personales particularmente sensibles, y este vacío hace peligrar la debida protección de los derechos a la privacidad e integridad de los ciudadanos.

La historia de los intentos de Brasil por adoptar un sistema automatizado de identificación ciudadana data de 1997; en 2004, el Ministerio de Justicia lanzó un prototipo de identificación que contiene la huella digital, el patrón de detección facial y el iris de los ciudadanos, cuya potencial implementación ha sido causa de preocupación dado que esta información estaría almacenada en una base de datos centralizada (Da Costa-Abreu & Smith, 2017). Asimismo, Brasil comenzó la implementación de un sistema de voto electrónico en 2008, y existen planes o implementaciones activas de tecnologías biométricas para autenticación y vigilancia en el sistema de transporte, para la identificación en escuelas y para la autenticación en entidades bancarias y cajeros automáticos. Las fuerzas de seguridad, las direcciones de tráfico, la policía y los tribunales de justicia electoral recaban huellas dactilares que son almacenadas en bases de datos cuya protección legal es débil (Asociación por los Derechos Civiles, 2017a).

La implementación de tecnologías biométricas en Brasil presenta una serie de retos particulares a su historia, su geografía y su composición socioeconómica. El costo de la adquisición de datos, de por sí elevado en la implementación de cualquier sistema biométrico universal, se eleva dada la amplitud territorial del país y su elevada población. En este sentido, Da Costa-Abreu & Smith señalan que, si bien los precios están bajando, el precio por unidad para los esquemas de identificación nacional aún exceden los niveles asequibles por países en desarrollo, y que cuando la tecnología es costosa, estos costos suelen ser trasladados al ciudadano, planteando así barreras al acceso. En el caso de Brasil en particular, y de América Latina en general, donde los sistemas biométricos han sido presentados como una solución a las barreras al acceso a bienes, servicios y derechos por parte de una población tradicionalmente discriminada, resulta un sinsentido buscar resolver esta brecha con soluciones tecnológicas costosas.

En Chile, el uso de sistemas biométricos está ampliamente extendido, y el uso de la huella digital como mecanismo de identificación se encuentra desde los procesos migratorios hasta el sistema de salud y los sistemas bancarios. Aunado a esto, existe un uso creciente de sistemas de reconocimiento facial, mecanismo que se utiliza en cámaras de vigilancia y sistemas de transporte público (Viollier, 2017). El caso de estos sistemas reviste particular interés, por cuanto

constituyen iniciativas de municipalidades, ministerios e instituciones que actúan independientemente y sin un marco regulatorio preexistente. La sociedad civil chilena ha señalado que no existe evidencia sobre la eficacia de estos mecanismos para los fines que buscan –particularmente, en lo que respecta al incremento de la seguridad ciudadana– y que estos han sido implementados sin estudios previos de finalidad, alcance, legalidad y proporcionalidad, por no mencionar sin transparencia en el proceso de licitación para la adquisición de las tecnologías.

Por su parte, Venezuela implementó mecanismos de reconocimiento biométrico por primera vez en su sistema electoral a través del SAI (Sistema de Autenticación Integral), que exigía la autenticación por huella digital del elector para la activación de las máquinas de votación (Consejo Nacional Electoral, s. f.) y que fue utilizado por primera vez en las elecciones del año 2012. Posteriormente se implementa el denominado Sistema Biométrico para la Seguridad Alimentaria, a través del cual se exige a los ciudadanos la verificación de su identidad a través de la huella digital al momento de adquirir productos categorizados como de "primera necesidad" (productos alimentarios, de higiene, y medicinas). En el caso venezolano, si bien el carnet de identidad nacional no incorpora tecnologías biométricas, los datos son incorporados al sistema nacional de identidad, dado que el registro civil y el electoral fueron unificados bajo la potestad del Consejo Nacional Electoral. Estos datos pasan así a formar parte de un sistema multimodal, al verse combinados con otras piezas de información como la dirección de la persona, su fecha de nacimiento y su número de identidad nacional (Díaz, 2015), sistema que a su vez es utilizado por operadores estatales tanto como por cajeros de supermercados y farmacias, funcionarios de migración y policías sin ningún tipo de requisito legal previo.

En ausencia de una ley nacional de protección de datos personales, y bajo un sistema que utiliza la información de sus ciudadanos como mecanismo de control político, el uso de tecnologías biométricas para el acceso a bienes y servicios básicos es un ejemplo claro de la creación de espacios sociopolíticos de "legalidad" e "ilegalidad". Desde el momento mismo de su implementación, comenzaron a presentarse infinidad de inconvenientes al verse negada la posibilidad de adquirir bienes básicos a adolescentes, a extranjeros –tanto legales como indocumentados– que por razones obvias no aparecían en la base de datos electoral (Miselem, 2014) o a personas transgénero cuya apariencia física no coincidía con la reflejada en la base de datos (Fundación Reflejos de Venezuela, 2016).

