Revista Ius et Praxis
Talca, Chile, 2023
Artículo
Fecha de recepción: 2022-05-31; fecha de aceptación: 2022-09-28

TECNOLOGÍAS DE RECONOCIMIENTO FACIAL EN COLOMBIA: ANÁLISIS COMPARATIVO EN RELACIÓN CON LA PROTECCIÓN DE DATOS

Facial recognition technologies in Colombia:
Comparative analysis in relation to data protection

MARÍA LORENA FLÓREZ ROJAS[*]
ANGÉLICA MARÍA CAMELO PIMIENTA[**]
Universidad de Los Andes

Resumen

La tecnología de reconocimiento facial es un ejemplo de tecnología blanda y flexible, cuyo funcionamiento se basa en datos biométricos, los cuales son procesados por sistemas algorítmicos que permiten la identificación o verificación de individuos. Puede ser aplicada a una diversidad de situaciones, tales como verificación de identidad en transacciones bancarias, o asistencia a personas en condición de discapacidad, entre otras. El presente artículo realiza un análisis de la regulación colombiana sobre protección de datos en relación con las tecnologías de reconocimiento facial en contraste con la regulación de la Unión Europea y de los Estados de California e Illinois en los Estados Unidos. El objetivo Fecha de recepción: 2021-03-01; fecha de aceptación: 2021-11-03nacional para enfrentar los riesgos y desafíos planteados por este tipo de tecnología y en esa medida plantear una propuesta en caso de que la norma resulte no serlo.

Palabras clave

Reconocimiento facial, biometría, protección de datos.

Abstract

Facial recognition technology is an example of soft and flexible technology, whose operation is based on biometric data, which are processed by algorithmic systems that allow the identification or verification of individuals. It can be applied to a variety of situations, such as identity verification in banking transactions, or assistance to people with disabilities, among others. This article makes an analysis of the Colombian regulation on data protection in relation to facial recognition technologies in contrast with the regulation of the European Union and the States of California and Illinois in the United States. The objective of this article is to make a comparative analysis as to the relevance of the national regulation to face the risks and challenges posed by this type of technology and, to that extent, to make a proposal in case the regulation turns out not to be adequate.

Key words

Facial recognition, biometrics, data protection.

Introducción

La tecnología de reconocimiento facial (TRF) es una herramienta adoptada tanto por el sector privado como en el público para brindar diversidad de bienes y servicios. Por ejemplo, el Mastercard FaceID de la compañía Mastercard International Inc para facilitar pagos[1]; los iPhone

[*] PhD cum laude Scuola Superiore Sant'Anna en Italia, con Máster en Derecho y Tecnología de la Universidad de Tilburgo en Holanda y Abogada de la Universidad de Los Andes. Actualmente es profesora de la Universidad de Groningen en Países Bajos e Investigadora del Centro CINFONIA de Inteligencia Artificial de la Universidad de los Andes, Bogotá. Correo: m.l.florez.rojas@rug.nl.
[**] Estudiante LLM Berkeley Program. Abogada de la Universidad de Los Andes con especialización en Derecho Comercial universidad y Mágister en Derecho Privado de la misma universidad. Bogotá, Colombia. Correo: am.camelo10@uniandes.edu.co.
[1] WONG (2020), pp. 189-229.

modelo X, el iPad Pro y Air 2020 de Apple, Inc. que incluyen dicha herramienta como mecanismo de seguridad para acceder al contenido de los celulares y tabletas; Google Photos y Facebook con su etiquetado automático de fotos; Walmart para mejorar la experiencia de compra de sus clientes[2]; entre otros.

Esta implementación de la TRF por el sector privado ha causado un uso y circulación masiva de datos personales, ocasionado conflictos entre los titulares de la información y las empresas que recolectan y usan estos datos. Sobre el particular, en *Patel v. Facebook*, 2015, los demandantes alegaban que Facebook había infringido la ley de datos biométricos del Estado de Illinois al utilizar datos biométricos faciales de los usuarios obtenidos a partir de las fotos subidas a la plataforma para perfilarlos, crear plantillas faciales y sugerir de manera automática etiquetados en dichas fotos, lo que permitía no solo identificar personas particulares dentro de las millones de fotos subidas a Facebook, sino también su localización[3].

En esta línea, el estudio *"Global biometric technologies market revenue from 2018 to 2027"*, publicado por Statista en 2019[4], indicó que según las cifras de crecimiento de tecnologías biométricas obtenidas durante 2018 y 2019, se podía proyectar un crecimiento de aproximadamente 38.8 billones de dólares en los próximos siete años, llegando a tener ganancias cercanas a los 56 billones de dólares en el 2027. Si bien, con los datos obtenidos por medio de este estudio no es posible afirmar que el uso de la tecnología aumenta entre los consumidores, el hecho de que las ganancias lo hagan, indica una tendencia de crecimiento del mercado de este tipo de tecnologías.

Colombia no es ajena a la innovación e implementación de todo tipo de tecnologías, incluyendo la TRF. Actualmente se encuentran en el mercado nacional productos y servicios con este tipo de tecnología, algunos de ellos permiten realizar transacciones bancarias desde el celular, solicitando cada cierto tiempo el escaneo del rostro para verificar la identidad; otros han incursionado en el reemplazo de las contraseñas por el escaneo facial en aplicaciones bancarias; o incluso la comercialización de equipos móviles que utilizan el reconocimiento facial como mecanismo de seguridad. Con todo lo anterior, es relevante preguntarse si ¿Es el marco regulatorio colombiano relativo a la protección de datos suficiente o es necesario adoptar algún cambio normativo o pragmático para enfrentar los desafíos planteados por la adopción de las tecnologías de TRF por parte del sector privado, teniendo en cuenta la experiencia de los estados de California e Illinois en los Estados Unidos y la Unión Europea?

1. Tecnología de reconocimiento facial (TRF)

La palabra 'tecnología' no tiene una única definición y no existe consenso ni científico ni académico sobre ello. Según la Real Academia se entiende por tecnología un *"[c]onjunto de teorías y de técnicas que permiten el aprovechamiento práctico del conocimiento científico"*, cuyo origen proviene de las expresiones griegas '*techne*' y '*logos*' que significan arte y razón respectivamente[5]. De igual forma, la Agencia Espacial Europea, establece que tecnología es *"(…) la aplicación práctica del conocimiento para que algo absolutamente nuevo pueda ser realizado, o que algo se pueda hacer de una forma completamente novedosa"*[6]. No obstante, para Aunger, establece que la tecnología es más*"(…)acerca de la interacción con artefactos en contextos particulares de participación"*[7] lo que evidencia una concepción de tecnología ligada al concepto evolucionista y filosófico. Así, para el propósito de la presente investigación, es posible afirmar que la tecnología implica dos elementos. De un lado, un factor transformador del conocimiento científico para crear productos nuevos o cambiar la forma en que se realizan las cosas; de otro,

[2] CRAWFORD (2019), p. 565; MANN et al. (2017) pp. 121-145.
[3] United States Court of Appeals for the ninth circuit, N. 18-15982, 8 de agosto de 2019.
[4] STATISTA (2022).
[5] RAE (2021).
[6] ESA (2021).
[7] AUNGER (2010), p. 764.

un factor relacionado con el propósito de suplir necesidades humanas y mejorar su calidad de vida.

Con el fin de discutir la tecnología de TRF en detalle, es importante describir los diferentes tipos de tecnología que existen. Según Economipedia, es importante especificar los tipos de tecnologías para así poder estudiar la utilidad y características que posee una tecnología cualquiera[8], así, se reseña una breve explicación de los tipos de tecnologías que existen[9]:

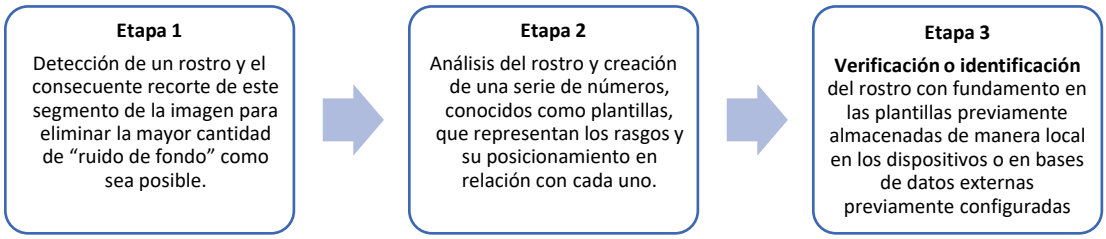
Tipo de Tecnología	Descripción
Fija	No sufre cambios constantes a excepción de aquellos para aumentar su rendimiento.
Flexible	Incluye una variedad en cuanto a los procesos en los cuales se pueden usar, con múltiples funciones y utilidades.
Blanda	Relacionada con procesos y métodos que conforman un activo intangible.
Dura	Consiste en el desarrollo, producción y fabricación de productos tangibles.
Limpia	No impacta o aminora el impacto negativo sobre el medio ambiente. Esta no utiliza factores que puedan contaminar, administra correctamente los recursos y se utilizan fuentes de energía alternativa.
De materiales	Transforma una serie de materias en producto final, indistintamente del impacto ambiental.
De operación	Se basa en el perfeccionamiento de procesos para la obtención de un mismo resultado de manera más eficiente o eficaz.
De producto	Se centra en la creación o desarrollo de un producto o servicio en base a un añadido innovador, ya sea de forma tangible o intangible.

Cuadro 1. Tipos de tecnología. Elaboración propia.

Asimismo, según la Fundación Frontera Electrónica (EFF), la tecnología de TRF es un mecanismo de identificación o verificación de identidad de un individuo que utiliza su rostro o rasgos faciales[10]. De igual manera, la empresa desarrolladora de software Electronic IDentification, define la TRF como aquella capaz de verificar o identificar a un individuo a través de una imagen, video o cualquier elemento audiovisual de su rostro[11]. Siguiendo esta línea, el Centro de Ética e Innovación de Datos del Reino Unido, explica que la TRF es un sistema algorítmico capaz de analizar el rostro de una persona y asociarlo a una identidad[12].

Así, la TRF encuentra patrones en las medidas de la cara de cada usuario, para crear plantillas del rostro, y posteriormente buscar similitudes entre dos plantillas. Esta tecnología usa algoritmos para detectar detalles del rostro y así convertir estos en una representación matemática o plantilla capaz de ser comparada con datos previamente recolectados y almacenados en una base de datos de reconocimiento facial. Algunos de los detalles utilizados para crear estas plantillas son la distancia entre los ojos o la forma de la barbilla, entre otros. Con todo lo anterior, el Centro de Ética e Innovación de Datos, establece que el despliegue de la TRF tiene las siguientes tres etapas o pasos[13]:

[8] LLAMAS (2020).
[9] VIU (2017); LLAMAS (2020).
[10] EFF (2017).
[11] EID (2021).
[12] CDEI (2020).
[13] VIU (2017).



