UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE DERECHO

SEMINARIO DE DERECHO CONSTITUCIONAL

TESIS PARA OBTENER EL TÍTULO DE LICENCIADO EN DERECHO

“EL USO DE LOS SISTEMAS BIOMÉTRICOS COMO FORMA DE IDENTIFICACIÓN Y DE CONSENTIMIENTO PARA ACTOS JURÍDICOS“

PRESENTA

Roberto Valente Morales Lavin.

Asesor: Doctor Diego Armando Guerrero García.

Ciudad Universitaria, Agosto de 2023.

VNIVERSIDAD NACIONAL
AVTÓNOMA DE
MEXICO

FACULTAD DE DERECHO
SEMINARIO DE DERECHO CONSTITUCIONAL
OFICIO FDER/SDC/030/2023
ASUNTO: Aprobación de tesis

M. EN C. IVONNE RAMÍREZ WENCE
DIRECTORA GENERAL DE ADMINISTRACIÓN ESCOLAR
DE LA UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO
P r e s e n t e

Por este conducto le informo que ROBERTO VALENTE MORALES LAVIN, con número de cuenta 314213628, concluyó la tesis intitulada "EL USO DE LOS SISTEMAS BIOMÉTRICOS COMO FORMA DE IDENTIFICACIÓN Y DE CONSENTIMIENTO PARA ACTOS JURÍDICOS", bajo la asesoría del DR. DIEGO ARMANDO GUERRERO GARCÍA. Este trabajo de investigación demuestra la capacidad de su autor para aplicar los conocimientos adquiridos durante la Licenciatura en Derecho y cumple con los requisitos establecidos en la normativa universitaria, por lo que en términos de lo establecido en los artículos 18, 19, 20, 26 y 28 del Reglamento General de Exámenes y con fundamento en el artículo 10 del Reglamento para el Funcionamiento de los Seminarios de la Facultad de Derecho, se aprueba este trabajo de investigación para su presentación al jurado respectivo.

La persona interesada deberá iniciar el trámite para su titulación dentro de los seis meses siguientes (contados de día a día) a aquel en que le sea entregado el presente oficio, en el entendido de que transcurrido dicho lapso sin haberlo hecho, caducará la autorización que ahora se le concede para someter su tesis a examen profesional, misma autorización que no podrá otorgarse nuevamente, sino en el caso que el trabajo recepcional conserve su actualidad y siempre que la oportuna iniciación del trámite para la celebración del examen haya sido impedida por circunstancia grave, todo lo cual calificará la Secretaría General de la Facultad.

A t e n t a m e n t e
"POR MI RAZA HABLARÁ EL ESPÍRITU"
Ciudad Universitaria, Cd. Mx., a 4 de agosto de 2023

EL DIRECTOR DEL SEMINARIO

DR. RODRIGO BRITO MELGAREJO

FACULTAD DE DERECHO
SEM... DERECHO
...AMPARO

VNIVERSIDAD NACIONAL
AVPNOMA DE
MEXICO

FACULTAD DE DERECHO

DR. RODRIGO BRITO MELGAREJO
DIRECTOR DEL SEMINARIO DE DERECHO CONSTITUCIONAL
FACULTAD DE DERECHO
UNAM
P R E S E N T E

Distinguido Doctor Rodrigo Brito,

Con su autorización tuve el agrado de coordinar la elaboración del trabajo intitulado *"EL USO DE LOS SISTEMAS BIOMÉTRICOS COMO FORMA DE IDENTIFICACIÓN Y DE CONSENTIMIENTO PARA ACTOS JURÍDICOS"*, que como tesis recepcional elaboró el alumno ROBERTO VALENTE MORALES LAVIN con número de cuenta: 314213628.

El mencionado trabajo reúne las cualidades y características que una investigación de esta naturaleza debe tener. En tal virtud, me es muy grato hacer de su conocimiento que expido mi correspondiente aprobación para que esta tesis, una vez autorizada por usted, continúe con los trámites necesarios para lograr la titulación del sustentante.

Sin más por el momento, aprovecho la ocasión para enviarle un cordial saludo y la seguridad de mi mayor consideración y aprecio.

A T E N T A M E N T E
"POR MI RAZA HABLARÁ EL ESPÍRITU"
CIUDAD UNIVERSITARIA, A 2 DE AGOSTO DE 2023

DR. DIEGO A. GUERRERO GARCÍA.

Dedicatorias

A Nidiyare, Enrique y a mis hermanos Román y Camilo, les dedico este logro que espero lo hagan y sientan suyo, gracias por su apoyo incondicional en la vida.

A ustedes que iniciaron este camino conmigo y que desafortunadamente físicamente ya no me acompañan: José Roberto, Yeya y Rosa, que sin duda alguna fueron durante el proceso y en mi vida fuente de inspiración y deseo para superarme.

A mi gran maestro en la vida y de la profesión, Luis Ángel, deseando que disfrute esta meta y continué motivándome a seguir siempre adelante.

A Renata, quien me ha permitido estar a su lado en nuestro camino, que sin dudarlo me brinda su apoyo en todo y cada día me ha inspirado a ser mejor.

Agradecimientos

A mi familia, que cada uno de ustedes pusieron parte de su tiempo y cariño para que pueda ser la persona que forjaron.

Al Doctor Diego Armando Guerrero García, quien desde el inicio de mi carrera ha impulsado mi desarrollo como mejor profesionista y ser humano.

Agradezco a la Universidad que ha sido mi fuente de amistades, amor y conocimiento y que me ha permitido progresar.

Agradezco a los profesionistas y maestros que han aportado a mi formación académica y que confiaron en que podría realizar mis metas.

A la Dirección General de Asuntos del Personal Académico de la Universidad Nacional Autónoma de México.

ÍNDICE

I. CAPÍTULO I MARCO TEÓRICO CONCEPTUAL DE LOS SISTEMAS BIOMÉTRICOS 12

I.1. DE LOS SISTEMAS BIOMÉTRICOS 12

I.1.1. MARCO CONCEPTUAL INFORMÁTICO-JURÍDICO DE LOS SISTEMAS BIOMÉTRICOS 12

I.1.2. BASES DE DATOS 24

I.1.3. OBTENCIÓN DE DATOS BIOMÉTRICOS MEDIANTE DISPOSITIVOS ELECTRÓNICOS 27

I.1.4. EL ALMACENAMIENTO DE DATOS BIOMÉTRICOS. 28

I.2. TRATAMIENTO E IMPORTANCIA DE LOS DATOS BIOMÉTRICOS 33

I.3. DE LA IDENTIDAD 35

I.4. DEL CONSENTIMIENTO EN ACTOS JURÍDICOS 37

II. CAPÍTULO II DEL USO DE SISTEMAS BIOMÉTRICOS COMO FORMA DE IDENTIFICACIÓN Y CONSENTIMIENTO EN ACTOS JURÍDICOS 41

II.1. USO DE SISTEMAS BIOMÉTRICOS COMO FORMA DE IDENTIFICACIÓN DE LAS PERSONAS 41

II.1.1. DE LA IDENTIFICACIÓN POR EL USO DE SISTEMAS BIOMÉTRICOS ... 45

II.1.2. LOS SISTEMAS BIOMÉTRICOS Y LA IDENTIDAD 53

II.1.3. ALCANCE JURÍDICO DE LA IDENTIFICACIÓN POR SISTEMAS BIOMÉTRICOS 53

II.2. USO DE SISTEMAS BIOMÉTRICOS COMO FORMA DE CONSENTIMIENTO EN LOS ACTOS JURÍDICOS 61

II.2.2. CELEBRACIÓN DE ACTOS JURÍDICOS EN PLATAFORMAS DIGITALES 65

II.2.3. EL USO DE APLICACIONES Y SU ACCESO MEDIANTE SISTEMAS BIOMÉTRICOS 67

II.2.4. SERVICIOS DE CERTIFICACIÓN EN MÉXICO 85

II.2.5. DISPOSICIONES INTERNACIONALES EN MATERIA DE SISTEMAS BIOMÉTRICOS RESPECTO DEL CONSENTIMIENTO EN ACTOS JURÍDICOS. . 105

II.3. PROBLEMÁTICA DE LOS SISTEMAS BIOMÉTRICOS EQUIPARABLE AL CONSENTIMIENTO EXPRESO 110

III. CAPÍTULO III DE LA PROTECCIÓN DE DATOS PERSONALES Y BASES DE DATOS DE SISTEMAS BIOMÉTRICOS. 115

III.1. LOS SISTEMAS BIOMÉTRICOS, USO Y DISPOSICIÓN EN BASES DE DATOS 115

III.2. TRATAMIENTO DE LOS SISTEMAS BIOMÉTRICOS COMO DATOS PERSONALES SENSIBLES 125
III.2.1. POSESIÓN Y USO DE BASES DE DATOS CON SISTEMAS BIOMÉTRICOS..... 139
III.2.2. EL VALOR COMERCIAL DE LOS DATOS PERSONALES 152
III.3. REGISTRO NACIONAL DE USUARIOS DE TELEFONÍA MÓVIL 154
IV. CAPÍTULO IV DE LAS PROBLEMÁTICAS DEL USO DE SISTEMAS BIOMÉTRICOS..... 163
IV.1. LA INSEGURIDAD JURÍDICA DEL USO DE SISTEMAS BIOMÉTRICOS COMO FORMA DE IDENTIDAD Y DE CONSENTIMIENTO PARA ACTOS JURÍDICOS 163
IV.2. EL SISTEMA JURÍDICO MEXICANO FRENTE A LOS SISTEMAS BIOMÉTRICOS 170
IV.2.1. LA VALIDACIÓN Y ALCANCE JURÍDICO DE LA IDENTIFICACIÓN A TRAVÉS DE LOS SISTEMAS BIOMÉTRICOS..... 170
IV.2.2. USURPACIÓN DE IDENTIDAD POR MEDIOS ELECTRÓNICOS 173
IV.2.3. ROBO DE LOS DATOS Y SISTEMAS BIOMÉTRICOS DE LA PERSONA 186
IV.3. PROTECCIÓN Y SEGURIDAD INFORMÁTICA DE LOS DATOS 191
IV.4. PANORAMA PROGRESIVO DE LOS SISTEMAS BIOMÉTRICOS COMO FORMA DE IDENTIFICARSE Y DE OTORGAR CONSENTIMIENTO EN ACTOS JURÍDICOS..... 198
IV.4.1. LAS BASES DE DATOS SENSIBLES Y SU INTEGRACIÓN DE SISTEMAS BIOMÉTRICOS..... 199
IV.4.2. CIBERSEGURIDAD PARA ACTOS JURÍDICOS CELEBRADOS POR MEDIOS ELECTRÓNICOS..... 201
IV.4.3. LA VALIDACIÓN DE LOS SISTEMAS BIOMÉTRICOS 206
IV.5. LA IMPORTANCIA DE LA INFORMACIÓN BIOMÉTRICA Y SU CUIDADO 212
V. CONCLUSIONES 217
VI. FUENTES 231
VI.1. BIBLIOGRAFÍA..... 231
VI.2. JURISPRUDENCIA 236
VI.3. HEMEROGRAFÍA..... 237

INTRODUCCIÓN

Derivado del acelerado avance de la tecnología y el uso cotidiano de los sistemas biométricos como forma de identificar a las personas y otorgar su consentimiento en los actos jurídicos celebrados por medios electrónicos, la legislación mexicana se ha visto superada, por lo que se han generado vacíos legales, propiciando un estado de incertidumbre jurídica y problemas derivados a los usuarios y titulares de estos datos biométricos, surgiendo la necesidad de legislar y aplicar las medidas y mecanismos de seguridad novedosas para proteger y adaptarse a los grandes cambios tecnológicos que están al alcance de las personas.