Al igual que Venezuela, Paraguay tampoco cuenta con una ley de datos personales, sin embargo se encuentra implementando progresivamente sistemas de reconocimiento biométrico. En este caso, al no existir una política pública definida, no hay claridad con respecto al manejo de la información recabada, sino que distintos organismos exigen la entrega de ciertos datos para llevar a cabo un determinado trámite (Asociación por los Derechos Civiles, 2017a). Ambos casos retratan la vulnerabilidad del individuo frente al Estado en la situación en la que sus datos son exigidos como requisito o contraprestación por un bien o

servicio; en Paraguay, se dieron casos en los que el Instituto de Previsión Social requería las huellas dactilares de los pacientes para permitirles retirar medicamentos (ABC Color, 2016), y en Venezuela, frente a la escasez de alimentos y al alto índice de inflación, los ciudadanos se ven forzados a pasar por el trámite de entregar sus datos a cambio de poder adquirir alimentos (Meza, 2014).

CONCLUSIONES

En la mayoría de los casos, la implementación de sistemas biométricos en América Latina es presentada como la solución, total o parcial, a una serie de problemáticas históricas de la región: la seguridad ciudadana, la distribución adecuada de beneficios asistenciales, la existencia jurídica del ciudadano frente al Estado en países con largos historiales de problemas en sus sistemas nacionales de identificación. Si bien suele ser cierta la existencia de estos problemas y la necesidad de afrontarlos mediante políticas públicas, con demasiada frecuencia son priorizados frente a los derechos a la privacidad, la integridad y la autonomía de los individuos. La seguridad, tanto online como offline, es usada como excusa y justificación para difuminar los límites que deben controlar y balancear las acciones de los Estados.

Las tecnologías biométricas, usadas en ciertas situaciones y bajo parámetros de seguridad, transparencia y control ciudadano, pueden ser de suma utilidad para facilitar procesos, aumentar la seguridad en protocolos y garantizar la identidad de los individuos involucrados. Sin embargo, al nivel actual de desarrollo tecnológico, su uso de manera universal (es decir, en poblaciones grandes, como toda una ciudad o todo un país) presenta consecuencias negativas importantes que pueden llevar a la exclusión social de ciertos sectores, a la acumulación de falsos negativos o falsos positivos, o simplemente a la erosión de la confianza social que a su vez repercute en la libertad del individuo para desenvolverse en el contexto de una sociedad democrática.

Para agravar aún más la situación, en una parte importante de América Latina, el acceso inconsistente y poco confiable al suministro eléctrico, al acceso a internet y en general a la utilización informada y segura de sistemas tecnológicos presenta una barrera imposible de obviar en lo que respecta a la posibilidad de las tecnologías biométricas para sostener el peso de funciones cruciales de servicio público. Esto se deriva en que, al nivel actual de desarrollo tanto tecnológico como legislativo, los riesgos y problemas que se derivan de la implementación de tecnologías biométricas sobrepasan por mucho sus posibles beneficios.

Por otra parte, la relación entre el cuerpo físico y su data doppelgänger nos invita a revisitar la relación jurídica entre la persona y los datos que su actividad genera. Es un despropósito que la misma regulación pretenda abarcar el manejo de una contraseña de acceso o de un número telefónico, y la digitalización del rostro de una persona o su huella dactilar. Al mismo tiempo, es indispensable reevaluar la interacción entre las distintas piezas de información que existen sobre nosotros en el ámbito digital, la manera en que interactúan con el individuo y conforman una o múltiples identidades acumuladas, piezas de muy diverso valor en cuanto a su relevancia para la autonomía del individuo, pero también de muy diverso valor en el mercado de los datos.

Así, parece que los enfoques que plantean que la biometría es un problema de privacidad resultan tan insuficientes como los que pretenden regular esta relación únicamente bajo el derecho a la propiedad. Si pensamos la digitalización

de los distintos rasgos biométricos como un mapa del cuerpo, quizás los parámetros para regular el análisis y uso de los datos biométricos deberían equipararse, no a la protección de las comunicaciones o de los datos personales, sino a los estándares para la regulación del cacheo, puesto que el nivel de intimidad implicado al navegar una representación digital del cuerpo físico de una persona muy probablemente se asemeja más a una radiografía o a un proceso de registro corporal migratorio. Esto exigiría un sistema de regulaciones mixto que entienda la naturaleza particular del dato biométrico en su relación intrínseca e inmutable con el cuerpo en tanto elemento del yo, del cuerpo como vehículo de la vida humana.