Cuadro 2. Etapas de la TRF. Elaboración propia.

Sin embargo, no existe un solo mecanismo de reconocimiento facial. Con base en las explicaciones abordadas, se puede afirmar que el objetivo de la TRF es la identificación **o** verificación de un individuo. Verbos que no se usan de manera indistinta pues los mismos se refieren a mecanismos diferentes de reconocimiento facial, pese a que ambos sigan la misma ruta de operación.

Existen dos mecanismos de reconocimiento facial: El de verificación y el de identificación. Según el Centro de Ética e Innovación de Datos, la TRF de verificación es aquella que *"trata de determinar si un rostro concuerda con una única plantilla, la cual usualmente esta guardada en un dispositivo"*[14] de manera local. Algunos ejemplos de esta modalidad son los mecanismos que incorporan los dispositivos móviles tales como los iPhone de nueva generación.

Por el contrario, la TRF de identificación es aquella que trata de determinar si un rostro concuerda con alguna de las plantillas faciales que han sido guardadas de manera previa en una base de datos, las cuales pueden ser de cualquier tamaño, pudiendo incluso llegar a almacenar millones de plantillas de diferentes rostros[15]. Algunos ejemplos del uso son aquellos utilizados por Facebook para sugerir etiquetas en las fotografías o las cámaras utilizadas en el concierto de Taylor Swift en el 2019 para identificar depredadores sexuales entre los asistentes[16]. Así, la TRF es un mecanismo de identificación o verificación de individuos, que utiliza rasgos faciales para contrastarlos con plantillas previamente almacenadas en bases de datos (locales o remotas) que tiene múltiples aplicaciones, desde el uso en dispositivos móviles hasta cámaras de seguridad.

Se puede concluir que la TRF es una tecnología blanda, flexible que tiene una multiplicidad de aplicaciones y representa un activo intangible para aquellos que hacen uso de ella. Asimismo, usa modelos algorítmicos matemáticos fundamentados en bases de datos previamente configuradas de manera externa o local para identificar o verificar individuos según el caso.

1.1. Usos de la tecnología de reconocimiento facial

El creciente uso en torno a las 'soluciones' biométricas es un ejemplo de ello. La biometría se refiere a los datos sobre nuestros rostros, cuerpos o comportamientos, que han sido sometidos a un tratamiento técnico específico para que puedan ser leídos por una máquina. Puede ser, que nuestro rostro en una foto se convierta en una plantilla facial dentro de una base de datos. Así, los sistemas biométricos utilizan el reconocimiento facial, las huellas dactilares y otros análisis de datos biométricos para identificar a las personas, clasificarlas o incluso juzgarlas. Algunas de las situaciones en las que se puede emplear esta tecnología son:

[14] CDEI (2020).
[15] CRAWFORD (2019), p. 565.
[16] BÉNICHOU (2019), p. 565.

Usos	Descripción
Prevención crimen	Prevenir y reducir robo de mercancía en centros comerciales, comparando el rostro los individuos que ingresan con bases de datos privadas que contienen las plantillas previamente almacenadas de individuos que han sido acusados de hurto con anterioridad.
Desbloqueo dispositivos	Celulares o tabletas hacen uso de esta tecnología para verificar la identidad de quien intenta acceder a ellos.
Mercadeo y publicidad	Estrategias de mercadeo de acuerdo con su audiencia objetivo, haciendo uso de esta tecnología para identificar factores decisivos tales como género y edad.
Asistencia a personas en condición de discapacidad	Aplicaciones que alertan a las personas con discapacidad visual cuando alguien está sonriendo a través de una vibración para ayudarles a comprender mejor las situaciones sociales.
Redes sociales	Identificar personas en las fotos que se suben a las plataforma.
Diagnosticar enfermedades	Detección de enfermedades que ocasionan cambios en la apariencia de las personas.
Transacciones seguras	Opción de realizar transacciones únicamente con el escaneo del rostro.

Cuadro 3. Usos de la TRF. Elaboración propia.

Existen otros usos de esta tecnología y algunos que son empleados de manera específica por el sector público, como por ejemplo para vigilancia masiva. Con frecuencia, hay una grave falta de cuidado y atención al hecho de que el uso de sistemas biométricos y otros sistemas digitales para rastrear, registrar o identificar a personas en situaciones de riesgo o vulnerables conlleva grandes riesgos para su privacidad y seguridad. Por ejemplo, el programa de la ONU para los refugiados fue criticado por E. Tendayi Achiume, por proyectos que condicionaban de forma coercitiva el acceso a los alimentos a la identificación biométrica, basándose en la débil justificación de evitar el fraude[17]. Este informe describe cómo un sistema biométrico defectuoso condujo a la denegación de alimentos a los refugiados que habían huido de las masacres.

Otro ejemplo, es Clearview AI como un servicio de reconocimiento facial que afirma haber creado enormes bases de datos, con más de 3.000 millones de rostros etiquetados, mediante la controvertida práctica de extraer fotos de redes sociales[18]. Los informes sugieren que más de 2.000 organismos policiales de todo el mundo habían utilizado los servicios de Clearview a principios de 2020. Varios países iniciaron investigaciones en contra de la compañía afirmando que esta eludía los procedimientos de contratación pública y podría usar herramientas como *web scrapping* para recolectar datos de forma inadecuada y sin la debida autorización[19].

Es importante resaltar, que en ninguna de sus aplicaciones esta tecnología resulta infalible, toda vez que los resultados obtenidos por los sistemas que emplean TRF están enmarcados en términos de 'puntaje de similitud' entre las dos plantillas de rostro a comparar y el análisis de los resultados puede ser complicado considerando que estos son resultados de procesos de cálculo propios de cada sistema y algoritmo[20]. Así, factores externos influyen en la eficacia de este tipo de sistemas como, la luz, la pose del sujeto o la edad. Estas circunstancias,

[17] ONU (2018).
[18] REZENDE (2020), pp. 375-389.
[19] SOBEL (2020), p. 75.
[20] LIAW et al. (2014), pp. 824-834.

hacen que los sistemas que incorporan la TRF arrojen lo que se conoce como 'falsos negativos' y 'falsos positivos'. Los falsos negativos son cuando el sistema debió haber arrojado coincidencia, pero no lo hizo; y los falsos positivos, en contraposición, son cuando el sistema debió haber establecido que no existía coincidencia, pero erróneamente encuentra una coincidencia[21].

1.2. Datos biométricos

Existen diferentes tipos de datos, sin embargo, teniendo en cuenta el objetivo del presente artículo, se hace referencia únicamente a datos biométricos. Según Catherine Jasserand el concepto de datos biométricos tiene principalmente dos significados[22]. Por un lado, la concepción científica de datos biométricos que cubre el proceso técnico a través del cual se captura la información biométrica y se transforma a formato digital; y por otro, la concepción legal la cual establece que los datos biométricos son un tipo de datos personales relacionados con características biométricas y vinculadas a la identificación de un individuo. Asimismo, según el Concepto No.18-171259 de la Superintendencia de Industria y Comercio de Colombia (SIC), los datos biométricos son aquellos relacionados con la biometría, la cual según esta entidad es el estudio de métodos automáticos o tecnología de seguridad basada en el reconocimiento de características físicas e intransferibles de las personas[23]. Entre ellos, se pueden encontrar las huellas dactilares, el iris, la voz, entre otros.

De esta forma, la definición de '*datos biométricos*' no es pacífica, pero para efectos del presente artículo se tomará la definición planteada por la autora Jasserand, ya que como se verá, la norma colombiana considera los datos biométricos como datos personales. Así, se puede concluir de manera preliminar, que la TRF es considerada como tecnología blanda y flexible, también, involucra datos biométricos que son procesados por sistemas algorítmicos que cumplen el objetivo de identificación o verificación. En ese sentido, el marco regulatorio de este tipo de tecnología resulta relevante, toda vez que las diversas técnicas de biometría se involucran directamente con el tratamiento de datos personales que puede representar un riesgo para los usuarios cuando ocurra un indebido tratamiento, pues no son sistemas infalibles y poseen altos márgenes de error.

2. Marcos regulatorios

2.1. Colombia

El derecho de habeas data fue introducido formalmente en el ordenamiento nacional a través del artículo 15 de la Constitución Política de 1991, tal y como lo afirma Remolina en su texto *"Tratamiento de datos personales, Aproximación internacional y comentarios a la Ley 1581 de 2012"* la Constitución contempla el habeas data como *"(…) un derecho fundamental, autónomo, diferente al derecho a la intimidad, y como un mecanismo de protección de otros derechos fundamentales frente a la eventual negligencia o a los posibles excesos en el tratamiento de datos personales"*[24]. Así, la Constitución marcó el inicio del nacimiento formal del derecho de habeas data que posteriormente fue desarrollado por la Corte Constitucional.

Resultan relevantes algunos pornunciamientos de la Corte Constitucional que desarrollan el contenido y función del derecho, así como los principios que luego serían la base de las leyes estatutarias. En primer lugar, según la sentencia T-729/02 existen tres derechos fundamentales autónomos derivados del artículo 15 Superior: i) derecho a la intimidad, ii) derecho al buen nombre y iii) derecho al habeas data. Afirma la Corte que esta diferenciación resulta de suma importancia debido a la posibilidad de obtener su protección judicial por vía de tutela de manera

[21] MANN et al. (2017), pp. 121-145.
[22] JASSERAND (2018), pp. 63-76.
[23] SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO (2018).
[24] REMOLINA (2013), p. 375.

independiente; así como, la identificación de las particularidades del régimen jurídico aplicable y las diferentes reglas para resolver la eventual colisión con el derecho a la información[25].

Habiendo definido la diferencia entre los tres derechos fundamentales autónomos, en sentencias T-303/98 y T-257/02 la Corte definió el contenido del derecho de habeas data y estableció que *"[e]l contenido básico (…) reside en la posibilidad que se otorga a toda persona para acudir a los bancos de datos y archivos de entidades públicas y privadas con el fin específico de demandar que le permitan el conocimiento, la actualización y la rectificación de las informaciones que hayan recogido acerca de ella"*, el cual constituye un instrumento de defensa de los ciudadanos[26] y se entiende como derecho fundamental autónomo[27].

Por otra parte, la sentencia T-729/02 desarrolló el tratamiento de datos y su fundamentación en principios afirmando que *"(…) el proceso de administración de los datos personales se encuentra informado por los principios de libertad, necesidad, veracidad, integridad, incorporación, finalidad, utilidad, circulación restringida, caducidad e individualidad"*[28] y estableció que el derecho de habeas data se podía también entender como el derecho a la autodeterminación para finalmente denunciar la falta de regulación respecto al tema y su importancia.