Con los avances en la tecnología y la fácil accesibilidad de medios electrónicos para la celebración de actos jurídicos y como forma de identificación, es indiscutible la necesidad de crear sistemas y mecanismos funcionales jurídicos que estén a la par de las prioridades de la población y de su realidad, los cuales en México no se han creado. En virtud del uso de la técnica de investigación legislativa en conjunto con la exploratoria y de cierto modo predictiva, este trabajo de investigación parte el estudio de las disposiciones relativas al uso de sistemas biométricos para la celebración de actos jurídicos, así como lo relativo a datos personales.

Utilizando el método de investigación deductivo, se parte de la premisa que existe un uso acelerado y cada día más común de los datos biométricos como una forma de identificación de las personas y como forma de consentir actos jurídicos, circunstancias que son observaciones reales que permiten dar a conocer las problemáticas generales, las cuales no pueden quedarse atrás y que deberán ser atendidas antes de lo que se espera.

Uno de estos problemas es la necesidad de regular dentro del sistema jurídico mexicano el uso progresivo de las tecnologías de la información en relación al uso de los datos biométricos, y otro tema es la progresividad en la defensa de los derechos humanos aplicables a su uso.

En esta tesitura, ambos temas deben considerarse como un binomio que conforme a la progresividad de los derechos humanos deben seguir un mismo camino de avance y protección, tomando siempre como consideración el hecho que el uso de sistemas biométricos se ha vuelto cada vez más cotidiano derivado de tener dispositivos móviles con lectores de diversos datos biométricos al alcance, en consecuencia se debe tener como común denominador que su uso provocará que la norma imperativa deba adecuarse a nuevas exigencias.

Partiendo desde un primer panorama y empleando la técnica de investigación legislativa y como método cualitativo conviene precisar desde este momento que dentro del sistema jurídico podrían existir diversos preceptos que de cierto modo podría considerarse que satisfacen el problema del vacío normativo en torno al uso de datos biométricos como forma de identificación y de consentimiento para actos jurídicos, como se expone en los siguientes párrafos.

Conforme a la fracción I del artículo 1803 del Código Civil Federal: “el uso de medios electrónicos, ópticos y de cualquier otra tecnología se equipara al consentimiento expreso, por lo que al utilizar estas tecnologías, surten los mismos efectos legales”,[1] no obstante lo anterior, se logra advertir que existe un vacío jurídico en virtud que los sistemas biométricos deben tener un tratamiento específico en los citados supuestos especificados en legislación, como se precisará en este trabajo, y que se debe tomar en consideración que el procesamiento de datos biométricos tecnológicamente implican el uso de sistemas más avanzados e involucran el manejo de datos personales.

De la misma forma el artículo 52 de la Ley de Instituciones de Crédito añade a lo expuesto en el párrafo anterior: “la posibilidad de celebrar con el uso de equipos,

[1] *Cfr.* artículo 1803 del Código Civil Federal.
El consentimiento puede ser expreso o tácito, para ello se estará a lo siguiente:
I.- Será expreso cuando la voluntad se manifiesta verbalmente, por escrito, por medios electrónicos, ópticos o por cualquier otra tecnología, o por signos inequívocos, y;
II.- El tácito resultará de hechos o de actos que lo presupongan o que autoricen a presumirlo, excepto en los casos en que por ley o por convenio la voluntad deba manifestarse expresamente.

medios electrónicos, ópticos o de cualquier otra tecnología, sistemas automatizados de procesamiento de datos y redes de telecomunicaciones, ya sean privados o públicos",[2] por lo que se advierte del citado precepto normativo que la naturaleza jurídica de la forma de otorgar consentimiento podrá hacerse en sustitución de la firma autógrafa, y tendrá los mismos efectos jurídicos.

Confrontando lo mencionado en el párrafo anterior, existe una colisión con lo dispuesto en los artículos 92, 101, 104 y 105 todos de la Ley General de Población, toda vez que, conforme a lo relativo al Registro Nacional de Población, el cual sirve para coordinar los métodos de identificación, así como los procedimientos de identificación personal, deriva en una contradicción y resulta en que no se tiene certeza de que la autoridad efectivamente cumpla con la obligación de verificar y proteger los datos de identidad de los titulares en la Cédula de Identidad Ciudadana que los citados preceptos establecen, tópico que será abordado en el aspecto dialéctico por lo que hace a los datos biométricos como datos personales sensibles, se advierte la existencia de una discrepancia normativa y como se estudiará la cédula referida a pesar de estar contemplada normativamente en la realidad no se utiliza, dejando al gobernado en un estado de incertidumbre jurídica.

Por lo que respecta al uso de sistemas biométricos para la identificación, y con relación a los párrafos anteriores del Reglamento de la Ley General de Población, se tiene lo siguiente: primero, el artículo 42 establece que: "corresponde únicamente al Registro Nacional de Población emplear los métodos de identificación y registro de las personas",[3] lo cual colisiona con lo antes mencionado de la Ley General de

---

[2] *Cfr.* artículo 52 de la Ley de Instituciones de Crédito.
Las instituciones de crédito podrán pactar la celebración de sus operaciones y la prestación de servicios con el público mediante el uso de equipos, medios electrónicos, ópticos o de cualquier otra tecnología, sistemas automatizados de procesamiento de datos y redes de telecomunicaciones, ya sean privados o públicos, y establecerán en los contratos respectivos las bases para determinar lo siguiente: […]

[3] *Cfr.* artículo 42 del Reglamento de la Ley General de Población.
El Registro Nacional de Población coordinará los métodos de identificación y registro de personas de la Administración Pública Federal y de las administraciones públicas estatales y municipales en los términos de los instrumentos que se celebren al respecto, con el propósito de constituir un sistema integrado de registro de población.

Instituciones de Crédito; segundo, el inciso i) del artículo 47 del precitado Reglamento ordena que el Registro Nacional de Ciudadanos debería tener cuando menos: “fotografía, huellas dactilares, imagen del iris y firma del ciudadano, como datos de las personas”,[4] la ley en cita deja de ser obligatoria y se convierte en opcional respecto de contar con dos datos biométricos para la identificación de personas como son las huellas dactilares e imagen del iris, y como se abordará el referido registro a pesar de estar previsto en las hipótesis normativas no cobra aplicación en el plano fáctico.

Ante la falta de normatividad jurídica, así como la incongruencia e insuficiencia de la existente, el operador jurídico y legislador necesitan de un método interpretativo e imperativo de legislación para hacer frente a la realidad, porque el uso desmedido sin regulación específica aplicable al caso concreto ha generado incertidumbre jurídica para las personas, aunado a que tratándose de materia de ciberseguridad y suplantación de identidad y demás delitos informáticos deben verse a la luz las deficiencias normativas respecto del uso de sistemas biométricos como una forma de equipararse a un consentimiento expreso y de identidad plena de las personas.

Hasta la fecha no se ha legislado para añadir o reformar disposiciones para brindar el estado de derecho y seguridad jurídica que se requiere para la celebración de actos jurídicos y que en consecuencia exista forma de exigir el cumplimiento de una obligación derivado su celebración, todo lo anterior, del uso de los datos biométricos, tampoco existe la certeza, seguridad y protección de identidad de las personas.

---

[4] *Cfr.* artículo 47 del Reglamento de la Ley General de Población.
El Registro Nacional de Ciudadanos se conforma con los datos de los mexicanos y mexicanas de dieciocho o más años, los cuales deberán ser, cuando menos, los siguientes: a) Nombre completo; b) Sexo del ciudadano; c) Lugar y fecha de nacimiento; d) Lugar y fecha en que se llevó a cabo la inscripción de la persona al Registro Nacional de Ciudadanos; e) Nombre completo y nacionalidad del padre y la madre cuando se consignen en los documentos presentados; f) Datos de localización del acta de nacimiento en el Registro Civil, o del certificado de nacionalidad, o de la carta de naturalización; g) Nacionalidad de origen cuando el ciudadano haya adquirido la nacionalidad por naturalización; h) Clave Única de Registro de Población, y i) Fotografía, huellas dactilares, imagen del iris y firma del ciudadano.

Por cuestiones de metodología, la investigación se deriva en dos vertientes torales del uso de la biometría de los individuos: la primera, en relación con su uso como forma de identificación, que aborda tópicos del derecho de las personas a la identidad, nombre, protección de datos personales, y derecho a la intimidad, todos reconocidos en la Constitución Política de los Estados Unidos Mexicanos, y; segundo, la vertiente de su uso como una aducida e inducida forma de otorgar el consentimiento para la celebración de actos jurídicos, en específico su uso como una artificiosa equivalencia a una firma electrónica, ya sea avanzada o no.

En el mismo tenor y empleando el método de investigación inductivo, se tiene que el uso de los datos biométricos como forma de identidad y de consentimiento para actos jurídicos ha sido un tema poco explorado en el ámbito del Poder Judicial de la Federación, en específico de las sentencias que han tratado o intentado abordar el tema.

Se parte de lo anterior porque se realizó una búsqueda de sentencias en la plataforma del buscador de sentencias en versión pública del Consejo de la Judicatura Federal, en el cual se partió de ingresar como campo de búsqueda la palabra biométrico como frase exacta, en índice temático, a lo cual se arrojó la cantidad de 133 sentencias en versión pública que abordan alguna cuestión sobre el tema de datos biométricos de un total de 7,457,826 sentencias disponibles, con lo cual se vislumbra que es un tópico de cierto modo poco aplicado por los Juzgados y Tribunales del Poder Judicial de la Federación, aunado a que la mayoría son relacionadas al Registro Nacional de Usuarios de Telefonía Móvil con motivo de las reformas y adiciones a diversas disposiciones de la Ley Federal de Telecomunicaciones y Radiodifusión, publicado el 16 de abril de 2021 en el Diario Oficial de la Federación, con lo cual no se atiende a la problemática del vacío legal que se plantea. Aunado a que se considera no existe jurisprudencia como fuente del derecho que permita resolver la problemática que se plantea, se tomarán en consideración las resoluciones emitidas por el Instituto Nacional de Transparencia,

Acceso a la Información y Protección de Datos Personales, en lo relacionado a lo que interesa en este trabajo de investigación.

Por otra parte, también se abordará la problemática empleando el método comparado, pues a lo largo de la investigación se realizan diversas referencias a legislaciones tanto nacionales, en relación a delitos como usurpación de identidad, e internacionales.

De lo anterior, surge la idea de realizar la presente investigación, de tal suerte que se pueda evaluar la viabilidad de proponer diversas disposiciones del sistema jurídico mexicano para brindar certeza y protección jurídica a quienes utilizan los sistemas biométricos en la celebración de actos jurídicos para otorgar su consentimiento y a quienes los utilizan como forma de identificase.

I. CAPÍTULO I MARCO TEÓRICO CONCEPTUAL DE LOS SISTEMAS BIOMÉTRICOS

I.1. DE LOS SISTEMAS BIOMÉTRICOS

El presente capítulo tiene como objetivo sentar las bases conceptuales y técnicas de la presente investigación, partiendo del método analítico, sin pretender exponer el todo en relación a los datos biométricos porque es un tema bastante amplio y que sería imposible ser abordado en un trabajo de esta naturaleza, por lo que se hará el enfoque primordial en las partes que importan e interesan a la investigación y al ser un tema técnico-jurídico, se deja en claro que existe una complejidad para aplicar en el campo del derecho cuestiones de índole de la ciencia informática, requiriendo de un nuevo paradigma para el operador del derecho, esto es, el perfil de un abogado digital, el cual debe no sólo enfocarse en el ámbito del derecho sino también en entender cómo funcionan los diversos sistemas tecnológicos y así encontrar los retos que implican para poder aplicar el conocimiento jurídico a la solución de los problemas derivados de su uso.

I.1.1. MARCO CONCEPTUAL INFORMÁTICO-JURÍDICO DE LOS SISTEMAS BIOMÉTRICOS

Los sistemas biométricos son el resultado de un proceso tecnológico en los que el ser humano se ve en la necesidad de adecuarse, conforme al enorme y constante proceso tecnológico y su uso en las actividades que desarrolla cotidianamente, circunstancia que se ha acelerado en los últimos años con la innovación de nuevas tecnologías que se ponen al alcance de la mayoría de la población, ejemplo de ello, son los dispositivos electrónicos móviles que implementan entre sus funciones los lectores de huellas digitales, reconocimiento facial y de voz, entre otros, los cuales hacen que en general la sociedad disponga fácilmente del uso los sistemas biométricos cotidianamente.