En cualquier caso, la puesta en marcha de sistemas de identificación biométrica exige salvaguardas de índole legal que permitan proteger los derechos fundamentales del individuo: este debe ser informado sobre el procedimiento de recolección de datos, el propósito para el cual serán usados debe estar definido con anterioridad y ser claro y específico, y debe indicarse previamente quién tendrá acceso a tales datos, bajo qué protocolos, y qué medidas de seguridad se emplearán para su protección y eliminación. Esto implica asegurar que los datos recabados no puedan ser utilizados para otros fines ni sometidos a registros o pruebas adicionales sin la autorización específica de un órgano judicial, así como que los datos adicionales sean destruidos luego de la creación de la plantilla.

En nuestra opinión, el uso de tecnologías biométricas tal como es llevado a cabo actualmente en América Latina pareciera remitir a un concepto de "identidad" que, más que ser un derecho del individuo frente al Estado (el derecho a ser reconocido como un sujeto pleno de derechos en un sistema social), parece ser un derecho del Estado frente al individuo (la potestad de poseer y manipular las piezas que conforman la identidad de un individuo, de almacenarlas, procesarlas y utilizarlas para diversos fines políticos), lo que remite a una relación de poder que desnaturaliza los derechos humanos que subyacen en esta discusión.

El actual estado de las cosas es la consecuencia natural de la tendencia de la región hacia una retórica de la "securitización" que pretende justificar una invasión cada vez mayor del ámbito de la vida privada de los individuos en razón de la obtención de mayores estándares de seguridad. No obstante, y como es bien sabido, los derechos humanos son por definición integrales, y cualquier pretendida negociación que se haga a costa de alguno de ellos en beneficio de otros irá en detrimento de las posibilidades del ciudadano para alcanzar una vida digna.

Ineludiblemente, la implementación de estas tecnologías de acuerdo con los estándares mínimos de protección de los derechos humanos requiere, primero que nada, un nivel básico de transparencia que representa un problema para la mayor parte de los países latinoamericanos. No obstante, la creación de estándares mínimos es indispensable y urgente, puesto que el carácter único y permanente de los datos biométricos significa a la vez que su uso indebido presenta riesgos irreversibles para los derechos básicos de los individuos afectados.

BIBLIOGRAFÍA

ABC Color. (2016, septiembre 3). Toman huellas dactilares para retirar medicamentos. ABC Color.

Ajana, B. (2013). Governing through biometrics: The biopolitics of identity. Palgrave MacMillan. https://doi.org/10.1080/1369118X.2014.900103

Alterman, A. (2003). "A piece of yourself": Ethical issues in biometric identification. Ethics and information technology, 5(3), 139-150. https://doi.org/10.1023/B:ETIN.0000006918.22060.1f

Asociación por los Derechos Civiles. (2017a). Cuantificando identidades en América Latina.

Asociación por los Derechos Civiles. (2017b). La identidad que no podemos cambiar: cómo la biometría afecta nuestros derechos humanos.

Berry, J., & Stoney, D. A. (2001). The history and development of fingerprinting. Advances in fingerprint Technology, 2, 13-52.

Bourcha, C., Deftou, M.-L., & Koskina, A. (2017). Data mining of biometric data: revisiting the concept of private life? Ius et scientia, 3(2), 37-62.

Ceyhan, A. (2006). Enjeux d'identification et de surveillance à l'heure de la biométrie. Cultures & Conflits, 4, 33-47. https://doi.org/10.4000/conflits.2176

Consejo Nacional Electoral. (s. f.). Tecnología electoral en Venezuela. Recuperado a partir de http://www.cne.gob.ve/web/sistema_electoral/tecnologia_electoral_descripcion.php

Currah, P., & Mulqueen, T. (2009). Securitizing Gender: Identity, Biometrics, and Transgender Bodies at the Airport. Social Research, 78(2), 557-583. https://doi.org/10.1353/sor.2011.0030

Da Costa-Abreu, M., & Smith, S. (2017). Using biometric-based identification systems in Brazil: A review on low cost fingerprint techniques on-the-go. Computer Law & Security Review.

De Witte, J. I., & Ten Have, H. (1997). Ownership of genetic material and information. Social Science and Medicine, 45(1), 51-60. https://doi.org/10.1016/S0277-9536(96)00309-7

Díaz, M. (2015). Tu huella digital por un kilo de harina: biométrica y privacidad en Venezuela. Recuperado 22 de noviembre de 2017, a partir de https://www.digitalrightslac.net/es/tu-huella-digital-por-un-kilo-de-harina-biometrica-y-privacidad-en-venezuela/

Douilhet, E., & Karanasiou, A. (2016, noviembre). Legal responses to the commodification of personal data in the era of big data: The paradigm shift from

data protection towards data ownership. Effective Big Data Management and Opportunities for Implementation.

Foessel, M., & Garapon, A. (2006). Biométrie: les nouvelles formes de l'identité. Esprit, 8, 165–172.