Posteriormente, se expidió la Ley 1266 de 2008 (L-1266/08) *"[p]or la cual se dictan las disposiciones generales del habeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones"*[29]. Esta ley representó el primer acercamiento hacia una legislación en torno a la protección de datos, sin embargo, se concentró en el sector e información financiera y comercial, respondiendo al contexto de ese entonces, pues buscaba que las personas tuvieran acceso a su información financiera y crediticia, la conocieran, rectificaran o aclararan para evitar que se impusieran sanciones excesivas por el no pago de una obligación y que estas se extendieran hasta después de haber saneado la obligación afectando el derecho constitucional al buen nombre.

Finalmente, se expidió la Ley Estatutaria 1581 de 2012 (L-1581/12) cuyo objeto es desarrollar el derecho constitucional al habeas data, y los demás derechos, libertades y garantías constitucionales a que se refiere el artículo 15 de la Constitución Política; así como el derecho a la información consagrado en el artículo 20[30], la cual, fue parcialmente reglamentada por los Decretos 1377 de 2013 y 090 de 2018. Así, la Corte Constitucional por medio de Sentencia T-260/12 estableció que, según el desarrollo jurisprudencial de dicha corporación, el derecho de habeas data debe ser *"(…) entendido como un derecho autónomo compuesto por la autodeterminación informática y la libertad"*[31].

En ese sentido, el derecho de habeas data en Colombia es un derecho fundamental autónomo compuesto por la autodeterminación informática y la libertad que permite que las personas conozcan, actualicen y rectifiquen las informaciones que se hayan registrado sobre ellas en bancos de datos. De igual manera, exige que las entidades que realicen tratamiento de datos observen el cumplimiento de los principios relativos a dicha actividad en pro de la protección del derecho de habeas data.

2.1.1. Ley 1581 de 2012 y sentencia C–748 de 2011

La L-1581/12 fue expedida en el 2012 como consecuencia del vacío legal en torno al habeas data fuera del contexto bancario y financiero. En ese sentido, esta ley se fundamentó en lo previamente establecido en la L-1266/08 en cuanto a desarrollar el contenido de los artículos

[25] REMOLINA (2013), p. 375.
[26] Corte Constitucional, Sentencia T-303 de 1998, de 18 de junio de 1998.
[27] Corte Constitucional, Sentencia T-257 de 2002, de 11 de abril de 2001.
[28] Corte Constitucional, Sentencia T-729 de 2002, de 5 de septiembre de 2002.
[29] Ley Nº 1266, de 2008.
[30] Ley Nº 1581, de 2012.
[31] Corte Constitucional, Sentencia T-260 de 2012, de 29 de marzo de 2012.

15 y 20 de la Constitución. No obstante, el ámbito de aplicación de la presente es más amplio, en respuesta al vacío mencionado, y *"aplica a los datos personales registrados en cualquier base de datos que los haga susceptibles de tratamiento por cualquier entidad pública o privada. Aplica en el territorio colombiano o cuando el responsable o encargado no establecido en Colombia le sea aplicable la legislación colombiana en virtud de normas y tratados internacionales"*[32].

Es importante resaltar que la L-1581/12 incorporó definiciones, principios, derechos y deberes que habían sido regulados en la L-1266/08 para el sector financiero, y a la vez introdujo nuevos conceptos. Una de las contribuciones de esta ley hace referencia al concepto de datos sensibles establecido en el artículo 5º. Este apartado incluye de manera explícita los datos biométricos y se les clasifica como datos sensibles, reconociendo así el desarrollo tecnológico y abarcando un grupo mayor de datos de los que se abarcaron con la ley anterior.

Adicionalmente, el artículo 6º establece una prohibición general al tratamiento de los datos sensibles, salvo en los siguientes casos: i) autorización expresa para el tratamiento, salvo en casos que no se requiera dicha autorización; ii) cuando se requieran para salvaguardar el interés vital del titular; iii) cuando se de en el curso de actividades legítimas por parte de organizaciones sin ánimo de lucro; vi) dentro de un proceso judicial y v) si tienen una finalidad histórica, estadística o científica[33].

Posterior a su expedición, la Corte Constitucional realizó estudio de constitucionalidad de la norma a través de sentencia C-748/11. La Corte estableció que Colombia tiene un sistema híbrido de tratamiento del derecho de habeas data, significando que existen normas generales y sectoriales que regulan este aspecto, en contraposición con el modelo europeo que es exclusivamente general y el modelo estadounidense que es sectorial[34], teniendo en cuenta que la L-1266/08 regula específicamente el sector financiero, y con la L-1581/12 se introdujo un modelo general de regulación. Además, esta última fue parcialmente reglamentada por los decretos D-1377/13 y D-090/18.

El primero reglamentó entre otras, las diversas formas de obtención de la autorización por parte de los titulares, mecanismos para obtener autorización para tratar datos sensibles, la obligación de conservar prueba de las autorizaciones otorgadas por los titulares y la posibilidad de que los titulares revoquen las autorizaciones en cualquier momento. Finalmente, introdujo la obligación de que los responsables del tratamiento desarrollen políticas para ello, que deberán ser puestas en conocimiento de los titulares para proteger sus derechos, al igual que generar avisos de privacidad para brindar claridad a los titulares y se refiere también a las transferencias y transmisiones de datos personales, al igual que desarrolla los requisitos que se deben cumplir y la forma en que dicha transferencia se puede llevar a cabo. Mientras que el segundo decreto por su parte, introdujo la reglamentación relativa al registro nacional de bases de datos. Con todo lo anterior, la Resolución No.38281 de 2020 de la SIC afirma que la ley en mención es neutral tecnológica y temáticamente. Lo que implica que *"aplica a cualquier Tratamiento con independencia de las técnicas, procesos o tecnologías – actuales o futuras- que se utilicen para dicho efecto"*[35], como lo sería el tratamiento a través de TRF.

Con la expedición de la L-1581/12, se introdujeron, dos conceptos relevantes para este estudio: la autodeterminación y la privacidad. De un lado, la sentencia T–729/02 se refiere al derecho de autodeterminación como sinónimo del derecho de habeas data. Posteriormente, sentencia T–260/12 estableció la autodeterminación como un componente del derecho constitucional de habeas data y que ésta a su vez está compuesta por las facultades que tiene el titular de los datos a conocer, rectificar, actualizar y eliminar su información de cualquier base de datos. En ese mismo sentido, sentencia T–058 de 2013 reiteró que *"[e]n cuanto al núcleo esencial del habeas data, se ha dicho que está constituido por el derecho a la autodeterminación informática y por la libertad en general, y en especial la libertad económica."*[36] Es así, que en

[32] Ley Nº 1581, de 2012.
[33] Ley Nº 1581, de 2012.
[34] Corte Constitucional, Sentencia C-748 de 2011, de 6 de octubre de 2011.
[35] Superintendencia de Industria y Comercio, Resolución No.38281, de 2020.
[36] Corte Constitucional, Sentencia T-058 de 2013, de 7 de febrero del 2013.

razón a que el derecho de autodeterminación constituye el núcleo esencial del derecho de habeas data, se puede encontrar que la Corte se refiera indistintamente a estos dos conceptos pues representan lo mismo.

De otro lado, con respecto al concepto de privacidad, la sentencia C–748/2011 establece que el término "*privacidad*" proviene del modelo anglosajón y se refiere a la intimidad. Cuando se examina la constitucionalidad del artículo 4º de la L-1581/12, esta corporación procede a establecer que privacidad *"no implica sencillamente la falta de información sobre nosotros por parte de los demás, sino más bien el control que tenemos sobre las informaciones que nos conciernen"*[37]. Se puede evidenciar, que al igual que la autodeterminación, la privacidad está ligada al derecho de habeas data en el sentido de tener control sobre la información.

Se puede concluir que Colombia ha tenido un desarrollo extenso del derecho de habeas data, desde su introducción formal por medio de la Constitución de 1991, posteriormente, un desarrollo jurisprudencial de la Corte Constitucional hasta llegar a la actualidad en donde se tiene un sistema híbrido de regulación. Este sistema está compuesto por una norma sectorial, que regula el tratamiento de datos personales en el sector financiero y una norma general que viene a llenar los diversos vacíos en materia de aplicación, deberes, derechos y sanciones en relación con su aplicación general. Es importante mencionar que, si bien la regulación actual se rige bajo el principio de neutralidad tecnológica, esta no es suficiente para enfrentar los desafíos planteados por la adopción de las tecnologías de reconocimiento facial. Por tal razón, es imperativo establecer el estado actual de la regulación de los Estados Unidos específicamente en California e Illinois y de la Unión Europea en relación con el derecho de habeas data de manera general, y con el manejo de las tecnologías de reconocimiento facial en el sector privado de manera específica.

2.2. Internacional

En razón a la insuficiencia de regulación respecto a la TRF en el ámbito nacional, se hace necesario recurrir al estudio de otras jurisdicciones que lo han desarrollado. Para ello, se seleccionaron los estados de California e Illinois en Estados Unidos y la Unión Europea. Estas dos jurisdicciones son relevantes, pues como se evidenció el actual modelo colombiano es una combinación de los modelos estadounidense y europeo. En adición a lo anterior, se tiene que, por un lado, Estados Unidos es casa de las grandes empresas de tecnología del mundo; y por otro, la Unión Europea es conocida por ser líder en temas de protección a los datos personales, contando con un modelo que es considerado proteccionista.

2.2.1. Unión Europea

La normativa europea en relación con la protección del derecho de habeas data es el Reglamento General de Protección de Datos (RGPD) que tiene por objeto establecer las normas relativas a la protección de las personas físicas en relación con el tratamiento de datos personales y su libre circulación, así como proteger los derechos y libertades fundamentales en especial el derecho a la protección de datos personales[38]. Asimismo, tiene como ámbito de aplicación *"el tratamiento total o parcialmente automatizado de datos personales, así como el tratamiento no automatizado de datos personales contenidos o destinados a ser incluidos en un fichero"*[39]. Además, esta normativa incluye una definición de datos biométricos en el artículo 4º num.14 que establece que los datos biométricos son *"(…) datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o*

[37] Corte Constitucional, Sentencia C-748 de 2011, de 6 de octubre de 2011.
[38] Parlamento Europeo y del Consejo, Reglamento (UE) 2016/679, de 27 de abril de 2016. Art. 1.
[39] Parlamento Europeo y del Consejo, Reglamento (UE) 2016/679, de 27 de abril de 2016. Art. 2.

conductuales de una persona física que permitan o confirmen la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos"[40].