Para comenzar, a través del método fenomenológico se tiene la premisa que en más de una ocasión se ha observado que personas en diversos lugares como:

bancos, oficinas, hospitales, instituciones gubernamentales, para ingresar a su fuente de trabajo o para la realización de listas de asistencia, o como forma de identificarse frente a un grupo, utilizando sus datos biométricos.

Para lo cual se aproximan a un dispositivo electrónico que en cuestión de segundos les brinda o niega acceso, les identifica, autentica o en su caso pide aproximar de nuevo su huella dactilar, mano, rostro al dispositivo o hablar, para consolidar un sistema automatizado, estos dispositivos electrónicos son cada día más usados y emplean todos estos elementos que son inherentes a la naturaleza del ser humano los cuales permiten hacerlos únicos por sus caracteres especiales biológicos se pueden denominar a grandes rasgos como sistemas biométricos.

Para la delimitación conceptual de los sistemas biométricos se vuelve necesario realizarlo desde un enfoque multidisciplinario, toda vez que se involucran diversas disciplinas de la ciencia para su estudio, innovación e implementación cotidiana para su uso por sociedad en general.

De acuerdo con Cuauhtémoc Vélez Martínez, quien cita al Subcomité en Biometría perteneciente al Consejo Nacional de Ciencia y Tecnología de los Estados Unidos, la biometría es un término que tiene dos enfoques principales, como se precisa en los términos siguientes:

> Primero, para describir una característica como una medición biológica (anotómica o fisiológica) o de conducta, empleadas para realizar un reconocimiento automatizado; segundo, como proceso de reconocimiento de un individuo basado en características biológicas y conductuales que sean medibles, es decir, consiste en la medición de ciertas características biológicas o de comportamiento que poseen todas las personas, pero que son únicas e irrepetibles en cada una de ellas, todo esto con el fin de llevar a cabo un proceso de reconocimiento comprobado así, que la persona es quien dice ser. La biometría se divide fundamentalmente en dos tipos; fisiológica (se nace con ella)

como la huella dactilar, el rostro, la mano, el iris, la retina o los labios; y la conductual (se adquiere) como la forma en que un usuario teclea, la velocidad en que firma o la manera en que camina.[5]

Conforme a lo precisado son las ramas de la ingeniería informática y la biometría las que sirven para la delimitación conceptual de los sistemas biométricos, al respecto interesa resaltar tres puntos fundamentales de la definición precitada en el párrafo anterior:

Primero, como aquel proceso de reconocimiento automatizado de una persona;

Segundo, como la característica de emplear rasgos tanto fisiológicos como conductuales que distinguen o hacen diferente a una persona de todas las demás, y;

Tercero, como la medición de los rasgos mencionados y su captación por dispositivos electrónicos.

Estos puntos son resaltados por la importancia que tienen para este trabajo de investigación, porque delimitan el camino que siguen los rasgos físicos que se captan por los dispositivos de reconocimiento, para que posteriormente se haga el ejercicio comparativo automatizado de verificación o autenticación, es decir, establecer que es la persona quien dice ser, y dan como resultado que se distinga una persona del resto de las personas, por medio de características biológicas únicas de cada individuo, esto último, por ser útil para la celebración de actos jurídicos a través de dispositivos electrónicos y ser un rubro toral en la identificación de las personas.

[5] *Cfr.* VÉLEZ MARTÍNEZ, Cuauhtémoc, *Dispositivos Biométricos,* México, Instituto de Ingeniera de la Universidad Nacional Autónoma de México, núm. 11, disponible en: <http://www.ii.unam.mx/es-mx/AlmacenDigital/CapsulasTI/Paginas/dispositivosbiometricos.aspx> [Consulta: 08-agosto-2021].

Continuando con lo anterior, en este capítulo se realizará un estudio de los principales y más usados sistemas biométricos, entre ellos; los sistemas de biometría fisiológica: huella dactilar, iris, retina o geometría de la mano, sistemas de autenticación de patrones vasculares o características faciales; y los sistemas derivados de la biometría conductual o de comportamiento como: dinámica de firma, ritmo o forma de escritura o forma de caminar.

I.1.1.1. Biometría fisiológica

La biometría fisiológica abarca todo lo relacionado a la medición de características biológicas que son únicas en cada individuo, tales como: la huella dactilar, el rostro, la mano, el iris, la retina.

De estos se advierte que la característica principal es que son inalterables de forma fácil, por considerarse como inherentes a la persona y que todas las personas cuentan con estas características, salvo contables excepciones por accidentes y problemas de salud, de igual forma, se caracterizan por ser patrones únicos que hacen diferente a una persona del resto, por lo que si son medibles pueden ser considerados como potenciales formas para identificar a las personas.

I.1.1.1.1. Huella dactilar

La dactiloscopia es la ciencia que se encarga del estudio de las huellas dactilares, y conforme a la investigadora de la Universidad Nacional Autónoma de México, Isabel Pérez, puede definirse como: “El estudio de la forma, disposición, registro y clasificación de las crestas papilares que se encuentran en la extremidad de la yema de los dedos de la mano. Se trata del método identificativo por excelencia debido a sus tres principios: perennidad, inmutabilidad y diversiformidad.”[6]

[6] PÉREZ, Isabel, *Avances en la identificación de las personas mediante las huellas dactilares,* México, Universidad Nacional Autónoma de México, 11 de mayo del 2020, disponible en: <http://ciencia.unam.mx/leer/994/avances-en-la-identificacion-de-personas-mediante-las-huellas-dactilares> [Consulta: 08-agosto-2021].

En el mismo orden de ideas, la investigadora precitada señala tres principios por los que se rige la dactiloscopia:

> Primero, el principio de perennidad, que sostiene que las denominadas crestas del dibujo dactilar se observan a partir de la sexta semana de vida intrauterina y participan en el crecimiento de la persona hasta su muerte y su putrefacción o momificación; segundo, el principio de inmutabilidad, es decir, que las huellas no cambian; tercero, el principio de la diversiformidad de las huellas se refiere a todos los seres humanos poseen un sistema decadactilar individual y con características únicas, esto por la diversidad de formas que tienen estos dibujos papilares, en los que jamás podrán hallarse dos iguales, podemos denominarlos diversiformes.[7]

Con relación a la investigación es dable afirmar que la huella dactilar por sus características y conforme a los principios de la dactiloscopia, es una característica biológica que puede obtenerse de la yema de los dedos de la mano, compuesta por surcos y crestas papilares, que son únicas para cada ser humano, que no cambian por el tiempo, y que prevalecen en la persona desde la sexta semana de gestación hasta la muerte y en consecuencia por la inalterabilidad son únicos e irrepetibles en cada ser humano, por lo que si son medibles y comparables son un medio para identificar a las personas.

En el mismo sentido, es importante decir que para que estas huellas dactilares sean medibles es necesario, como señala el Maestro Israel Estrada Camacho:

> Se cubran ciertos requisitos para que esta medición sea útil para identificar a una persona, estableciendo cuatro requisitos para ello:

[7] *Ibidem.*

- Idoneidad: Los calcos papilares deben ser idóneos, lo que significa que deben poseer condiciones suficientes de nitidez e integridad.
- Similitud: Los papilogramas a confrontar deben corresponder a una misma área papilar.
- Cantidad suficiente de puntos: de exigencia técnica para expedir una conclusión categórica e indudable por parte del perito está fijada por un parámetro de 12 a 15 puntos característicos.
- Calidad: los puntos determinados en número suficiente deben guardar requisitos de calidad: exacta ubicación, situación y dirección.[8]

Por último, es importante mencionar que de los sistemas informáticos a través de los cuales se obtienen la medición de estas características de las huellas dactilares actualmente cuentan con sistemas o programas que mediante bases de datos procesan las huellas dactilares electrónicamente almacenadas con información dactilar, utilizando los puntos de característicos, surcos y crestas papilares de cada persona que se obtienen con el sólo hecho de colocar su dedo en la placa de vidrio de un lector óptico, y que con un sistema automatizado realiza el comparativo con el dato almacenado en la base de datos y corrobora la similitud.

I.1.1.1.2. Geometría de la mano

La geometría de la mano, puede definirse como la forma de la mano, como lo advierten César Tolosa Borja y Álvaro Giz Bueno:

> A diferencia de las huellas dactilares, la mano humana no es única, y sus características individuales no son suficientes para identificar a una persona. Sin embargo, su perfil resulta útil si el sistema biométrico lo combina con imágenes individuales de algunos dedos, extrayendo datos como las

[8] ESTRADA CAMACHO, Israel, *Huella genética vs. Huella dactilar,* México, Procuraduría General de la República, 2014, pp. 5 y 6, disponible en: <https://biblat.unam.mx/hevila/Archivosdecriminologiaseguridadprivadaycriminalistica/2015/vol4/6.pdf> [Consulta:10-agosto-2021].

longitudes, anchuras, alturas, posiciones relativas y articulaciones. Estas características se transforman en una serie de patrones numéricos que pueden ser comparados.[9]

De lo anterior se desprende que se trata de un sistema biométrico que comparado con otros es de menor precisión pero de más rápido procesamiento, toda vez que es un sistema parecido con el de huella dactilar, pero que este involucran una toma de muestra completa de la mano, es decir, que no se limita exclusivamente a la yema de un dedo.

Por lo que esta geometría de mano y sus mediciones se almacenan en una base de datos con las imágenes previamente capturadas de la persona y se comparan con las que se tienen al momento sobre el lector o vidrio, para corroborar que se trata de la misma imagen y por ende del mismo sujeto, con las desventajas que se deben considerar como son los aspectos individuales y accidentales, tales como lesiones en los dedos o cortaduras para el momento de esta comparativa, distorsiones en la geometría de la mano por fracturas o amputaciones, así como la suciedad almacenada en la mano.

I.1.1.1.3. Iris y retina

El ojo humano, es considerado por diversos autores como un elemento biológico del ser humano por medio del cual se puede hacer identificable a una persona, pero el ojo humano es un concepto amplio que no toda su composición anatómica sirve para la presente investigación, por lo que este estudio se centrará en el análisis del iris y de la retina que son partes de ojo por ser útiles para los sistemas biométricos como la característica biológica por la cual se puede hacer única a una persona.

En esta tesitura, es indispensable el apoyo de la rama de la anatomía para entender el sustento de este sistema biométrico, en este efecto se cita a César

[9] TOLOSA BORJA, César y Álvaro Giz de Bueno, *Sistemas biométricos,* México, p. 21, disponible en:<https://www.dsi.uclm.es/personal/MiguelFGraciani/mikicurri/Docencia/Bioinformatica/web_BIO/Documentacion/Trabajos/Biometria/Trabajo%20Biometria.pdf > [Consulta: 02-septiembre-2022].

Tolosa Borja y Álvaro Giz Bueno, en relación con el iris del ojo humano nos dicen que:

> Se trata de la estructura indivisible del cuerpo humano más distintiva matemáticamente. En sus 11 milímetros de diámetro cada iris concentra más de 400 características que pueden ser usadas para identificar a su propietario (criptas, surcos, anillos, fosos, pecas, corona en zig-zag). Cuenta con un número de puntos distintivos 6 veces superior al de una huella dactilar. Hay que tener en cuenta que el iris no cambia a lo largo de la vida, y que sus patrones no están determinados genéticamente, por lo que incluso el ojo izquierdo y el derecho de un mismo individuo son diferentes.[10]

Respecto de la retina se señala que, conforme a los autores antes mencionados: "La retina es la capa más interna de las tres capas del globo ocular. Es el tejido sensible a la luz (fotorreceptor) que se encuentra en la parte posterior interna del ojo. Los sistemas basados en las características de la retina analizan la capa de vasos sanguíneos localizados en la parte posterior del ojo."[11]

Concluyendo que para el funcionamiento del escaneo de la retina y del iris debe existir de cierto modo un contacto directo con el lector, por lo que se concluye que estos sistemas biométricos son considerados mecanismos intrusivos, es decir, que tiene que existir un contacto directo con las personas, específicamente del ojo de la persona a identificar, de tal forma que puedan obtenerse un escaneo o imagen detectando los puntos distintivos del iris o de la retina para que se puedan comparar con los escaneos o imágenes que previamente se obtuvieron y que se encuentran almacenados en la base de datos.