Fundación Reflejos de Venezuela. (2016). El drama de ser transgénero e intentar comprar en un supermercado. Recuperado a partir de https://www.fundacionreflejosdevenezuela.com/discriminados-drama-transgenero-e-intentar-comprar-supermercado/

Gemalto. (2018). Biometric data and the General Data Protection Regulation. Recuperado 23 de marzo de 2018, a partir de https://www.gemalto.com/govt/biometrics/biometric-data

Herring, J., & Chau, P. L. (2007). My body, your body, our bodies. Medical Law Review, 15(1), 34–61. https://doi.org/10.1093/medlaw/fwl016

Higgs, E., & Caplan, J. (2013). Identification and Registration Practices in Transnational Perspective: People, Papers and Practices. Springer.

Kindt, E. (2007). Biometric applications and the data protection legislation: the legal review and the proportionality test. Datenschutz und Datensicherheit, 31(August 2003), 166–170. https://doi.org/10.1007/s11623-007-0064-6

Meza, A. (2014, agosto 22). Una huella dactilar a cambio de comida. El País.

Miselem, S. (2014). Crecen interrogantes en torno a supervisión de compras en Venezuela. El Nacional.

Mordini, E. (2008). Biometrics, human body, and medicine: A controversial history. En Ethical, Legal and Social Issues in Medical Informatics (pp. 249–272). IGI Global.

Mordini, E., & Massari, S. (2008). Body, biometrics and identity. Bioethics, 22(9), 488–498. https://doi.org/10.1111/j.1467-8519.2008.00700.x

Phillips, T. (2002). Imagined Communities and Self-identity: An Exploratory Quantitative Analysis. Sociology, 36(3), 597–617. https://doi.org/10.1177/0038038502036003006

Privacy International. (2013). Biometrics: friend or foe of privacy (Vol. 35).

Rao, R. (2000). Property , Privacy , and the Human Body. Boston University Law Review, 359.

Ricanek Jr, K., & Barbour, B. (2011). What are soft biometrics and how can they be used? Computer, 44(9), 106–108.

Ruyg, M. (2016). Does the Data Doppelgänger Reside in The Uncanny Valley? Master's Thesis for the Media Technology programme, Leiden University (The Netherlands).

Sanz Salguero, F. J. (2016). Relación entre la protección de los datos personales y el derecho de acceso a la información pública dentro del marco del derecho comparado. Ius et Praxis, 22(1), 323–376. https://doi.org/10.4067/S0718-00122016000100010

Schwartz, P. M. (2003). Property, Privacy, and Personal Data. Harv. L. Rev., 117, 2056.

Slobogin, C. (2002). Public privacy: camera surveillance of public places and the right to anonymity. Miss. LJ, 72, 213. https://doi.org/10.3868/s050-004-015-0003-8

Sutrop, M. (2010). Ethical issues in governing biometric technologies. Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 6005 LNCS, 102–114. https://doi.org/10.1007/978-3-642-12595-9_14

Toombs, S. K. (1999). What Does It Mean To Be Somebody? Phenomenological Reflections and Ethical Quandaries. En Persons and Their Bodies: Rights, Responsibilities, Relationships (pp. 73–94). Dordrecht: Kluwer Academic Publishers. https://doi.org/10.1007/0-306-46866-2_4

Torrano, A., & Barrionuevo, L. (2016). Políticas extractivistas sobre el cuerpo : SIBIOS y el Derecho a la identificación y la privacidad 1 , 2. Año Págs, 127–149.

Vagle, J. L. (2016). The History, Means, and Effects of Structural Surveillance. Faculty Scholarship, (Paper 1625).

van der Ploeg, I. (2002). Biometrics, and the body as information: normative issues of the socio-technical coding of the body. En D. Lyon (Ed.), Surveillance as Social Sorting: Privacy, Risk, and Automated Discrimination (pp. 57–73). New York: Routledge.

van der Ploeg, I. (2007). Genetics, biometrics and the informatization of the body. Annali dell'Istituto Superiore di Sanita, 43(1), 44–50.

Viollier, P. (2017). Biometría: tecnosolucionismo a costa de nuestros derechos. Recuperado 22 de noviembre de 2017, a partir de https://www.derechosdigitales.org/11333/biometria-tecnosolucionismo-a-costa-de-nuestros-derechos/

Walker, E. M. (2015). Biometric Boom: How the Private Sector Commodifies Human Characteristics. Fordham Intellectual Property, Media and Entertainment Law Journal, XXV(3).

Wickins, J. (2007). The ethics of biometrics: The risk of social exclusion from the widespread use of electronic identification. Science and Engineering Ethics, 13(1), 45–54. https://doi.org/10.1007/s11948-007-9003-z

Zureik, E., & Hindle, K. (2004). Governance, security and technology: The case of biometrics. Studies in Political Economy, 113–137.


DERECHOSDIGITALES
Derechos Humanos y Tecnología en América Latina