En relación con el tratamiento de este tipo de datos, estos se encuentran clasificados bajo "Tratamiento de categorías especiales de datos personales" en el artículo 9º. En este se establece una prohibición general sobre el tratamiento de entre otros, datos biométricos, tales como los que utiliza la TRF, salvo que se presente una circunstancia especial y siempre que quien haga el tratamiento sea un profesional sujeto a la obligación de secreto profesional, o bajo su responsabilidad, de acuerdo con el Derecho de la Unión.

Por otra parte, la Comisión Europea publicó el Dictamen 3/2012 sobre la evolución de las tecnologías biométricas, por medio del cual se *"establecen medidas técnicas y organizativas para la protección de datos y de la intimidad que contribuyan a evitar los efectos negativos en la vida de los ciudadanos y en su derecho fundamental a la protección de datos"*[41]. Aunque este documento se expidió bajo los lineamientos de la Directiva 95/46/CE, que posteriormente fue reemplazada por el RGPD discutido en párrafos anteriores, resulta relevante para la presente investigación pues es un documento que trata en detalle el desarrollo e implementación de tecnologías de identificación biométricas y los límites a estas.

Este documento realiza un análisis jurídico y explica los riesgos para la protección de datos en la utilización de cada tipo de dato biométrico. En ese sentido, se mencionan algunos riesgos existentes cuando se utiliza la TRF: el nivel de precisión es variable; el impacto de estos sistemas dependerá de la finalidad para la que se empleen; el hecho que puede no necesitarse consentimiento para la captación de estos datos; la capacidad que tienen de ser utilizados para fines ulteriores y la susceptibilidad de suplantación de los sistemas. Finalmente, el documento cierra brindando sugerencias para disminuir los riesgos planteados en los sistemas de tratamiento de datos biométricos. Recomendaciones que incluyen el aumentar la cooperación entre los participantes, reforzar la seguridad de los sistemas e inculcar la protección de la intimidad de los usuarios desde el diseño de los sistemas[42].

También, la Comisión Europea expidió el Libro Blanco sobre la inteligencia artificial - un enfoque europeo orientado a la excelencia y la confianza el cual *"(…) ofrece alternativas políticas para facilitar un desarrollo de la inteligencia artificial seguro y fiable en Europa, que respete plenamente los valores y los derechos de los ciudadanos de la UE"*[43]. En ese sentido tiene por objeto *"(…) ayudar a Europa a convertirse en la economía con agilidad en el manejo de los datos más atractiva, segura y dinámica del mundo, lo que fortalecerá a Europa con información para reforzar sus decisiones y mejorar las vidas de todos sus ciudadanos"*[44]. Aunque este libro es un documento investigativo que no es estrictamente jurídico, brinda una idea de lo que se puede considerar como "mejores prácticas" para la implementación y adopción masiva, tanto por parte del sector público como del privado, de las tecnologías que incorporan inteligencia artificial, como es el caso de los sistemas de reconocimiento facial.

Una de las metodologías adoptadas al interior de la Unión Europea ha sido el Análisis de Impacto Tecnológico (TIA por sus siglas en inglés)[45]. Las evaluaciones de impacto se dieron a conocer en otras de áreas de investigación, sin embargo, uno de los primeros usos para esta metodología se encuentra documentado en la adopción de políticas públicas. Entre los principales tipos de evaluaciones de impacto se encuentran las evaluaciones globales, de impacto de políticas y de impacto ambiental. Así, esta metodología ha sido adoptada por diversas organizaciones nacionales e internacionales para identificar el impacto o el posible impacto de una regulación, de una industria e incluso de una tecnología en un determinado espacio.

[40] Parlamento Europeo y del Consejo, Reglamento (UE) 2016/679, de 27 de abril de 2016. Art. 4.
[41] UE (2012).
[42] UE (2012).
[43] CE (2020).
[44] CE (2020).
[45] UE (2018).

De esta forma, el sistema de evaluación de impacto de la Comisión Europea sigue un enfoque integrado que evalúa las repercusiones que las tecnologías disruptivas pueden llegar a tener frente a la adopción de políticas públicas o la vulneración de algún derecho. Los análisis de impacto se han convertido en herramientas de mitigación y atención de riesgos, tanto para el sector público como privado, con miras a evaluar las afectaciones de una nueva política o tecnología. Así, en materia de datos parsonales esta metodología se ha denominado Análisis de impacto en Privacidad (DPIA por sus sigles en inglés), aplicándose en diversas organizaciones para evaluar el impacto en materia de privacidad de algún proyecto innovador o disruptivo, tal y como lo señala el Artículo 35 del RGPD[46]. Con todo lo anterior, las evaluaciones de impacto sobre la protección de datos describen un proceso diseñado para identificar los riesgos derivados del tratamiento de datos personales y minimizarlos en la medida y con la mayor antelación posible, en especial cuando se usan tecnologías como las TRF para la recolección de los datos personales.

2.2.2. Estados de California e Illinois en los Estados Unidos

En relación con la normativa en Estados Unidos, existen dos normas relevantes para el análisis de la presente investigación. Estas son el Consumer Privacy Act (CCPA) del Estado de California y la Biometric Information Privacy Act (BIPA) del Estado de Illinois.

La CCPA *"les otorga a los consumidores más control en relación con su información personal que las empresas recolectan sobre ellos"*[47]. Esto ha garantizado nuevos derechos de privacidad a los consumidores en California dentro de los que se encuentran: i). El derecho a conocer sobre la información personal que una compañía recolecta sobre un individuo y cómo se usa y comparte; ii). El derecho a eliminar la información personal recolectada sobre los individuos, salvo algunas excepciones; iii). El derecho de "*opt-out*" o salirse de la venta de su información personal y iv). El derecho de no discriminación por ejercer los derechos conferidos por la CCPA. Del texto de la norma en comento, se puede afirmar que esta es una norma menos rígida que la europea, pues si bien otorga derechos a los usuarios o consumidores, también permite que las empresas no tengan que cumplir con ciertas exigencias amparándose en una variedad de causales.

A manera de ejemplo, sobre la obligación de eliminación de información de un titular a petición de este, consagrada en la sección 1798.105 de la ley, una empresa puede no eliminar la información amparándose en el ejercicio de libertad de expresión; para permitir únicamente usos internos que estén razonablemente alineados con las expectativas del consumidor basadas en la relación del consumidor con la empresa; para identificar y reparar errores que perjudican la funcionalidad prevista existente; entre otras[48]. En el mismo sentido, varias secciones de la norma contemplan la posibilidad de vender la información personal de los titulares, siempre que se cuente con la autorización de estos. Así, la sección No.1798.140 de la norma en mención incluye definiciones sobre la venta y la acción de vender dicha información.

Así, la norma en California se diferencia a la regulación de Illinois que rige la protección de datos en temas relativos a información biométrica, y se le conoce como Biometric Information Privacy Act (BIPA). Esta es considerada más estricta al tiempo que es específica en cuanto al tipo de datos que trata. Esta disposición incluye la recolección de datos biométricos por parte de entidades privadas, generando claridad en torno al uso de estas tecnologías. Por tal razón, la sección 10 de definiciones incluye conceptos como identificadores biométricos e información biométrica.

En este sentido, el BIPA prohíbe la venta, comercialización o cualquier actividad lucrativa con datos biométricos de los usuarios. También, prohíbe la revelación o diseminación de la

[46] UE (2022).
[47] California Consumer Privacy Act, de 2018.
[48] California Consumer Privacy Act, de 2018.

información biométrica de los usuarios, salvo en casos específicos[49]. Igualmente, la Sección 20 de esta ley, otorga a los usuarios el derecho de acción que a su vez contempla un régimen sancionatorio específico por violación y abuso por parte de entidades privadas a usuarios en relación con datos biométricos.

A manera de ejemplo, en el caso *Patel v. Facebook Inc.,* 2015, se alegaba que Facebook había infringido el BIPA al utilizar los datos biométricos faciales de los usuarios sin su autorización para perfilarlos, crear plantillas faciales y sugerir etiquetados en las fotos, lo que no solo permitía identificar personas en las millones de fotos de Facebook, sino que podían identificar sus amigos y las localizaciones. En este caso, la Corte de Apelaciones del Noveno Circuito de los Estados Unidos decidió que los demandantes podían reclamar indemnizaciones de Facebook teniendo en cuenta el incumplimiento al BIPA, en el sentido de que no contar con autorización, ocasionaba perjuicios a los usuarios, aunque estos no fueran materiales. Facebook había infringido la norma de manera directa, al no haber obtenido la respectiva autorización de los usuarios para utilizar la TRF en sus fotos con el fin de realizar perfilamiento de los usuarios[50].

En 2016, Martínez, Neal y otros radicaron una demanda en contra de SNAPCHAT, INC., por presuntamente recolectar datos de sus usuarios a través de la funcionalidad de filtros, con TRF, sin informarles previamente conforme lo ordena el BIPA. Este caso nunca llegó a juicio[51], pero la Corte de California en un análisis preliminar estableció que al no informar de manera clara a los usuarios que a través de los filtros se utilizaba TRF para guardar información biométrica violó de manera directa la norma y se recolectaba información de manera fraudulenta[52].

Por último, en 2019, *Rosenbach v. Six Flags Entertainment*, los padres de un menor demandaron al parque Six Flags por la obtención de información biométrica a través de la huella dactilar sin el consentimiento de estos y por el hecho de no haber revelado qué se hizo con esa información, en directa violación del BIPA. Los demandados alegaban que para que la demandante pudiera obtener indemnización, la sola violación a la ley no era suficiente, sino que se tenía que probar la ocurrencia de un daño. Sin embargo, la Corte Suprema de los Estados Unidos estableció que, bajo el BIPA, no se requiere que los demandantes sufran daños materiales para que estén facultados a reclamar indemnizaciones por parte de entidades que violan dicha norma. En ese sentido, es claro que el solo hecho de incumplir las reglas estipuladas en la norma de Illinois faculta a los usuarios a obtener compensación[53].

Habiendo definido la evolución y el estado actual de la regulación de habeas data en Colombia en relación con TRF o biométricas, y habiendo hecho un resumen del estado actual de la regulación de protección de datos y su aplicación en la Unión Europea y Estados Unidos (California e Illinois) como jurisdicciones relevantes, el siguiente apartado se encarga de desarrollar el análisis de dichos bloques normativos para finalmente concluir, si en Colombia la normativa vigente es suficiente para enfrentar la implementación de las tecnologías de reconocimiento facial por parte del sector privado de modo que se preserve el derecho de habeas data de los usuarios; o si por el contrario, es necesario realizar algunas modificaciones o adiciones a la ley.