I.1.1.1.4. Reconocimiento facial

[10] *Ibidem.* p. 20.
[11] *Ibidem.* p. 23.

El reconocimiento facial consiste en un sistema que permite comparar la imagen del rostro de una persona, es decir, como si tratase de una fotografía, en conjunto con rasgos característicos, medias del ancho y largo de la cara, así como localización de las orejas, nariz, labios, ojos, cejas y demás rasgos biológicos que permitan a una persona compararse del resto, y esta imagen se almacena en una base de datos y se permite compararla con la imagen que se vaya a identificar, en términos de César Tolosa Borja y Álvaro Giz Bueno:

> El funcionamiento a lo largo del tiempo y gracias al avance tecnológico ha evolucionado; en un primer momento, se realizaba a través de una imagen obtenida directamente de la persona, por medio de una imagen real o bidimensional, como una fotografía, automáticamente el sistema determinaba la alineación y medias del rostro por los denominados puntos duros de la cara, basado en la posición de la nariz, boca y ojos, posteriormente, el sistema previas plantillas las traducía en códigos numéricos a modo de poder ser comparadas con otras plantillas y así encontrar la similitudes de las previamente guardadas; en un segundo momento, los sistemas biométricos empezaron a utilizar imágenes tridimensionales, pudiéndose considerar sistemas más precisos, el funcionamiento de estos es similar a los de imágenes bidimensionales, con la distinción que el sistema crea nodos para que se cree un mapa de la cara de la persona en tres dimensiones, y se miden las distancias entre los puntos o nodos que se determinen en el programa, el beneficio que se sumó este sistema de imagen tridimensional es que estos a comparación se tiene la capacidad de reconocimiento hasta en una imagen de rostro girada 90 grados, además ya consideran la variante de la iluminación y las diferentes expresiones faciales que pudiera tener el individuo.[12]

Aunado a que los mismos autores citados, establecen que:

[12] *Cfr., Ibidem*, p. 22.

El punto medular de este sistema biométrico es el derivado de la capacidad de procesar e identificar los nodos o puntos duros del rostro del ser humano, es decir, el poder distinguir de los fondos y relieves de la cara, y medir la distancia y profundidad de estos, y la comparativa que se hace respecto de los datos ya previamente obtenidos en las bases de datos del sistema, los autores citados en el párrafo anterior establecen que hay aproximadamente 80 nodos en un rostro de los que el sistema hace uso (entre ellos se incluye el largo de la línea de la mandíbula, la profundidad de los ojos, la distancia entre los ojos, la forma del pómulo, la anchura de la nariz).[13]

Por lo que se concluye que estos constituyen el sostén informático-biológico que hacen identificable a una persona por las características de su rostro.

I.1.1.2. Biometría conductual

En el presente apartado se abarcarán los patrones de conducta que son medibles y que hacen que una persona pueda distinguirse del resto.

Actualmente por su confiabilidad, comparado con las biometrías biológicas o fisiológicas es poco usual el escuchar de su aplicabilidad y su uso, pero empleando el método fenomenológico y predictivo en un pensamiento futurista y progresivo estos podrían estar más próximos a utilizarse.

De la biometría conductual se desprenden todos los patrones relativos a las actividades de las acciones de las personas, por ejemplo: de la firma, el ritmo o forma de escritura o la forma de caminar, estos son todos aquellos hábitos de comportamiento que tienen las personas y que pueden ser medibles, actualmente se observan algunos de estos principalmente empleados en el registro de actividades deportivas, tal como el uso de relojes inteligentes que permiten la medición de actividades cotidianas, como: el control del sueño, número de pasos,

[13] *Idem.*

escalones subidos o bajados en un día, horario de comida, saturación en la sangre, ritmo cardiaco dependiendo de la hora del día o actividad.

El uso de dispositivos móviles permiten una mayor captación de estos biométricos conductuales, mismos que cada día son más utilizados, como el estilo de tecleo de un celular, deslizamientos o toques de la pantalla táctil, movimientos de los dedos en el dispositivo móvil, la forma en que se sujeta o mueve el dispositivo en uso o en modo espera, los cuales son rasgos de conducta que se pueden medir a lo largo de horas y días, y que son datos que se recaban y almacenan de forma automática para brindar una mejor interacción con el usuario y hacen la vida más sencilla o cómoda, por ejemplo una escritura más fácil con el uso del corrector automático de textos o de predicción de palabras, apertura de cámara con movimiento del móvil sin necesidad de desbloquear el dispositivo, accesos rápidos a aplicaciones, sugerencias de actividad, todo esto genera un perfil biométrico conductual.

El punto de investigación de estos biométricos conductuales es por el inminente desarrollo de las tecnologías y su inclusión en la vida cotidiana, aunado al uso de dispositivos que permiten su medición y captación en bases de datos que se generan para brindar una mejor experiencia de uso al operador.

Lo que se debate es aquí su fiabilidad, toda vez que se debe tomar en cuenta el rango o porcentaje de fallo el identificar a una persona, porque razonablemente se entiende que la conducta y comportamiento humano son únicos y cambiantes en cada ser humano.

Pero que incluso en ciertos grupos de personas podría ser idénticos o similares pero pueden cambiar en todo momento, entonces lo cuestionable es el parámetro de su medición a la que indiscutiblemente afectan factores imprevistos o poco previsibles al comportamiento. Si bien es cierto que, existen hábitos y patrones que repetimos diario o con relación a ciertas actividades, también lo cierto es que, cada

humano y su actuar pueden ser modificados por diversas causas tanto internas como externas.

De este modo se concluye que los datos biométricos conductuales no serían aptos para distinguir de forma fehaciente a un individuo del resto, pero para objeto de este trabajo era necesario dedicarle un apartado pensando en su futura aplicación.

I.1.1.3. Funcionamiento general de los sistemas biométricos

Para Cuauhtémoc Vélez Martínez en términos generales los sistemas biométricos funcionan de la siguiente forma:

> El primer paso es el denominado registro (*enrollment*) donde el dispositivo toma muestras de las características biológicas del usuario; posteriormente el sistema las convierte en una plantilla (*template*) y la almacena en una base de datos (no necesariamente como imagen sino como una representación de ésta); el siguiente paso es la identificación o "uno a muchos" donde el sistema biométrico identifica a la persona del resto de la población que ha sido registrada; y el último paso es la autenticación o "uno a uno". Aquí, el sistema hace coincidir la identidad de la persona con su biometría, complementando en ocasiones este proceso, con el uso de otras tecnologías como contraseñas, número de identificación personal o tarjetas.[14]

La aplicación de lo definido anteriormente radica en que se permita la medición de las características biológicas y su utilidad para identificación y acreditación de consentimiento de las personas, es por ello que se debe establecer que los sistemas biométricos de identidad y autenticación se componen de un *hardware* y un *software*, en palabras del Maestro Israel Estrada Camacho:

[14] *Op. cit.,* VÉLEZ MARTÍNEZ, Cuauhtémoc, *Dispositivos Biométricos,* número 11.

> El primero enunciado captura la característica biométricos concreta del individuo y el segundo realiza el sistema automatizado de interpretación y procesamiento de la información y determina su aceptabilidad o rechazo dentro del proceso automatizado de comparación, todo en función de los datos que han sido almacenados por medio de un registro inicial de la característica biométrica que mide el dispositivo en cuestión. La capacidad de este registro inicial o toma de muestra es lo que determina la eficacia del sistema, es decir, la capacidad del *hardware*, y después, el programa guarda la información como un modelo; la próxima vez que ese usuario intente acceder al sistema deberá repetir la operación y el software verificará que los datos corresponden con el modelo. [15]

Del funcionamiento de los sistemas biométricos se advierten dos aspectos por lo que hace a la exactitud en la verificación de la característica almacenada y la muestra que se pretende comparar: primeramente dependen del cambio que se puede producir en las personas, dependiendo conforme características físicas que se trate, producto de accidentes, raspaduras, amputaciones o naturalmente al envejecimiento de las personas; y en un segundo aspecto dependen de las condiciones ambientales en donde se tomen las muestras, condiciones que afectan a las características biológicas como la humedad en el aire, presencia de suciedad de la parte que se realiza la toma de muestra, así como capacidad de procesamiento en la captura y uso del dato almacenado, elementos que sin lugar a dudas limitan la fiabilidad, así como precisión de los mecanismos utilizados, cuestiones que en todo momento deben ser consideradas.

I.1.2. BASES DE DATOS

Una vez expuestos los diferentes tipos de datos biométricos, así como su aplicación práctica, conviene precisar que es lo que sucede con las bases de datos que contienen los datos biométricos de las personas, las cuales son de importancia en la presente investigación, toda vez que en ellas se almacenan y se hace posible el procesamiento comparativo de los datos almacenados previamente y la muestra

[15] *Cfr.* ESTRADA CAMACHO, Israel, *Huella genética vs. Huella dactilar, op.cit.,* p. 16.

biométrica a validar para autenticar la identidad de una persona mediante estos sistemas biométricos que se realiza de forma automatizada y en cuestión de segundos.

En el presente apartado se busca delimitar la naturaleza jurídica de estas bases de datos de los sistemas biométricos, así como delimitar la normatividad aplicable y realizar un estudio jurídico respecto de las principales connotaciones en torno al manejo y uso de las bases de datos.

La definición legal de las bases de datos se encuentra en el artículo 3º, fracción III de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, en adelante también denominada LGPDPPSO que establece que: "Bases de datos: Conjunto ordenado de datos personales referentes a una persona física identificada o identificable, condicionados a criterios determinados, con independencia de la forma o modalidad de su creación, tipo de soporte, procesamiento, almacenamiento y organización."[16]

De la anterior definición legal se contemplan a los datos biométricos en un concepto amplio y que se trata de un concepto que abarca cualquier forma, es decir, sin importar su forma en que se encuentren los datos.

Bajo este sentido aquellos datos empleados en forma de sistemas biométricos, el tipo de soporte, que en su mayoría respecto de los datos biométricos se encuentran en soporte electrónico, el procesamiento, conforme al estudio comparativo que se debe realizar para la validación de una identidad, por lo que hace a una persona identificable, efectivamente se actualiza la porción normativa y se advierte que los datos biométricos permiten hacer una distinción entre las personas, limitado evidentemente a la capacidad de las bases de datos y las personas que en ella se almacenen.

[16] *Cfr.* artículo 3o., fracción III de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

Adicionalmente, dentro del marco normativo mexicano se encuentra otra definición legal relativa a las bases de datos, contenida en la Ley Federal de Protección de Datos Personales en Posesión de Particulares, también denominada LFPDPPP, en el artículo 3o. fracción II se establece que son: “Bases de datos: El conjunto ordenado de datos personales referentes a una persona identificada o identificable”.[17]

Comparando esta definición con la referida en el párrafo anterior es notorio que esta se puede traducir como más concreta y general, es decir, en ella no cabe la distinción entre las modalidades de su obtención, soporte en que se encuentran, por ende la ley se limita a establecer como base de datos a todo aquello que contenga datos personales referentes a una persona identificable o identificada, y en ello cabe la hipótesis de los datos biométricos al poderse considerar datos personales la biometría de una persona, datos personales que lo hacen identificable del resto de las personas, con la limitante que dependerá de la capacidad y alcance comparativo de los datos almacenados en las bases de datos.