3. Análisis de la regulación colombiana vs. la regulación de la Unión Europea y de California e Illinois en los Estados Unidos

Colombia maneja un modelo híbrido de regulación basado en: i) Normas sectoriales de protección de datos (como es el caso de la L-1266/08), y ii) Regulación basada en una norma general tal como la L-1581/12. La conveniencia de uno u otro modelo es una discusión más

[49] Biometric Information Privacy Act, de 2008.
[50] Corte de Apelaciones para el Noveno Circuito de los Estados Unidos, N. 18-15982, de agosto 8 de 2019.
[51] Se resolvió en arbitraje, no hay reportes públicos.
[52] Superior del Condado de Los Ángeles de California, N. 2:2016cv05182, de mayo 23 de 2016.
[53] Corte Suprema de los Estados Unidos, N. 123186, de enero 25 de 2019.

amplia que no se abarcará en el presente trabajo, sino que se realizará un análisis normativo de las jurisdicciones seleccionadas, así como de la situación actual en torno a la TRF, para finalmente concluir.

3.1. Definiciones relevantes

Es importante resaltar que los marcos normativos bajo estudio incluyen definiciones específicas en relación con conceptos técnicos respecto a la protección de datos. Estas definiciones resultan relevantes pues permiten tanto a personas naturales y jurídicas, así como a jueces y autoridades situarse en un terreno común que facilite el entendimiento y la aplicabilidad de la norma.

Así, tanto la norma europea, como la de California e Illinois, incluyen definiciones específicas en torno al concepto de **datos e identificadores biométricos**; mientras que la norma colombiana no incluye una definición específica al respecto, sino que circunscribe dicho concepto dentro de la definición de dato sensible. Si bien, tanto el RGPD como la CCPA y el BIPA consideran los datos biométricos como datos sensibles, estas dos últimas brindan definiciones específicas del mismo. Brindar una definición específica de dato biométrico es relevante en Colombia pues, como se verá a continuación, el concepto en el país no ha sido aplicado uniformemente como consecuencia directa de la falta de significado en la norma.

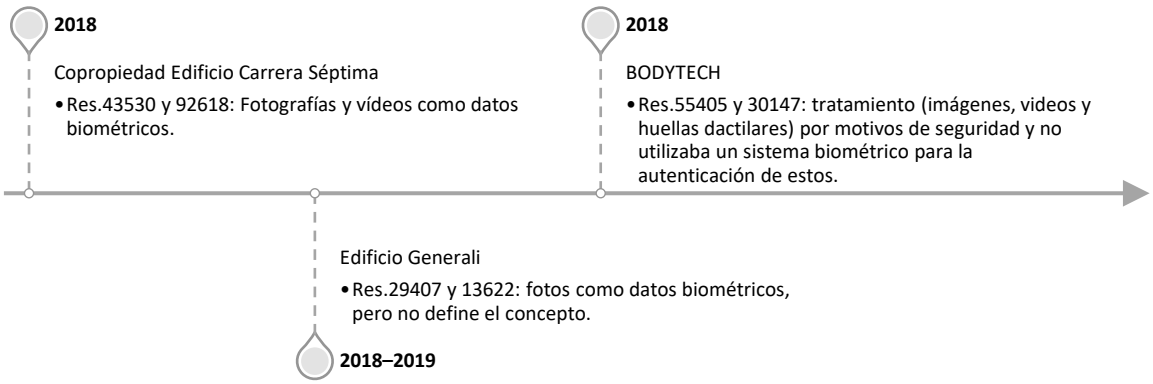
De otro lado, el RGPD en su artículo 4º num.14 establece que los datos biométricos son *"(…)* ***datos personales obtenidos a partir de un tratamiento técnico específico****, relativos a las características físicas, fisiológicas o conductuales de una persona física que permitan o confirmen la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos*"[54] (Negrilla y subraya propias). Por su parte, la normativa estadounidense es específica, en la CCPA sección 1798.140 literal c) establece que *"información biométrica significa las características fisiológicas, biológicas o conductuales de un individuo, incluyendo la información relativa al ADN, que es usada sola o en combinación con otro tipo de información para identificar a un individuo"*[55]. De otro lado, el BIPA, incluye el concepto de **identificador biométrico**, como el modo de obtención de la información biométrica y, asimismo, excluye qué tipos de prácticas no pueden considerarse como tal. Así, según la sección 10 de esta norma, un identificador biométrico es aquel que tiene la capacidad de escanear el iris o la retina, la huella dactilar, la voz o la geometría facial.

Así, es posible evidenciar que las normas mencionadas desarrollan específicamente qué se considera por dato biométrico, aunque estas definiciones no sean coincidentes. Por un lado, la CCPA establece que dato biométrico es cualquier característica física o conductual de un individuo; mientras que para el RGPD y el BIPA dato biométrico solo son aquellos datos obtenidos a través de tratamientos técnicos que permitan la identificación de un individuo. Se puede concluir que el CCPA tiene un concepto amplio de dato biométrico y en contraposición tanto el RGPD como el BIPA manejan un concepto cerrado y específico.

Por otra parte, la regulación colombiana establece que los datos biométricos son datos sensibles, pero, no estipula qué tipo de tecnología o técnica se necesita para que se considere biométrico o si no se requiere que sea obtenido por medios técnicos específicos. Sobre el particular, es relevante analizar la aplicación de los artículos 28 y 29 del Código Civil que establecen que *"las palabras de la ley se entenderán en su sentido natural y obvio, según el uso general de las mismas palabras"*[56] cuando no exista definición legal y que "*las palabras técnicas de toda ciencia o arte se tomarán en el sentido que les den los que profesan la misma ciencia o arte; a menos que aparezca claramente que se han formado en sentido diverso*"[57].

[54] Parlamento Europeo y del Consejo, Reglamento (UE) 2016/679, de 27 de abril de 2016. Art. 4.
[55] California Consumer Privacy Act, 2018. Section. 1798.140 (c)..
[56] Ley Nº 57, 1887. Art. 28.
[57] Ley Nº 57, 1887. Art. 28.

Sin emabrgo, no existe una única definición relativa a datos biométricos. Este no es un concepto pacífico y en ese sentido, remitirse a la aplicación de los artículos citados del Código Civil, no resolvería el vacío legal en el ordenamiento colombiano. Pues se enfrenta al dilema de qué concepción aplicar y por qué. ¿Cuál es el sentido natural y obvio de dato biométrico? Y si la definición científica planteada en la primera parte de este texto establece que la definición de datos biométricos debe cubrir el proceso técnico a través del cual se captura la información y se transforma a formato digital, ¿por qué la SIC no aplica esta definición? Así, será indispensable revisar las diversas decisiones de la SIC, como autoridad competente, que se han presentado sobre la recolección y tratamiento de datos personales.



Cuadro 5. Resoluciones SIC relevantes sobre datos biométricos. Elaboración propia.

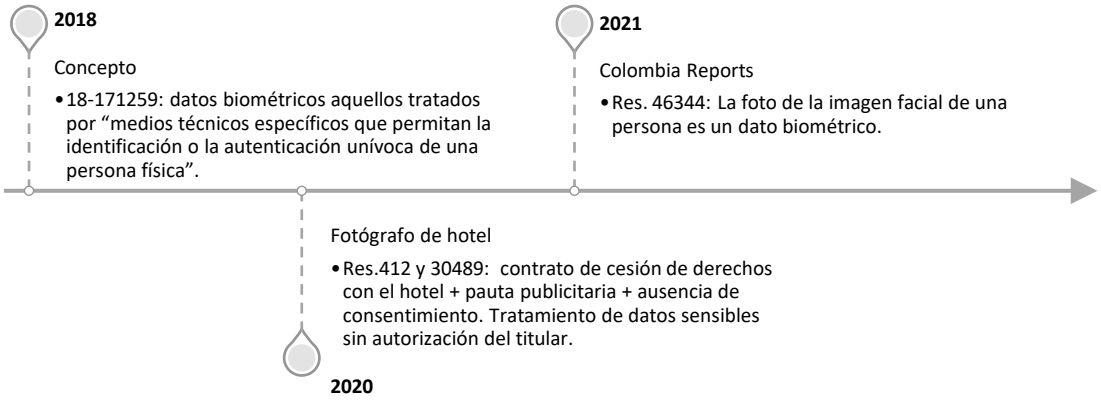
En 2018, la SIC impuso sanciones a dos edificios sometidos al régimen de propiedad horizontal, la Copropiedad Edificio Carrera Séptima[58] y el Edificio Generali[59], por realizar tratamiento de datos sensibles sin contar con autorización del titular, argumentando que las fotografías y vídeos eran tal, por ser datos biométricos. Aunque la inclusión de las fotografías como datos biométricos en estos casos no fue explícita en primera instancia, la SIC, mediante Resolución No.13622 en segunda instancia del caso Generali, estableció que las fotos si eran datos biométricos pero no definió el concepto.

En contraposición, en el caso BODYTECH[60], la SIC estableció que el establecimiento sí bien recolectaba la imagen de los titulares, esta lo hacía por motivos de seguridad y no utilizaba un sistema biométrico para la autenticación de estos. La entidad consideró que la empresa no estaba haciendo tratamiento de datos sensibles y, por lo tanto, en lo que respecta a este cargo en específico, no procedía sanción. En sede de apelación esta decisión fue confirmada, a pesar de que la Resolución No.30147 de 2019 consideró como dato biométrico aquella información relativa a las características físicas y comportamentales.

[58] Superintendencia de Industria y Comercio, Resolución No.43530, de 2018; Superintendencia de Industria y Comercio, Resolución No.92618, de 2018.

[59] Superintendencia de Industria y Comercio, Resolución No.29407, de 2018; Superintendencia de Industria y Comercio, Resolución No.13622, de 2019.

[60] Superintendencia de Industria y Comercio, Resolución No.55405, de 2018.



Cuadro 6. Resoluciones SIC relevantes sobre datos biométricos. Elaboración propia.

Igualmente, por medio del Concepto No.18-171259 de 2018, la SIC afirmó que datos biométricos eran aquellos tratados por *"medios técnicos específicos que permitan la identificación o la autenticación unívoca de una persona física"*[61], en consonancia con las definiciones del RGPD y el BIPA.

Recientemente, en las Resoluciones No.30412 y 30489 de 2020, la SIC resolvió un caso referente a un fotógrafo que fue contratado para tomar fotos de un matrimonio celebrado en un hotel en Medellín. Posterior al evento, el fotógrafo celebró un contrato de cesión de derechos con el hotel, para que este último pudiera utilizar dichas fotos en una pauta publicitaria en una revista, sin que el fotógrafo contara con el consentimiento de la pareja. El problema recaía en el hecho de que en una de las fotos aparecía el rostro de los novios. Respecto a esta situación, la SIC consideró que el fotógrafo estaba haciendo tratamiento de datos sensibles sin autorización del titular, afirmando que la sola fotografía contenía datos biométricos, así: *"(…) nótese que algunas fotos captan la imagen del rostro o la cara de las personas, las cuales son consideradas como información biométrica. Los datos biométricos, a su vez, son un ejemplo de dato sensible tal y como se puede constatar en la definición legal del artículo 5 de la Ley 1581"*[62]. Cabe resaltar que en estos casos la SIC en ningún momento hizo referencia a identificadores biométricos o un tipo de tecnología específica por medio de la cual debían ser obtenidos estos datos, dando a entender que la sola fotografía o imagen ya es considerada como dato biométrico.