Una definición doctrinal es la proporcionada por Ester Chicano Tejada, quien establece que:

> A modo de resumen, se define una base de datos como un conjunto de datos organizados y relacionados entre sí. Para ordenar la información de manera lógica, la base de datos posee un orden que debe ser cumplido para acceder a la información de manera coherente. Existen varias tipologías y modos de clasificar las bases de datos. Un modo es clasificarlas según la forma, es almacenar y recuperar los datos, y en la concepción que debe adoptar el usuario

[17] *Cfr.* artículo 3o., fracción II de la Ley Federal de Protección de Datos Personales en Posesión de Particulares.

para interactuar con el sistema o, lo que es lo mismo, según su modelo de datos (o estructura).[18]

La anterior definición sirve para el entendimiento de que una base de datos es todo aquello que guarda una serie de datos almacenados, esto es de relevancia porque los datos que recolectan y almacenan son los datos biométricos de las personas, mismos que sirven para poder hacer el proceso de comparar las mediciones a la biometría de las personas, y a través de procesos automatizados hacer medibles sus características particulares a fin de ser inidentificables.

Se tiene entonces que para poder aplicar los sistemas biométricos como forma de identificar o hacer identificable a una persona deben estar sus características biométricas previamente capturadas, y almacenadas en bases de datos, las cuales deben permitir realizar la comparación automática en el momento de la toma de la muestra con la del dato biométrico almacenado.

Lo anterior interesa porque existe un manejo de datos biométricos, los cuales deben estar protegidos por el marco jurídico del derecho mexicano, toda vez que se entiende de su naturaleza jurídica la necesidad del tratamiento de estos biométricos almacenados.

I.1.3. OBTENCIÓN DE DATOS BIOMÉTRICOS MEDIANTE DISPOSITIVOS ELECTRÓNICOS

Una vez que se conoce del procesamiento de los datos personales obtenidos a través de sistemas biométricos, así como de su recolección y almacenamiento en bases de datos, es menester estudiar cómo se realiza la recolección de los datos biométricos exclusivamente en medios o dispositivos electrónicos, es así porque la tecnología ha avanzado de tal suerte que existen dispositivos móviles al alcance de un gran porcentaje de la población que permiten que pueda ser más frecuente su

[18] CHICANO TEJADA, Ester, *Utilización de las bases de datos relacionales en el sistema de gestión y almacenamiento de datos*, Málaga, IC Editorial, 2013, p. 140.

obtención, en consecuencia se deben analizar las formas en que actualmente se colectan los datos biométricos de las personas.

Partiendo de la fenomenología como método de investigación se tiene que para la captación de la biometría de las personas se han vuelto necesarios el uso de dispositivos electrónicos que permitan la captura y recolección de las características particulares, para lo cual actualmente ya no sólo se utilizan dispositivos fijos en centros de trabajo, como lectores de huellas dactilares, sino que ahora a través de los dispositivos móviles como celulares y tabletas electrónicas se contiene la tecnología necesaria que permite la captación de la biometría del usuario, ejemplo de ello son los lectores de huellas integrados, el reconocimiento facial, en los teléfonos móviles y todos estos datos son almacenados en su mayoría en la misma memoria del equipo móvil.

Pero el tema medular se vierte en que los datos biométricos recabados por particulares o por sujetos obligados se almacenan en sus propias bases de datos, es decir, cuando se acude al banco se pide que se ingrese la huella dactilar para acreditar nuestra identidad, cuando existe un ingreso a servicios electrónicos de grandes plataformas como *Google* se le pide al usuario además de crear una contraseña, que se realice la toma de una huella dactilar o reconocimiento facial para ingresar a los servicios, y estos datos biométricos en su mayoría se almacenan en la nube, que es un almacenamiento remoto propiedad del servidor o de un tercero que presta el servicio y en su minoría se almacenan en bases de datos propias en soportes físicos, como discos duros, tal es el caso de industrias y comercios que realizan el pase de lista mediante dispositivos fijos que captan los datos biométricos.

I.1.4. EL ALMACENAMIENTO DE DATOS BIOMÉTRICOS.

Una vez recabados los datos biométricos de la persona, lo que sigue es su almacenamiento para su utilización, con la finalidad de poder comparar los datos recabados con los que se pretenden autenticar a una persona. Para este rubro es

importante establecer desde este momento que los datos biométricos deben tener el mismo tratamiento que el marco jurídico mexicano le otorga a los datos personales sensibles, por lo que las reglas de su almacenamiento serán descritas en términos de la legislación aplicable.

En primer lugar, la Ley Federal mencionada en su artículo 2o. establece quiénes son los particulares a quienes para lo cual se ordena que son sujetos regulados por la ley son: "todos aquellos particulares ya sean personas físicas o morales siempre que entre sus actividades lleven a cabo el tratamiento de datos personales,"[19] exceptuando de esta porción en la fracción I, a las sociedades de información crediticia en los supuestos de la Ley para Regular las Sociedades de Información Crediticia, y en su fracción II exceptuando de ser sujetos privados obligados a las personas que lleven a cabo la recolección y almacenamiento de datos personales, que sea para uso exclusivamente personal, y sin fines de divulgación o utilización comercial.

De la cita anterior se deben advertir varias circunstancias de mucha importancia para sentar las bases de la esta investigación:

Primero, en relación con las Sociedades de Información Crediticia, por lo que respecta a que serán regulados por una legislación especializada y apartada;

Segundo, y muy importante en términos de particulares se limita a decir que no serán sujetos obligados aquellos particulares que realicen la recolección y almacenamiento de datos personales, que sea para uso exclusivamente personal, y sin fines de divulgación o utilización comercial, derivado que en esta última hipótesis normativa se podrían adecuar la mayoría de los particulares que efectúan

[19] *Cfr.* artículo 2 Ley Federal de Protección de Datos Personales en Posesión de Particulares.
Son sujetos regulados por esta Ley, los particulares sean personas físicas o morales de carácter privado que lleven a cabo el tratamiento de datos personales: […]

el almacenamiento de sistemas biométricos para su propio beneficio y que no se obligan en términos de la citada ley, resultando es evidentemente permea un estado de incertidumbre jurídica para el gobernado por existir un vacío legal que no regula a todos los sujetos particulares respecto de la recolección y almacenamiento, tratamiento en general, de los datos personales y datos biométricos.

Las Sociedades de Información Crediticia se encuentran definidas en el artículo 5o. de la Ley para Regular las Sociedades de Información Crediticia que establece que:

> Serán aquellas entidades que realicen la prestación de servicios consistentes en la recopilación, manejo y entrega o envío de información relativa al historial crediticio de personas físicas y morales, así como de operaciones crediticias y otras de naturaleza análoga que éstas mantengan con Entidades Financieras, Empresas Comerciales o las Sofomes E.N.R., por lo que para operar como sociedades de información crediticia, […][20]

Además se remite al artículo 6o. de la citada ley advirtiendo que el requisito legal es que: "para constituirse y operar como Sociedad de Información Crediticia se requerirá autorización del Gobierno Federal, misma que compete otorgar a la Secretaría de Hacienda y Crédito Público, oyendo la opinión del Banco de México y de la Comisión, en suma que, estas autorizaciones serán intransmisibles."[21]

En la misma tesitura, los datos biométricos como datos personales sensibles recolectados y almacenados de los clientes de las sociedades de información

---

[20] *Cfr.* artículo 5o, Ley para Regular las Sociedades de Información Crediticia.
La prestación de servicios consistentes en la recopilación, manejo y entrega o envío de información relativa al historial crediticio de personas físicas y morales, así como de operaciones crediticias y otras de naturaleza análoga que éstas mantengan con Entidades Financieras, Empresas Comerciales o las Sofomes E.N.R., sólo podrá llevarse a cabo por Sociedades que obtengan la autorización a que se refiere el artículo 6o. de la presente ley.

[21] *Cfr.* artículo 6o. de la Ley para Regular las Sociedades de Información Crediticia.
Para constituirse y operar como Sociedad de Información Crediticia se requerirá autorización del Gobierno Federal, misma que compete otorgar a la Secretaría, oyendo la opinión del Banco de México y de la Comisión. Por su naturaleza, estas autorizaciones serán intransmisibles.

financiera se protegen en términos del artículo 28 de la precitada ley, en el sentido que, se ordena que las sociedades, sus empleados y funcionarios tienen prohibido proporcionar información relativa a datos personales de los clientes para comercialización de productos o servicios que pretendan ofrecer los usuarios o cualquier tercero, salvo para la realización de consultas relativas al historial crediticio.

Estableciendo que en materia punitiva, quien proporcione información inobservando lo establecido por el citado artículo, específicamente de datos personales, incurrirá en el delito de: "revelación de secretos"[22] a que se refiere el artículo 210 del Código Penal Federal.

Conforme a la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, en el artículo 1o. establecen quienes son los sujetos obligados, en este sentido son: "sujetos obligados en el ámbito federal, estatal y municipal, cualquier autoridad, entidad, órgano y organismo de los Poderes Ejecutivo, Legislativo y Judicial, órganos autónomos, partidos políticos, fideicomisos y fondos públicos."[23]

También son sujetos obligados los sindicatos y cualquier otra persona física o moral que reciba y ejerza recursos públicos o realice actos de autoridad en el ámbito federal, estatal y municipal serán responsables de los datos personales conforme a la citada Ley General.

---

[22] *Cfr.* artículo 28 de la Ley para Regular las Sociedades de Información Crediticia.
Las Sociedades solo podrán proporcionar información a un Usuario, cuando este cuente con la autorización expresa del Cliente, mediante su firma, en donde conste de manera fehaciente que tiene pleno conocimiento de la naturaleza y alcance de la información que la Sociedad proporcionará al Usuario que así la solicite, del uso que dicho Usuario hará de tal información y del hecho de que este podrá realizar consultas periódicas de su historial crediticio, durante el tiempo que mantenga relación jurídica con el Cliente. La firma a que se refiere este párrafo podrá ser recabada de manera autógrafa o por medios electrónicos, en este último caso, siempre que cumpla con los términos y condiciones establecidos por el Banco de México. […]

[23] *Cfr.* artículo 1o. de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

Por último, se remite en materia de protección de datos personales para el caso de todos los demás supuestos diferentes a los mencionados, las personas físicas y morales a lo previsto por la Ley Federal de Protección de Datos Personales en Posesión de Particulares.

Por lo que respecta al almacenamiento de los datos biométricos, como datos personales la Ley General referida en el artículo 3o. fracción XXII ordena que:

> Serán medidas de seguridad físicas como todas aquellas acciones y mecanismos para proteger el entorno físico de los datos personales y de los recursos involucrados en su tratamiento, es decir, se involucran los sistemas biométricos. Y entre sus actividades yace la de proveer a los equipos que contienen o almacenan datos personales de un mantenimiento eficaz, que asegure su disponibilidad e integridad. [24]

En el mismo sentido la fracción XXIII ordena lo relacionado a medidas de seguridad técnicas que son:

> Todas aquellas acciones y mecanismos que se valen de la tecnología relacionada con *hardware* y *software* para proteger el entorno digital de los datos personales, por consecuente los datos biométricos y los recursos involucrados en su tratamiento, y entre sus funciones están el gestionar las comunicaciones,

[24] *Cfr.* artículo 3o. de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.
[…] XXII.-Medidas de seguridad físicas: Conjunto de acciones y mecanismos para proteger el entorno físico de los datos personales y de los recursos involucrados en su tratamiento. De manera enunciativa más no limitativa, se deben considerar las siguientes actividades: a) Prevenir el acceso no autorizado al perímetro de la organización, sus instalaciones físicas, áreas críticas, recursos e información; b) Prevenir el daño o interferencia a las instalaciones físicas, áreas críticas de la organización, recursos e información; c) Proteger los recursos móviles, portátiles y cualquier soporte físico o electrónico que pueda salir de la organización, y d) Proveer a los equipos que contienen o almacenan datos personales de un mantenimiento eficaz, que asegure su disponibilidad e integridad; […]

operaciones y medios de almacenamiento de los recursos informáticos en el tratamiento de datos personales.[25]

Por lo que desde este momento para la investigación se sientan las bases de los mecanismos de seguridad que deben tener los sistemas informáticos que empleen el uso de los sistemas biométricos en sus equipos que almacenan datos personales.

I.2. TRATAMIENTO E IMPORTANCIA DE LOS DATOS BIOMÉTRICOS

Una vez delimitado lo anterior, debe señalarse específicamente a que se refieren el tratamiento y porque es tan importante conocer las medidas de protección que tienen los datos biométricos como datos personales sensibles, e inducir a lo que en capítulos siguientes será definido.

La LGPDPPSO establece en el artículo 3o. fracción XXXIII qué es lo que se entiende por tratamiento como cualquier operación o conjunto de operaciones efectuadas mediante procedimientos manuales o automatizados aplicados a los datos personales, relacionadas con la obtención, uso, registro, organización, conservación, elaboración, utilización, comunicación, difusión, almacenamiento, posesión, acceso, manejo, aprovechamiento, divulgación, transferencia o disposición de datos personales.

En continuidad con la línea de investigación, en la fracción XVIII del artículo 6o. de la Ley Federal de Protección de Datos Personales en Posesión de Particulares, se ordena qué debe entenderse por tratamiento la obtención, uso, divulgación o

[25] *Cfr.* artículo 3o. de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.
[…]XXIII. Medidas de seguridad técnicas: Conjunto de acciones y mecanismos que se valen de la tecnología relacionada con hardware y software para proteger el entorno digital de los datos personales y los recursos involucrados en su tratamiento. De manera enunciativa más no limitativa, se deben considerar las siguientes actividades: a) Prevenir que el acceso a las bases de datos o a la información, así como a los recursos, sea por usuarios identificados y autorizados; b) Generar un esquema de privilegios para que el usuario lleve a cabo las actividades que requiere con motivo de sus funciones; c) Revisar la configuración de seguridad en la adquisición, operación, desarrollo y mantenimiento del software y hardware, y d) Gestionar las comunicaciones, operaciones y medios de almacenamiento de los recursos informáticos en el tratamiento de datos personales;
[…]

almacenamiento de datos personales, por cualquier medio, y se distingue que el uso abarca cualquier acción de acceso, manejo, aprovechamiento, transferencia o disposición de datos personales.

Lo anterior cobra relevancia porque se define el tratamiento de los datos biométricos como datos personales, toda vez que de ellos pueden identificarse a una persona, y que tendrán la naturaleza jurídica de datos personales para efectos de lo conducente a su protección.

En la misma línea de investigación, la legislación internacional, específicamente el Reglamento General de Protección de Datos Personales de la Unión Europea, en el artículo 4o. define el tratamiento de datos personales como:

> Cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción.[26]

También se añade un concepto de tratamiento de datos personales denominado transfronterizo, por lo que refiere que puede dividirse en dos tipos: primero, es aquel realizado en el contexto de las actividades de establecimientos en más de un Estado miembro de un responsable o un encargado del tratamiento en la Unión, si el responsable o el encargado está establecido en más de un Estado miembro, o; segundo, el tratamiento de datos personales realizado en el contexto de las actividades de un único establecimiento de un responsable o un encargado del tratamiento en la Unión, pero que afecta sustancialmente o es probable que afecte sustancialmente a interesados en más de un Estado miembro.

[26] Artículo 4o. del Reglamento General de Protección de Datos Personales de la Unión Europea.

Concomitante con lo anterior, es de destacarse que el tratamiento de los datos personales sensibles en el mundo se ha visto afectado con la utilización de tecnología que permite a las personas acceder a los datos desde cuales parte y en cualquier momento, con lo cual la problemática se hace más latente y de ahí la necesidad de resolverla.

Sin que se pretenda ser globalizador, el principal problema en el uso de los datos biométricos sin una robusta legislación a nivel nacional y mundial, genera problemas que serán abordados en otro capítulo de este trabajo, entre los que destacan la usurpación de la identidad, robo de identidad y el indebido tratamiento de los datos biométricos para la comisión de fraudes, los cuales no son un problema menor para la sociedad pues implican trastocar más que la seguridad y certeza jurídica, pues se afecta la esfera más íntima de las personas que es su identidad.

Concluyendo de este apartado que, los datos biométricos son datos personales sensibles y que por consiguiente tienen el carácter y protección jurídico como tal, y que derivado de un largo y constante progresivo proceso de evolución de los derechos humanos, los datos personales son constitucionalmente tutelados, por lo tanto, cualquier violación y menoscabo a estos derechos de protección, incluyendo el de la intimidad, merecen que el gobernado acuda a los medios de control constitucional, previo a agotar los requisitos que la legislación en la materia exigen.

Finalmente, y como parte de la delimitación cualitativa de la investigación, el trabajo como su título lo refiere será divido en dos vertientes principales: la primera el uso de los datos biométricos como una forma de identidad y de un proceso de autenticación y; segundo como una forma de otorgar el consentimiento para la celebración de actos jurídicos, vertientes que serán analizadas en los capítulos 2 y 3 y cuyo objeto principal es el análisis de los datos biométricos y efectos en el mundo del derecho en su aplicación.

I.3. DE LA IDENTIDAD

Cómo una forma de introducir a los siguientes capítulos, se tiene que la identidad es un derecho humano, y como se abordará en un capítulo siguiente, merece un marco regulatorio específico, es por ello, que de este apartado exclusivamente se delimitarán las bases para su estudio y análisis posterior.

La identidad de las personas es un tópico que día con día evoluciona y que siempre será cambiante de acuerdo a cada persona, y esto es así porque cada persona es única y su identidad sigue la misma suerte, como se precisará en el siguiente capítulo existen diversos tipos de identidad y que los mismos remiten a un aspecto sustantivo y subjetivo de los individuos, pero para efectos de las bases metodologías y aplicado a esta investigación, los datos biométricos implican una base fundamental para la identidad.

Los datos biométricos como forma de identidad, presuponen vertientes no sólo en el ámbito tecnológico sino que también ideológico, pues además de interferir en el aspecto técnico también repercute en la vida de las personas, y como será motivo de disenso posteriormente, el problema planteado radica en que actualmente se están aplicando sistemas informáticos que posibilitan identificar a las personas mediante el uso de tecnologías de la información, específicamente a través de sistemas computarizados, los cuales previamente tiene acceso a datos almacenados, y que permiten hacer el análisis comparativo que distingue a las personas del resto.

La problemática surge desde la concepción del derecho de identidad como un derecho humano y que con el uso desmedido de tecnologías, la legislación se ve superada para proteger al titular de la identidad, la misma sociedad y eficacia en trámites y procesos exigen que existan nuevas formas de identificarse, luego entonces, el uso de los datos biométricos encuentran su sustento para buscar resolver esta problemática, ya sea como un proceso de identificación o uno de autenticación.

I.4. DEL CONSENTIMIENTO EN ACTOS JURÍDICOS

La segunda vertiente del uso de los datos biométricos se concibe como una forma de otorgar el consentimiento en los actos jurídicos, pues con la incorporación y cada vez más constante uso de los mecanismos de comercio electrónico, así como de contratación de servicios en línea, la utilidad radica en que los datos biométricos se han considerado por diversos operadores como una forma de firmar los documentos o incluso como un signo inequívoco por el cual se afirma la voluntad de una parte para crear efectos de derecho, comparándolo inclusive como una firma electrónica o una firma electrónica avanzada.

Como parte de los antecedentes del uso de los sistemas biométricos se recuerda que anteriormente se comenzaron a emplear manualmente las huellas digitales para signar y brindar un segundo paso de seguridad para el otorgamiento de la voluntad para la celebración de los actos jurídicos.

Se hace la referencia a cuando en papel se plasmaban las huellas dactilares de un individuo o la geometría de la mano, se almacenaba dicho dato biométrico y posteriormente se pedía plasmar de nuevo el dato biométrico, para manualmente a través de un peritaje hacer el comparativo con el primer documento, y así con el apoyo de una ciencia se podría corroborar que se tratara de la misma persona, lo anterior puede observarse como un símil a obtener las firmas indubitables de una persona.

Ahora bien, este proceso que se realizaba manualmente ahora se realiza a través de un proceso automatizado y que involucra un sistema informático y tecnologías que permiten el proceso masivo y automático de datos biométricos, y se puede traducir como una capacidad y rapidez de comparación que nunca podría alcanzarse manualmente, con el apoyo de los sistemas digitales que además permiten tener un mayor número de datos biométricos almacenados, también permiten que ahora se realice en cuestión de segundos un proceso que a sus inicios tardaba mucho y que forzosamente requería involucrar un perito en la materia.

En México la implementación de los datos biométricos como forma de consentimiento expreso ha incrementado de forma proporcional al aumento de disponibilidad de dispositivos electrónicos y del uso de plataformas que permiten el comercio electrónico, así como de la contratación de servicios y pago de los mismos, actos que tradicionalmente se signaban en físico y mediante presentes, derivado de ello surgió la necesidad de la creación de firmas electrónicas que permitieran la agilidad en los actos, por lo que la legislación es específica respecto de la implementación y regulación de las firmas electrónicas como forma de consentir actos a través de dispositivos electrónicos.

Conforme a lo anterior, además de la legislación específica en materia de firmas electrónicas se reformaron diversas disposiciones inherentes al comercio electrónico, como se sustentan en el paquete de reformas publicadas en el Diario Oficial de la Federación con fecha 29 de mayo del 2000, en la cual se reestructuró el Título Segundo del Código de Comercio que incorporó dentro del sistema jurídico mexicano principios e instituciones relativas al comercio electrónico y desde esa fecha en México se aceptaba u presuponía una visión a futuro de la celebración de actos jurídicos por medios digitales y que hoy es una realidad.

El comercio electrónico doctrinalmente en palabras de María Susana Dávalos Torres se ha definido como: “actos jurídicos realizados a través de instrumentos que permiten transmitir información por medio de la electricidad. De manera general, el término «medios electrónicos,» incluye al telégrafo, el teléfono, el fax y la televisión, por mencionar alguna, pero frecuentemente es identificado o es asociado con el internet.”[27] Siendo un parteaguas para el aspecto conceptual del comercio electrónico y que para esta investigación resulta trascendental conocer.

[27] DÁVALOS TORRES, María Susana, *Manual de introducción al derecho mercantil,* México, Instituto de Investigaciones Jurídicas UNAM, 2010, p. 63.

En relación el comercio electrónico debe precisarse que como cualquier otra rama del derecho, las disposiciones imperativas y vigentes siempre buscan alcanzar la realidad de la sociedad, ejemplo de ello fue el Título Segundo del Código de Comercio pues incorporó desde el 2000 este concepto a nuestra realidad, pero que en ese entonces los datos biométricos no estaban contemplados como una forma para el otorgamiento del consentimiento para la celebración de actos jurídicos.

Se debe de hablar entonces de una nueva forma en que se están celebrando los actos jurídicos, ya no como tradicionalmente se hacían, ni como se reguló en el espíritu legislador del año 2000, pues con la implementación de lectores y procesadores de datos biométricos se ha creado una nueva forma en la que los prestadores de servicios y comerciantes buscan otorgar su consentimiento de manera que sea inmediata, desde cualquier momento y desde cualquier parte del mundo.

Entonces existen nuevas formas de otorgar el consentimiento que sin lugar a dudas benefician la agilidad en los procesos y hasta cierto punto brindan un sentimiento de mayor confianza con respecto a métodos tradicionales, y como se analizará, estos elementos se pueden poner a discusión.

Estas nuevas aplicaciones en el mundo de derecho exigen que la legislación no se quede atrás porque ya no son los mismos alcances a dispositivos que los que se previeron en el espíritu legislador con las reformas del Título Segundo de Código de Comercio y las leyes relativas a la firma electrónica.