En este mismo sentido, por medio de la Guía sobre el Tratamiento de las Fotos como Datos Personales, publicada en 2020, la SIC consideró que aquellas imágenes *"que captan la imagen de la cara de las personas u otras partes de su cuerpo que permiten identificarlas"* son información biométrica, estando estas definiciones más alineadas con lo que se estipula en el CCPA.

Finalmente, en 2021 la SIC se pronunció sobre una solicitud de bloqueo temporal del portal web -Colombia Reports-, pues había utilizado la foto del rostro de una periodista para expresar una opinión sobre un medio de comunicación sin su autorización. En esta oportunidad, la SIC reafirma su línea sobre que la foto de la imagen facial de una persona es un dato biométrico, pero no lo define en sus métodos o técnicas[63].

Debido a la amplitud y ambigüedad que conlleva el término "dato biométrico", y teniendo en cuenta que en la legislación colombiana no hay definición de este concepto, en palabras de Giraldo, la norma resulta insuficiente al momento de ser aplicada[64] y puede tener un impacto directo en las sanciones de determinadas conductas como se pudo evidenciar. Adicionalmente, la ausencia de una estructura delineada y clara para determinar qué es y qué no es un dato

[61] SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO (2018).
[62] Superintendencia de Industria y Comercio, Resolución No.30412, de 2020.
[63] Superintendencia de Industria y Comercio, Resolución No.46344, de 2021.
[64] AGUDELO-GIRALDO (2018) p. 183.

biométrico, sus tipologías y sus técnicas puede llevar a interpretaciones inconsistentes alrededor del concepto.

De esta forma, si se adoptará en Colombia el concepto de dato biométrico esgrimido por las resoluciones del caso del fotógrafo y las copropiedades, la guía de tratamiento de fotos, el caso del portal Colombia Reports y la CCPA, el espectro cubierto por esta definición sería muy amplio, bajo el cual, dato biométrico es cualquier rasgo físico o conductual indistintamente de si es tratado por medios técnicos específicos que permitan la identificación o verificación de la identidad de una persona. Esto entre otros, podría incluir videos de vigilancia que no integren tecnologías de reconocimiento facial, fotografías que capten rostros almacenadas en dispositivos móviles o computadores, entre otros. Lo que en consecuencia tornaría la aplicación de la norma respecto de datos biométricos, muy complicada.

Mientras, que si se adoptará la definición estipulada en el RGDP y el BIPA y esgrimida en el caso BODYTECH y en el Concepto No.18-171259 de 2018, dato biométrico será entonces aquel que obtenido bajo medios técnicos específicos permiten la identificación o verificación de la identidad de una persona. En caso de no ser obtenidos por medio de una tecnología con estos atributos dicho dato sería considerado como un dato personal, como lo estableció la SIC en el caso BODYTECH. Bajo este entendido, dato biométrico solo será aquel que se obtenga a partir del escaneo del rostro por parte de un dispositivo que integre reconocimiento facial.

De lo anterior se observa un vacío alrededor del concepto de dato biométrico en la legislación colombiana y una ambigüedad en la interpretación del concepto por parte de la autoridad de protección de datos. Esta situación ha impactado en la aplicación de sanciones lo que en consecuencia afecta la seguridad jurídica. Adoptar un concepto delimitado y específico, tal como el incorporado tanto el RGPD como el BIPA, no solo da claridad alrededor de lo que es y no es dato biométrico, sino también contribuye a la creación de un terreno legal común tanto para jueces, autoridades, usuarios y empresas que permite el entendimiento del concepto, de las tecnologías que se desarrollan alrededor de este tipo de datos y por lo tanto facilita una aplicación eficiente de las normas.

3.2. Riesgos

Debido a que los datos biométricos que se utilizan en la TRF son rasgos faciales y corporales de fácil recolección, se puede afirmar que el aval del titular no representa un impedimento para su obtención. Por ejemplo, en la ciudad de Como, la municipalidad instaló cámaras de seguridad que integraban la TRF de Huawei sin informar a los ciudadanos y sin contar con un marco legal claro que definiera y limitara la situación. Durante el tiempo que estuvieron instaladas, escanearon rasgos faciales de miles de transeúntes, sin que estos se enteraran[65]. En este caso, no es claro si la información recolectada por las cámaras es únicamente tratada por la municipalidad, y en ese sentido estaría amparada bajo la excepción formulada en el literal g) del artículo 9 del RGPD, o si, por el contrario, la empresa privada también tiene acceso a ella. Cabe entonces preguntarse, ¿de qué manera se debería abordar el tema de asociaciones público-privadas en este tipo de contratos? De nuevo se hace evidente la importancia de un marco regulatorio claro al respecto.

Si bien, tanto la norma nacional como el CCPA, el BIPA y el RGPD contemplan que no se puede recolectar datos personales sensibles sin que medie autorización expresa del titular, por la forma de funcionamiento de este tipo de tecnologías esa falta de autorización no representa un impedimento para obtener los datos de los titulares, como se evidenció en el caso anterior. Incluso habiendo dado autorización para el tratamiento, no existe un límite legal sobre lo que se puede hacer con este tipo de información íntimamente ligada con la identidad de los titulares, siempre y cuando medie dicha autorización. Un ejemplo de ello, es la demanda que instauró

[65] PI (2020).

Anne Longfield, excomisionada infantil del Reino Unido, en contra de la aplicación TikTok[66] por recolectar datos personales sensibles de menores de edad, tales como geolocalización y posiblemente reconocimiento facial, sin contar con la autorización de sus padres o cuidadores.

Asimismo, otro de los riesgos que representan estas tecnologías, es el alto grado de imprecisión que acarrean estos sistemas. Sabiendo que, las TRF se fundamentan en algoritmos y plantillas numéricas, el rango de imprecisión es alto. Así, en un video publicado por *Coding Rights*, 2021, se establece que los sistemas de reconocimiento facial operan mejor en hombres que en mujeres, y a su vez tienen mejor desempeño en personas de piel clara que de piel oscura. Lo que significa que en mujeres de piel oscura la probabilidad de obtener error o una identificación errónea es mayor[67].

Adicionalmente, la información sujeta al tratamiento debe ser veraz, completa y exacta; sin embargo, los sesgos mencionados anteriormente, pueden ocasionar que el tratamiento de los datos biométricos no sea adecuado e incluso que la información no corresponda con los rasgos faciales del titular, en directa violación al principio de veracidad. Por ejemplo, en el caso de *Coding Rights*, se estableció que el algoritmo de reconocimiento facial no era capaz de identificar el género de una figura pública como Oprah Winfrey. Frente a este problema, la ley es reactiva, pero ¿cabe la posibilidad de imponer sanciones por algoritmos que contienen sesgos? Y más importante aún ¿es esa la manera de enfrentar este desafío?

Finalmente, otro riesgo es la posibilidad de transferencia de bases de datos que almacenen plantillas de los rasgos faciales de los usuarios. Aunque esto es posible con todo tipo de bases de datos, en este caso particular cobra mayor relevancia no solo porque se estarían transfiriendo datos sensibles que se relacionan de manera directa a la identidad, sino porque si se adiciona el nivel de imperfección que acarrean estos sistemas, también se transfiere información errada en detrimento de los derechos de los usuarios.

Producto de esto, organizaciones EDRi promueven una acción regulatoria con el fin de que se defina de manera clara el uso e implementación de este tipo de tecnologías y buscan la prohibición absoluta de su uso en lugares públicos a través de campañas como "*Reclaim your Face*" [68] que argumenta que el reconocimiento facial puede y será usado en contra de los ciudadanos por gobiernos y corporaciones, en función de quiénes somos y cómo nos vemos[69]. De manera similar, el Supervisor Europeo de Protección de Datos (EDPS) se pronunció, en respuesta a un borrador de reglas que contempla la implementación de reconocimiento facial en casos de niños perdidos y actos terroristas, estableciendo que este tipo de tecnologías debían ser prohibidas en Europa considerando su profunda y no democrática intrusión en la vida privada de las personas[70].

En esta línea, tanto la L-1581/12 como el RGPD no contemplan una prohibición expresa a la transferencia de datos personales, siempre que los terceros países cuenten con estándares de seguridad para los derechos de los titulares y que a su vez estén aprobados por las autoridades nacionales. Esta transferencia, hace parte de la información que se le debe suministrar al titular al momento de la recolección y autorización del tratamiento de los datos, y, por lo tanto, cada titular debe autorizar dicha operación. Sin embargo, el BIPA contempla una prohibición expresa de transferencia de bases de datos salvo, entre otras, medie autorización del titular.

Así, aunque la regulación colombiana en relación con la protección de datos, de manera general, es fuerte y contempla de manera clara derechos a favor de los titulares, deberes y responsabilidades en cabeza de responsables y encargados, mecanismos de defensa de los derechos y procedimientos de investigación y sanciones, de cara a la implementación de las TRF es insuficiente para enfrentar los desafíos y riesgos que presenta la implementación de este tipo

[66] , Superintendencia de Industria y Comercio, Resolución No.62132, de 2020. La SIC ordenó a TikTok cumplir los estándares de protección de datos establecidos en la normativa.
[67] CODING RIGHTS ORGANIZATION (2021).
[68] EDRI et al. (2020).
[69] UE (2022).
[70] NEWSHUB (2021).

de tecnologías. En primera medida, por la ambigüedad respecto de la definición de dato biométrico; y en segundo lugar por la complejidad que reviste su uso.

4. Aspectos de cambio y propuestas

Se ha evidenciado que la regulación de las TRF, tanto en el sector público como en el privado, no es un tema pacífico. Producto de ello, existen organizaciones como el *Biometrics Institute*, *Coding Rights*, la *Electronic Frontier Foundation* entre otros, que se dedican a investigar la aplicabilidad, riesgos y oportunidades de mejora de estas tecnologías para así determinar la mejor manera de implementarla en relación a la normativa vigente.

Como consecuencia de las investigaciones realizadas, y del análisis expuesto, se propone la expedición de una guía por parte de la SIC que trate de manera específica el tema de tecnologías biométricas, en especial la TRF que contenga pero no se limite a: i) lineamientos para la adopción por parte de las empresas del concepto de privacidad desde el diseño y mejores practicas en privacidad; ii) impulsar iniciativas de investigación en dichas tecnologías; iii) la recomendación de adecuación de la norma vigente y iv) la posibilidad de adoptar "*Privacy Enhancing Technologies*" para mejorar la actividad de vigilancia de la SIC y prevenir violaciones al derecho de habeas data.