Respecto del presente capítulo y una vez que se ha expuesto el marco teórico y conceptual de los datos o sistemas biométricos, es procedente acudir al panorama del derecho para realizar el estudio de las problemáticas expuestas, siendo necesario que la investigación se efectúe en dos vertientes, por una parte desde el derecho de datos personales, como una forma de identidad, y por otro lado desde

la óptica del acto jurídico, relativo al consentimiento, abordando el comercio electrónico y el uso de firmas electrónicas.

II. CAPÍTULO II DEL USO DE SISTEMAS BIOMÉTRICOS COMO FORMA DE IDENTIFICACIÓN Y CONSENTIMIENTO EN ACTOS JURÍDICOS

Este segundo capítulo tiene como principal objetivo la delimitación conceptual y en el plano fáctico en un primer término del uso de los sistemas biométricos como una forma de identificación y, en segundo lugar del uso de los sistemas biométricos como una forma de manifestar el consentimiento en los actos jurídicos que se celebran, resultando relevante para el trabajo de investigación, toda vez que desde este apartado logran advertirse las omisiones y vacíos jurídicos del sistema jurídico mexicano derivado de la deficiente o en su caso nula legislación, así como sus repercusiones en la esfera jurídica de seguridad y certeza jurídica, y que finalmente producen un estado de indefensión para hacer valer los derechos sustantivos.

II.1. USO DE SISTEMAS BIOMÉTRICOS COMO FORMA DE IDENTIFICACIÓN DE LAS PERSONAS

Contemporáneo a la identidad de las personas se ha visto inmersa en los diversos avances de la tecnología y acelerado por el uso de dispositivos móviles que permiten un rango de alcance mayor a las tecnologías de identificación, partiendo del uso del método de investigación de la fenomenología, ha cobrado relevancia la identidad tanto en el interés individual de cada persona a ser distinguida del resto, así como un interés que en la colectividad, es decir, se habla de una dualidad de intereses que importan a la identidad, dado que la identidad sólo sería aplicable si se logra hacer un ejercicio comparativo con otra persona.

El punto de partida de la identidad se encuentra en el valor de acuerdo al interés que se tenga al hacer a una persona distinguible de las demás, por lo que al realizar un ejercicio hipotético en el que sólo existiera una persona en el mundo, su identidad no tendría sentido más que de forma interna para esta persona, al no poderse hacer un ejercicio de comparación de rasgos, nombre, edad, sexo, biometría característica, pero en una concepción fáctica, real y vigente, el número de personas

en este mundo aumenta cada día y con ello aumenta la necesidad de hacer distinguible a una persona de una colectividad.

Primeramente, al hablar de la identificación de las personas cada día se convierte en un tema controversial, dada la propia naturaleza de la identidad, por lo que de esta premisa y necesidad se parte para el estudio del derecho a la identidad, entendido como un derecho humano, se debe entender el concepto de identidad, por lo que se apoya el trabajo de investigación en diversidad de autores que se exponen en los siguientes párrafos.

En la Comisión de Derechos Humanos del Distrito Federal ahora Ciudad de México lo definen como: "Un derecho humano fundamental que da existencia a los seres humanos."[28]

Y confrontándolo con el artículo 11 de la Convención Americana sobre Derechos Humanos, nos dice que: "cuando analizamos el derecho a la identidad de las personas es necesario tener presente la conexión de este derecho con la vida privada de éstas y la prohibición de injerencias en su honra y dignidad."[29]

Sin perjuicio de lo citado, desde este momento se establece que el artículo 18 de la Convención en cita es la que expresamente regula el derecho a la identidad por referirse: "al derecho al nombre y apellidos de una persona,"[30] y que son datos personales inherentes a su titular que lo hacen identificable.

---

[28] COMISIÓN DE DERECHOS HUMANOS DEL DISTRITO FEDERAL, *Informe especial, situación de los derechos humanos de las poblaciones callejeras en el Distrito Federal 2012-2013*, México, CDHDF, 2014, p. 71, disponible en: <https://piensadh.cdhdf.org.mx/images/publicaciones/Informe_especial/2014_Informe_esp_poblaciones_callejeras.pdf > [Consulta: 10- octubre-2021].

[29] *Cfr.* artículo 11 de la Convención Americana sobre Derechos Humanos.
Protección de la Honra y de la Dignidad.
1. Toda persona tiene derecho al respeto de su honra y al reconocimiento de su dignidad.
2. Nadie puede ser objeto de injerencias arbitrarias o abusivas en su vida privada, en la de su familia, en su domicilio o en su correspondencia, ni de ataques ilegales a su honra o reputación.
3. Toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques.

[30] *Cfr.* artículo 18 de la Convención Americana sobre Derechos Humanos. Derecho al Nombre.

En el mismo orden de ideas, en el sistema jurídico mexicano la incorporación del derecho de identidad como un derecho humano, fue reconocido como actualmente se concibe mediante las reformas del año 2014, específicamente las publicadas en el Diario Oficial de la Federación en data 17 de junio del 2014, reformas a la Constitución Política de los Estados Unidos Mexicanos estableciéndose desde ese entonces concepto actual del derecho a la identidad en su artículo 4o. en el párrafo 8, cuyo extracto a continuación se reproduce: "Toda persona tiene derecho a la identidad y a ser registrado de manera inmediata a su nacimiento. El Estado garantizará el cumplimiento de estos derechos. La autoridad competente expedirá gratuitamente la primera copia certificada del acta de registro de nacimiento."[31] Precepto normativo que tutela el derecho a la identidad como un derecho humano y que por ende goza de los mecanismos de protección que la Constitución Política de los Estados Unidos Mexicanos establece.

Advirtiéndose de las dos concepciones legales citadas, que el derecho a la identidad se reconoce con el rango y protección que implica ser un derecho humano, y que no sólo importa para la vida privada del individuo, sino también como un beneficio para la sociedad, es decir, es un derecho humano que no sólo contiene rasgos de individualistas si no colectivos, siendo un elemento clave para la distinción de los integrantes de una población.

Lo anterior, se sustenta en la premisa que el derecho a la identidad no sólo se entiende como el origen o diferencia de las personas entre otras, sino que además es un elemento clave para la identificación.

Al respecto Gilberto Giménez, establece que:

Toda persona tiene derecho a un nombre propio y a los apellidos de sus padres o al de uno de ellos. La ley reglamentará la forma de asegurar este derecho para todos, mediante nombres supuestos, si fuere necesario.

[31] *Cfr.* artículo 4o., párrafo 8 de la Constitución Política de los Estados Unidos Mexicanos.

> El concepto de identidad implica siempre por lo menos los siguientes elementos: (1) la permanencia en el tiempo de un sujeto de acción (2) concebido como una unidad de límites (3) que lo distinguen de todos los demás sujetos, (4) aunque también se requiere el reconocimiento de estos últimos.[32]

Elementos que en relación con el tema que nos ocupa sustentan la implementación de los sistemas biométricos para lograr que se identifiquen a las personas.

Respondiente a un plano fáctico en México y como ejemplo de la identidad de las personas se puede hablar de las actas de nacimiento y en concordancia con la Constitución Política de los Estados Unidos Mexicanos, estas se pudieran afirmar como el atestado que proporciona la identidad, el cual protege y garantiza el derecho humano, pero pese a las diversas codificaciones estatales y legislación aplicable que estipulan una serie de directrices, como resultado de una necesidad de registrar a un menor ante la autoridad competente, se tiene que el Juez u Oficial del Registro Civil, casi acto inmediato después de su nacimiento registran al recién nacido y en el acta se contienen rasgos que hacen identificable a una persona como; su nombre, ascendencia, apellidos, fecha y lugar de nacimiento, sexo, nacionalidad, son los que hacen a una persona distinta e identificable del resto, pero en la realidad existen personas que no se encuentran registradas por situaciones diversas, las cuales se constriñen como situaciones que agravan la problemática de la identidad.

En cambio, si se cree que el problema se solucionaría con tener un registro confiable y de todas las personas, en la realidad el problema de identidad persiste en personas cuyos registros se realizaron de manera equivocada, ejemplo de ello son las personas con el nombre mal escrito, sin reconocimiento de los ascendentes, falta de apellidos, omisiones que en general pudieran implicar un menoscabo a su derecho humano a la identidad, de igual forma como sucede con la adecuación del

---

[32] GIMÉNEZ, Gilberto, C*ultura, Identidad y Procesos de Individualización*, México, Instituto de Investigaciones Sociales, Universidad Nacional Autónoma de México, 2010, p. 4.

acta a la realidad social del individuo, como el caso de la concordancia sexo-genérica de una persona, cambio de nombre, reconocimiento de hijos e hijas, situaciones que de no atenderse por las autoridades responsables convalidan un plano de transgresión a derechos humanos.

Por lo tanto, la identidad y su objetivo de hacer una distinción entre las personas, importa en la colectividad para que en un sentido propio y de rasgos únicos a los sujetos individuales, o identificables de la totalidad de población, y consecuentemente se pueda determinar esta cualidad de distinción con el uso de sus datos personales, entre ellos, los sistemas biométricos, en atención a que a través de la biometría como los rasgos únicos de cada individuo pueda hacerse el ejercicio comparativo entre un sujeto y con las limitantes y variantes que se han mencionado, y así hacer la diferenciación de ese rasgo único con el de las demás personas, teniendo con fin último un proceso subjetivo por el que los sujetos definen su diferencia de otras personas.

Así se tiene como premisa que el derecho a la identidad puede entenderse como un derecho fundamental de contar con un nombre, nacionalidad, apellidos, fecha de nacimiento, sexo y origen, o de elementos que permiten que un individuo pueda ser identificable y distinguible del resto de la población, en el tenor que con estos datos se produzca una certeza respecto a la identidad del individuo, y de tal suerte que pueda ejercer su derecho sin restricciones.

II.1.1. DE LA IDENTIFICACIÓN POR EL USO DE SISTEMAS BIOMÉTRICOS

El enorme interés contemporáneo que se tiene para identificar a las personas es una problemática que se refleja en las demás ramas de las ciencias sociales, específicamente en el derecho, problemática que se agudiza con el uso e implementación de tecnologías como se analizó en el primer capítulo, tecnologías que sirven para lograr identificar y hacer identificable a una persona del resto.

Una vez que se conoce respecto al derecho a la identidad, del tema que ocupa es cómo el avance tecnológico ha permitido la utilización de los sistemas biométricos para distinguir a un individuo, para lo cual es indispensable abordar lo relativo a los tipos de identidad, dentro de la cual existe una categorización de las formas en las que una persona se identifica, la cual las distingue como; identidad legal, identidad vivencial, identidad física, identidad digital e identidad social y virtual.

La identidad legal, se entiende por María Luisa Santillán como:

> La llave de acceso para todos los derechos. La Declaración de los Derechos del Hombre y del Ciudadano reconoce a la persona como integrante de una comunidad política, así como la garantía de su libertad y de su propiedad. Por lo tanto, para poder identificarse como un ciudadano que forma parte de una comunidad, el primer derecho que se le debe garantizar es el de la identidad.[33]

De lo anterior, puede desprenderse que se trata dentro del sistema jurídico mexicano a la identidad desde que dentro del Estado surge la identidad de una persona en el Registro Civil.

La identidad vivencial es: "un concepto derivado del punto anterior, con la obtención de la Clave Única de Registro de Población por sus siglas CURP,"[34] siendo esta con la que se efectúa un ejercicio comparativo entre la población mexicana, es decir, se tiene como objetivo de hacer distinguible a una persona mexicana del resto de la población mediante el uso de letras y números que conforme a su orden pueden establecer el nombre, apellidos, año, mes y día de nacimiento de una persona, lugar de registro, que a través de una clave elaborada

---

[33] SANTILLÁN, María Luisa, *Los derechos de los invisibles,* México, Universidad Nacional Autónoma de México, 2019, número 1, disponible en: <http://ciencia.unam.mx/leer/839/los-derechos-de-los-invisibles-identidad-legal-de-las-poblaciones-callejeras> [Consulta: 04- septiembre-2021].