En este sentido, según Kim, en la conferencia *CODEX Future Law* 2021, la manera en que la tecnología podría seguir avanzando y ser implementada para su uso sin poner en riesgo los derechos de los usuarios es una mezcla de los siguientes tres factores: i) Estandarización: estándares globales consistentes en diferentes jurisdicciones, las cuales permiten mayor control y mitigación de riesgos; ii) Regulación: la cual es inevitable y debe buscar el balance para permitir el desarrollo tecnológico e iii) Innovación basada en principios: las compañías deben tener sus principios que guíen su desarrollo y comportamiento en el mercado. Lo ideal es que cada industria tenga sus principios éticos y los tengan en consideración a lo largo del diseño, desarrollo e implementación de productos[71].

De manera similar, la regulación por sí sola no puede asegurar la seguridad y el respeto a los derechos de los usuarios y, por lo tanto, es necesario aliarse con las empresas de tecnología teniendo en cuenta que estas se encuentran en una mejor posición para hacerlo en razón a sus conocimientos[72]. Asimismo, Wilson establece la importancia de educar a los ingenieros que diseñan los sistemas y softwares de recolección y tratamiento de datos, en el derecho de habeas data y protección y tratamiento adecuado de datos teniendo en cuenta el contexto actual de tecnificación, automatización y desarrollo de nuevas tecnologías, tales como la TRF, para que dichos sistemas incluyan el concepto de privacidad desde el diseño y por defecto[73].

En ese sentido, la guía entonces deberá propender por la estandarización de conceptos conforme la tendencia global, así como promover la adopción de la privacidad desde el diseño por parte de los desarrolladores y empresas que trabajan con este tipo de tecnologías, al igual que promover la adopción de mejores practicas en temas de privacidad, incorporando principios que guíen todos los aspectos de desarrollo e implementación de producto que se ajusten con el objetivo de la empresa, pero que tengan al usuario como centro del desarrollo.

4.1. Evaluación de impacto en privacidad

Las Evaluaciones de Impacto sobre la Privacidad y la Protección de Datos (PIAs / DPIAs por sus siglas en inglés) son herramientas para organizaciones con miras a gestionar los riesgos que se derivan de un modelo de negocio o de un producto. La realización de una EIPD mejorará la concienciación de la organización sobre los riesgos de protección de datos asociados a un proyecto. Esto ayudará a mejorar desde el diseño la comunicación sobre los riesgos de la

[71] KIM (2021).
[72] HOFFMAN Y RIMO (2018), pp. 546-560.
[73] WILSON en SVANTESSON Y KLOZA (2017), pp. 379-390.

protección de datos con las partes interesadas pertinentes. Así, las EIPD garantizan y demuestran que la organización cumple con la regulación en materia de datos y de igual forma evitar sanciones.

De acuerdo con el RGPD, una DPIA es obligatoria cuando el procesamiento de datos "puede dar lugar a un alto riesgo para los derechos y libertades de las personas físicas". Esto es especialmente relevante cuando se introduce una nueva tecnología de procesamiento de datos, cómo lo serían las TRF. En los casos en los que no está claro si la EADP es estrictamente obligatoria, la realización de una EADP sigue siendo una buena práctica y una herramienta útil para ayudar a los responsables del tratamiento a cumplir la legislación sobre protección de datos.

El Grupo de Trabajo del Artículo 29 (GT Art.29), formado por los representantes de cada autoridad de protección de datos de la UE, ha adoptado directrices sobre las EIPD y sobre si el tratamiento puede dar lugar a un alto riesgo a efectos del RGPD[74]. Para evaluar si el tratamiento puede suponer un riesgo elevado, el GT Art.29 ha establecido algunos criterios para tener en cuenta: i) Tener por objeto la evaluación o puntuación, incluida la elaboración de perfiles y la predicción; ii) Tener como finalidad la toma de decisiones automatizada con efectos jurídicos o significativos; iii) Cuando la recolección se base en datos sensibles, como lo serína los datos recolectados a través de TRF; entre otros criterios.

Con todo lo anterior, el RGPD en su Artículo 35.1 y considerandos 89 y 91 establece que el uso de una nueva tecnología puede desencadenar la necesidad de realizar una EIPD. Esto se debe a que el uso de una nueva tecnología puede implicar formas novedosas de recogida y uso de datos, posiblemente con un alto riesgo para los derechos y libertades de las personas. De hecho, las consecuencias personales y sociales del despliegue de una nueva tecnología pueden ser desconocidas. Una EIPD ayudará al responsable del tratamiento a comprender y tratar dichos riesgos.

Así, esta evaluación hace parte de la adopción del principio de privacidad desde el diseño y, en consecuencia, podría mitigar los riesgos relevantes a los sesgos que pueden incluir los algoritmos de reconocimiento facial, reduciendo la tasa de error en beneficio de los titulares. A pesar de que el concepto central de esta investigación no es Inteligencia Artificial, muchas técnicas de biometría, tal como la relacionada con el reconocimiento facial, implican el uso de esta tecnología a través de algoritmos o modelos de identificación o verificación. En ese sentido, sería beneficioso incluir este ítem en la guía en razón a los beneficios que representa frente a la efectiva protección del derecho de habeas data.

4.2. Recomendación de Adecuación Normativa

Debido a la insuficiencia normativa, y reconociendo que la SIC no emite Resoluciones ni conceptos jurídicamente vinculantes en los términos que una sentencia podría serlo, se propone que de acuerdo al literal i) del artículo 21 de la L-1581/12 y el Decreto 4886 de 2011, la SIC sugiera la adecuación de la norma en el sentido de buscar definir de manera clara y expresa qué se entiende por dato biométrico, adoptando la definición esbozada en el caso BODYTECH, en el RGPD y el BIPA, en razón a los avances tecnológicos, para así estandarizar conceptos y en esa medida poder aplicar la norma de manera mas eficiente respecto de dichas tecnologías. Igualmente, podría sugerir la inclusión de una prohibición expresa respecto a la transferencia de bases de datos que contengan datos biométricos obtenidos por medio de tecnologías de reconocimiento facial en respuesta a la información sensible que contienen, tal como lo contempla el BIPA.

Es importante recalcar que esta propuesta de adecuación normativa no es excluyente de otros tipos de regulación, como lo sería la autoregulación y adopción de buenas prácticas en las empresas. Sin embargo, debido a la incursión de estas tecnologías y la ausencia de transparencia

[74] GT ART.29 (2017).

de las empresas frente a la realización de un análisis de impacto, es indispensable que la autoridad en ecargada, en este caso la SIC, establezca reglas claras más allá de recomendaciones y guías formativas. De esta forma, la norma sanearía el vacío encontrado alrededor del concepto de dato biométrico, brindando seguridad jurídica al respecto y establecería la prohibición de transferencia de bases de datos que contengan información biométrica en pro de la protección del derecho de habeas data.

5. Conclusiones

La TRF es un ejemplo de tecnología blanda y flexible, cuyo funcionamiento se basa en datos biométricos, los cuales son procesados por sistemas algorítmicos que permiten la identificación o verificación de individuos. Puede ser aplicada a una diversidad de situaciones, tales como verificación de identidad en transacciones bancarias, o asistencia a personas en condición de discapacidad, entre otras. Por tal razón, el marco regulatorio de este tipo de tecnología resulta relevante, toda vez que los riesgos que representa para los usuarios son altos, teniendo en cuenta no solo la facilidad de obtención de los datos; sino también la posibilidad de ocurrencia de un indebido tratamiento de la información, pues no son sistemas del todo eficaces o infalibles y poseen altos márgenes de error.

Igualmente, se estableció que Colombia cuenta con un aparato normativo fuerte sobre la protección de datos, de manera general, producto de la evolución que el derecho al habeas data ha tenido a través de pronunciamientos jurisprudenciales y posterior regulación mediante la L-1581/12 y sus decretos. No obstante, se evidenció que existe un vacío legal frente a la definición de dato biométrico, así como una interpretación imprecisa del concepto por parte de la SIC, lo que permite concluir que la normativa nacional es insuficiente para enfrentar los retos y desafíos planteados por la TRF.

Se describieron las regulaciones de la Unión Europea y Estados Unidos (California e Illinois), las cuales incluyen de manera expresa la definición de datos biométricos a través del Reglamento General de Protección de Datos de la Unión Europea, la California Privacy Act (California) y el Biometric Information Privacy Act (Illinois). Se concluyó que los modelos planteados por el RGPD y el BIPA de Illinois son más adecuados, por la claridad que brindan sobre concepto de dato biométrico y el tipo de tecnología que se vincula.

Si bien es cierto, la regulación colombiana se rige bajo el principio de neutralidad tecnológica, no queda claro si al momento de ser aplicada la norma esta cuenta con las suficientes herramientas no solo para hacer cumplir los lineamientos la misma, sino si cuenta con el poder y la capacidad suficiente de imponer sanciones efectivas a las empresas, están recolectando datos biométricos de sus usuarios. Por tal razón, el trabajo plantea una propuesta que cubre varios frentes que pretenden cubrir no solo una adecuación normativa, sino que se incluye la posibilidad de la elaboración de un análisis de impacto en materia de protección datos y la colaboración entre el sector privado y la autoridad tanto en investigación como en educación y formación de los privados en principios y lineamientos básicos en torno al respeto y protección del derecho de habeas data.

BIBLIOGRAFÍA CITADA

AGUDELO-GIRALDO, OSCAR (2018): "Los calificativos del Derecho en las Formas de Investigación Jurídica", en: Agudelo-Giraldo, Óscar; León-Molina, Jorge Enrique; Prieto-Salas, Manuel Asdrúbal; Alarcón-Peña, Andrea y Jiménez-Triana, Juan Carlos, La pregunta por el método: derecho y metodología de la investigación (Bogotá, Editorial Universidad Católica de Colombia), pp. 17-44.

AUNGER, ROBERT (2010): "Types of Technology", en: Technological Forecasting and Social Change (Vol. 77, Nº 5), pp. 762-782.

BÉNICHOU, BRAHIM (2019): "Taylor Swift Is Watching You Watching Her", en: Data Protection. Disponible en: https://lirias.kuleuven.be/3014655?limo=0 [visitado el 08 de febrero de 2021].

CDEI (2020): "Facial Recognition Technology", en: Centre for Data Ethics and Innovation. Disponible en: https://www.gov.uk/government/publications/cdei-publishes-briefing-paper-on-facial-recognition-technology [visitado el 08 de febrero de 2021].

CE (2020): Libro Blanco sobre la inteligencia artificial - un enfoque europeo orientado a la excelencia y la confianza (Bruselas, Comisión Europea de la Unión Europea).

CODING RIGHTS ORGANIZATION (2021): "Reconhecimento Facial: raça, gênero e território", en: From Devices to Bodies. Disponible en: https://www.youtube.com/watch?v=omP93gEuQfI&feature=youtu.be&ab_channel=CodingRights [visitado el 08 de febrero de 2021].

CRAWFORD, KATE (2019): "Halt the Use of Facial-Recognition Technology until It Is Regulated", en: Nature (Vol. 572, Nº 7771), pp. 565-565.

EDRI; SHARE FOUNDATION; HERMES CENTER; BITS OF FREEDOM; ARTICLE19; HOMO DIGITALIS (2020): "Campaign "Reclaim Your Face" calls for a Ban on Biometric Mass Surveillance". Disponible en: https://edri.org/our-work/campaign-reclaim-your-face-calls-for-a-ban-on-biometric-mass-surveillance/ [visitado el 26 de abril de 2021].

EFF (2017): "Face Recognition", en: Electronic Frontier Foundation. Disponible en: https://www.eff.org/pages/face-recognition [visitado el 08 de febrero de 2021].

EID (2021): "Face Recognition: How It Works and Its Safety", en: Electronic Identification. Disponible en: https://www.electronicid.eu/en/blog/post/face-recognition/en [visitado el 08 de febrero de 2021].

ESA (2021): "What is Technology?", en: The European Space Agency. Disponible en: http://www.esa.int/Enabling_Support/Space_Engineering_Technology/What_is_technology [visitado el 08 de febrero de 2021].

GT ART. 29 (2017): "Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679", en: Article 29 data protection working party. Disponible en: https://ec.europa.eu/newsroom/article29/items/611236 [visitado el 08 de febrero de 2021].

HOFFMAN, DAVID Y RIMO, PATRICIA (2018): "It Takes Data to Protect Data", en: Selinger, Evan; Polonetsky, Jules y Tene, Omer (Eds.), The Cambridge Handbook of Consumer Privacy (Cambridge, Cambridge Law Handbooks) pp. 546-560.

JASSERAND, CATHERINE (2018): "Avoiding Terminological Confusion Between the Notions of 'Biometrics' and 'Biometric Data': An Investigation Into the Meanings of the Terms From a European Data Protection and a Scientific Perspective", en: International Data Privacy Law (Vol. 6, Nº 1), pp. 63-76. Disponible en: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3230339 [visitado el 08 de febrero de 2021].

KIM, THOMAS (2021). "Conferencia CODEX FUTURE LAW 2021. Futere Law. "Opening remarks"". Disponible en: https://www.youtube.com/watch?v=7iqkbZqURtw [visitado el 08 de febrero de 2021].

LIAW, HONGMIN; CHIU, MEI HUNG Y CHOU, CHIN CHEUNG (2014): "Using Facial Recognition Technology in the Exploration of Student Responses to Conceptual Conflict Phenomenon", en: Chemistry Education Research and Practice (Vol. 15, Nº 4), pp. 824-834. Disponible en: https://doi.org/10.1039/C4RP00103F [visitado el 08 de febrero de 2021].

LLAMAS, JHONATAN (2020): "Tipos de Tecnología", en: Economipedia. Disponible en: https://economipedia.com/definiciones/tipos-de-

tecnologia.html#:~:text=La%20tecnolog%C3%ADa%20blanda%20consiste%20en,pueden%20almacenar%20de%20forma%20tangible [visitado el 08 de febrero de 2021].

MANN, MONIQUE Y SMITH, MARCUS (2017): "Automated Facial Recognition Technology: Recent Developments and Approaches to Oversight", en: The University of New South Wales Law Journal (Vol. 40, Nº 1), pp. 121-145. Disponible en: https://doi.org/10.53637/KAVV4291 [visitado el 16 de abril de 2021].

NEWSHUB (2021): "Facial Recognition Tecchnology should be Banned, EU Privacy Watchdog says". Disponible en: https://www.newshub.co.nz/home/technology/2021/04/facial-recognition-technology-should-be-banned-eu-privacy-watchdog-says.html2 [visitado el 26 de abril de 2021].

PI (2020): "How facial recognition is spreading in Italy: the case of Como". Disponible en: https://privacyinternational.org/case-study/4166/how-facial-recognition-spreading-italy-case-como [visitado el 09 de abril de 2021].

RAE (2021): "Definición de tecnología", en: Real Academia de la Lengua Española. Disponible en: https://dle.rae.es/tecnolog%C3%ADa [visitado el 08 de febrero de 2021].

REMOLINA, NELSON (2013): Tratamiento de Datos Personales : Aproximación Internacional y Comentarios a La Ley 1581 de 2012 (Bogotá, Ed. Legis).

REZENDE, ISADORA (2020): "Facial Recognition in Police Hands: Assessing the 'Clearview Case' from a European Perspective", en: New Journal of European Criminal Law (Vol. 11, Nº 3), pp. 375-389. Disponible en: https://doi.org/10.1177/2032284420948161 [visitado el 08 de febrero de 2021].

RED IBEROAMERICANA DE PROTECCIÓN DE DATOS (2019): "Recomendaciones Generales para el Tratamiento de Datos en la Inteligencia Artificial". Disponible en: https://www.redipd.org/es/noticias/la-ripd-aprueba-sendos-documentos-sobre-inteligencia-artificial-y-proteccion-de-datos [visitado el 16 de abril de 2021].

SOBEL, BENJAMIN (2020): "HiQ v. LinkedIn, Clearview AI, and a New Common Law of Web Scraping", en: SSRN Electronic Journal. Disponible en: https://doi.org/10.2139/ssrn.3581844 [visitado el 08 de febrero de 2021].

STATISTA (2022): "Global Biometrics System Market Revenue 2022". Disponible en: https://www.statista.com/statistics/1048705/worldwide-biometrics-market-revenue/ [visitado el 08 de febrero de 2021].

SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO (2018): "Concepto Radicación No. 18-171259 de 2018A". Disponible en: https://www.sic.gov.co/sites/default/files/normatividad/082018/Rad180171259TratamientoDatosSensibles.pdf [visitado el 10 de marzo de 2021].

ONU (2018): "Informe de La Relatora Especial Sobre Las Formas Contemporáneas de Racismo, Discriminación Racial, Xenofobia y Formas Conexas de Intolerancia". Disponible en: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N20/304/57/PDF/N2030457.pdf?OpenElement [visitado el 08 de febrero de 2021].

UE (2012): "Dictamen 3/2012 sobre la evolución de las tecnologías biométricas, Unión Europea". Disponible en: https://www.aepd.es/sites/default/files/2019-12/wp193_es.pdf [visitado el 08 de febrero de 2021].

UE (2018): "ICT Impact Assessment Guidlines, Practical tool and guidlines for assessing ICT implications". Disponible en: https://ec.europa.eu/isa2/sites/isa/files/leaflet_ict_impact_assessment_guidelines.pdf [visitado el 08 de febrero de 2021].

UE (2022): "Reclaim your Face". Disponible en: https://reclaimyourface.eu/ [visitado el 26 de abril de 2021].

UE (2022): "Data Protection Impact Assessment, GDPR.EU". Disponible en: https://gdpr.eu/data-protection-impact-assessment-template/ [visitado el 08 de febrero de 2021].

VIU (2017): "Los tipos de tecnología más representativos que debes conocer", en: Universidad Internacional de Valencia. Disponible en: https://www.universidadviu.com/es/actualidad/nuestros-expertos/los-tipos-de-tecnologia-mas-representativos-que-debes-conocer [visitado el 08 de febrero de 2021].

WILSON, STEPHEN (2017): "Blending the Practices of Privacy and Information Security to Navigate Contemporary Data Protection Challenges", en: Svantesson, Dan y Kloza, Dariusz (Eds.), Trans-Atlantic Data Privacy Relations as a Challenge for Democracy (Cambridge, Intersentia), pp. 379-390.

WONG, KELLY (2020): "The Face-ID Revolution: The Balance between Pro-Market and Pro-Consumer Biometric Privacy Regulation", en: Journal of High Technology Law (Nº 20), pp. 189-229

JURISPRUDENCIA CITADA

SENTENCIA T-303 de 1998, Corte Constitucional de Colombia, M.P. José Gregorio Hernández.

SENTENCIA T-257 de 2002, Corte Constitucional de Colombia, M.P. Marco Gerardo Monroy.

SENTENCIA T-729 de 2002, Corte Constitucional de Colombia, M.P. Eduardo Montealegre.

SENTENCIA C-748 de 2011, Corte Constitucional de Colombia, M.P Jorge Ignacio Pretelt.

SENTENCIA T-260 de 2012, Corte Constitucional de Colombia, M.P. Humberto Antonio Sierra.

SENTENCIA T-058 de 2013, Corte Constitucional de Colombia, M.P. Alexei Julio Estrada.

MARTINEZ NEAL V. SNAPCHAT, INC, N. 2:2016cv05182 (2016).

RESOLUCIÓN NO.43530 de 2018, Superintendencia de Industria y Comercio.

RESOLUCIÓN NO.92618 de 2018, Superintendencia de Industria y Comercio.

RESOLUCIÓN NO.29407 de 2018, Superintendencia de Industria y Comercio.

RESOLUCIÓN NO.55405 de 2018, Superintendencia de Industria y Comercio.

PATEL V. FACEBOOK, INC, N. 18-15982 (2019).

ROSENBACH V. SIX FLAGS ENTERTAINMENT, N. 123186 (2019).

RESOLUCIÓN NO.13622 de 2019, Superintendencia de Industria y Comercio.

RESOLUCIÓN NO.38281 de 2020, Superintendencia de Industria y Comercio.

RESOLUCIÓN NO.30412 de 2020, Superintendencia de Industria y Comercio.

RESOLUCIÓN NO.62132 de 2020, Superintendencia de Industria y Comercio.

RESOLUCIÓN NO.46344 de 2021, Superintendencia de Industria y Comercio.

NORMAS JURÍDICAS CITADAS

BIOMETRIC INFORMATION PRIVACY ACT (BIPA). General Assembly, 2008.

CALIFORNIA CONSUMER PRIVACY ACT (CCPA). Office of the Attorney General, California Department of Justice, 2018.

LEY Nº 1266 de 2008, por la cual se dictan las disposiciones generales del habeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones. Diario Oficial No. 47.219, 31 de diciembre de 2008.

LEY Nº 1581 de 2012, por la cual se dictan disposiciones generales para la protección de datos personales. Diario Oficial No. 48.587, 17 de octubre de 2012.

REGLAMENTO (UE) 2016/679, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE. 27 de abril de 2016.