[34] DIRECCIÓN DEL REGISTRO NACIONAL DE POBLACIÓN E IDENTIFICACIÓN PERSONAL, *Registro e Identificación de Población,* México, Secretaría de Gobernación, p. 9, disponible en: <https://www.transparenciapresupuestaria.gob.mx/work/models/PTP/Reingenieria_Gasto/imagenes/Ventanas/Ramo_4/04E012.pdf> [Consulta: 04-septiembre-2021].

de la combinación de números y letras se permite hacer distinguible a una persona registrada del resto de los registrados.

Ahora bien, la identidad física, en palabras de Leticia Adriana es: “la Identidad física: implica aceptación del propio cuerpo, y de éste en relación al otro.”[35] y añade que:

> Es aquella que se logra a través de la biometría de las personas, que importa para el tema de investigación toda vez que en este rubro se encuentran las características biométricas de las personas y que a través de estas se puede hacer distinguible a una persona del resto, basados en la premisa que cada individuo cuenta con características física únicas y que estas son susceptibles de ser medibles mediante el uso de las tecnologías.[36]

Respecto de identidad digital, en palabras de Miguel Ángel Morales Sandoval:

> Se debe entender como aquel tipo de identidad y conjunto de acciones que hacen identificables a las personas en internet, por lo tanto, a medida que la actividad en internet y redes sociales aumentan, se podría decir que la identidad digital aumenta, derivado de lo anterior, que mediante el uso de plataformas digitales pueda realizarse un estudio comparativo de rasgos y actividades en internet que permiten distinguir a una persona del resto, identidad digital e identidad social y virtual.[37]

---

[35] MARTÍNEZ DÍAZ BARRIGA, Leticia Adriana y Sergio Octavio González Nevarez, *La construcción de los procesos de identidad de las y los docentes de educación física,* México, X Congreso Nacional de Investigación Educativa, número 16, disponible en: <www.comie.org.mx> [Consulta: 08-septiembre-2021].

[36] *Idem.*

[37] *Cfr.* MORALES SANDOVAL, Miguel Ángel, *Nuestra identidad digital después de la muerte,* México, Instituto de Investigaciones Jurídicas, UNAM, julio- agosto 2020, número 58. <https://revistas.juridicas.unam.mx/index.php/hechos-y-derechos/article/view/14978/15940> [Consulta: 08-septiembre-2021].

Para finalizar esta categorización, la identidad social puede definirse en palabras de Raúl Béjar y Héctor Cappello como: “La identidad social corresponde a la pertenencia al grupo e implica la posesión de los atributos de criterio del grupo, por lo que el comportamiento de cualquier miembro, cuando actúa desde esa pertenencia, exhibirá, con una alta probabilidad, esos atributos.”[38]

En el aspecto colectivo, es la identidad que permite distinguir a una colectividad del resto de las colectividades, es decir, que tomando como base el carácter colectivo se puede hablar de una identidad de personas o grupos que sirve de sustento para ser sujetos de derechos subjetivos y mecanismos de protección distintos de los demás grupos de personas, tema que cobra importancia en la distinción si la cultura es una forma de identidad o la identidad como una forma de cultura, temas que abordan una perspectiva de permanencia y distinción de distintos grupos de personas que por cultura pueden hacerse distinguibles.

En consecuencia, una vez mencionados los tipos de identidad el panorama conceptual de la identidad de la persona se hace más extenso, y esto debería implicar un beneficio para el titular del derecho, pero esto no es así, en cada uno de los tipos de identidad pueden advertirse diversos tópicos que son problemáticos para identificar a un individuo, factores externos, subjetivos, diversos y variables que impiden que se compare a una persona de las demás, como lo son; la falta de actas de nacimiento, errores en el registro de las personas, la omisión de contar con la Clave Única de Registro de Población, la falta de adecuación de las actas de nacimiento a la realidad social de la persona, la diferencia social y económica para contar con servicios de internet, el nulo acceso a internet, el apoderamiento de los bienes culturales y la globalización.

II.1.1.1. La nueva identificación y los medios digitales

[38] BÉJAR NAVARRO, Raúl y Héctor M. Cappello y García, *Aproximaciones a la identidad nacional y sus correlatos fácticos,* México, Instituto de Investigaciones Sociales UNAM, 2009, p. 4.

En el ámbito actual y con los medios de comunicación más desarrollados que antes, las problemáticas para la identificación de las personas deben observar las soluciones que se han implementado y en este aspecto utilizando el método comparativo se tiene como un referente internacional al Banco Mundial que establece que:

> La tecnología digital ofrece a los países el potencial para lograr avances rápidos en sus objetivos en materia de identificación y mejorar la calidad y la utilidad de los sistemas de identificación, beneficiando a los individuos. Por ejemplo, las bases de datos de registros digitalizadas —en comparación con los libros de contabilidad guardados en una oficina local— facilitan la verificación a distancia de los documentos de una persona (incluida la verificación automática), haciendo más eficiente la prestación de servicios y permitiendo a los organismos de identificación reemplazar las credenciales y los archivos perdidos, robados o destruidos.[39]

Convalidando que la identificación a través del uso de tecnologías que permiten comparar bases de datos personales en una velocidad notablemente superior a lo que un ser humano podría hacerlo, es lo que ha sustentado el uso de estas tecnologías de identificación, se habla entonces, de una evolución en los procesos de individualización de las personas de forma automática e instantánea.

Así mismo, el Banco Mundial asegura que:

> Los mecanismos de autenticación digital posibilitan las transacciones automáticas que son más seguras y fiables que las realizadas mediante sistemas de autenticación manual (a saber, comparar visualmente a una persona con la

[39] BANCO MUNDIAL, *Sistemas de identificación digitales fiables e inclusivos pueden abrir oportunidades para las personas vulnerables del mundo,* Banco Mundial, agosto 2019, número 1, disponible en:<https://www.bancomundial.org/es/news/immersive-story/2019/08/14/inclusive-and-trusted-digital-id-can-unlock-opportunities-for-the-worlds-most-vulnerable> [Consulta: 20-septiembre-2021].

foto de su documento de identidad) y pueden reducir la cantidad de información personal que se revela en una transacción (p. ej., credenciales basadas en atributos). (i) El uso del reconocimiento biométrico automático (p. ej., usando las huellas digitales o escaneando el iris) puede ayudar a asegurar que las identidades sean únicas (esto es, que las personas no pueden inscribirse varias veces) y proporcionan un método de autenticación libre de contraseñas y conveniente.[40]

No obstante las ventajas señaladas, el mismo Banco Mundial establece que:

Si bien la tecnología digital puede aumentar la privacidad y la seguridad de cierta manera, puede también aumentar muchos de los riesgos asociados con la recopilación y la gestión de datos personales. Cuando las bases de datos se digitalizan, también aumenta el riesgo y la magnitud de las filtraciones y los robos de identidad. Además de las posibles violaciones a la privacidad, la digitalización de los registros de identificación puede crear asimismo nuevas barreras en materia de acceso e inclusión. Ciertas poblaciones —p. ej., los trabajadores manuales con huellas digitales desgastadas, los ancianos o las personas con discapacidad— podrían tener dificultades para inscribirse o usar sistemas de identificación que dependen de algunos datos biométricos, lo que puede ocasionar exclusión si no existen otras opciones. La utilización de la biometría genera también un conjunto específico de riesgos relacionados con la protección de los datos, que se debe estudiar cuidadosamente y mitigar de manera integral en cada aplicación de esta tecnología. De modo similar, los sistemas de identificación dependientes de tecnologías que no están disponibles de manera universal o consistente entre la población (p. ej., conexión a internet, correo electrónico, teléfonos móviles) pueden empeorar la brecha digital.[41]

[40] *Idem.*
[41] *Idem.*

De las anteriores citas se deprende que, si bien existen ventajas y beneficios extensos respecto del uso de los sistemas biométricos para poder identificar a las personas, también debe existir protección a los derechos humanos, protección de datos personales, derechos de los usuarios de plataforma digitales, sistemas incluyentes para que los beneficios mitiguen los riesgos que su utilización implica, lo anterior en suma a los lineamientos que el Banco Mundial reconoce deben existir dentro de los sistemas jurídicos de cada Estado, consistentes en que sean:

> (i) integrales para posibilitar los sistemas de identificación y proporcionar salvaguardias. También exige un enfoque de privacidad y seguridad mediante el diseño (ii) que integre los controles técnicos, administrativos y de gestión en el diseño del sistema, desde el inicio. Por otra parte, la consulta y la comunicación tempranas y permanentes con el público y la sociedad civil pueden ayudar a asegurar que los sistemas de identificación se diseñen tomando en consideración a las personas y se implementen de una manera responsable e inclusiva.[42]

Derivándose de lo expuesto en este apartado que, si bien ya existe un avance tecnológico para la identificación de las personas, aún debe trabajarse en consolidar sistemas inclusivos y que traten de mitigar la gran brecha de desigualdad y de acceso a los medios tecnológicos con el objeto de establecerse sistemas automatizados que ayuden en la tarea de identificación.

II.1.1.2. Formas de identificación electrónica

Siguiendo con la misma línea de investigación, el uso de estos sistemas de identificación electrónica recientemente va en aumento, no siendo así para el aumento en el marco regulatorio que los limita, en este apartado se aborda respecto de las formas de identificación electrónica, bajo la idea que se induzca el tópico del marco conceptual y la adecuación de la norma imperativa a la realidad del uso de la identificación electrónica.

[42] *Idem.*

En un primer momento se deben definir los sistemas de identificación, para Katia Gesell Torres Carrasco quien investiga dentro del ramo de la criminalística:

> Los sistemas de identificación de personas son procedimientos derivados de la criminalística y sus disciplinas auxiliares, en los que se emplean diversos métodos y técnicas para establecer la identidad de una persona, ya sea viva, muerta o en sus restos humanos; es decir, para determinar el conjunto de características o rasgos propios de una persona que la distinguen de otras; a fin de cerciorarse de que se trata de la persona que se necesita o que se busca.[43]

Y por lo citado se puede decir que los sistemas de identificación digital o electrónica, son aquel conjunto de acciones, procedimientos digitales que mediante el uso de herramientas o de sistemas digitales por medio de un sistema informático con una base de datos previamente obtenida directamente del usuario y que logran verificar la identidad de una persona. Deduciendo que, serán todos aquellos que utilicen los sistemas informáticos existentes para lograr mediante la automatización de los procesos identificar a las personas.

En el mismo orden de ideas, se ha incrementado considerablemente el uso de dispositivos móviles que cuentan con estas tecnologías de identificación de los individuos, por lo que, se puede hablar de una existencia mayor de usuarios dentro de las bases de datos de los sistemas identificadores, como el caso de usuarios de *Google*, mismos que proporcionan directamente su biometría, y en México con el uso de aplicaciones para ingresar a la banca móvil de las instituciones financieras, que adquieren un mayor uso por su efectividad en los movimientos que anteriormente necesitaban acudir a una sucursal directamente con un documento que los identificara, credencial para votar, pasaporte, cartilla militar y demás documentos autorizados.

---

[43] TORRES CARRASCO, Katia Gesell, *Sistemas de identificación de personas,* México, Ecos Sociales, 2020, número 23, p. 1216, disponible en: <file:///C:/Users/Roberto%20M%20L/Downloads/4155-Texto%20del%20art%C3%ADculo-22274-1-10-20201127.pdf> [Consulta: 21-septiembre-2021].

II.1.2. LOS SISTEMAS BIOMÉTRICOS Y LA IDENTIDAD

En concordancia con los apartados antes expuestos, y una vez establecidas las bases, bajo el sostenido argumento que los sistemas biométricos a través del uso de los medios informáticos pueden hacer identificable a una persona, definiendo a esta identificación como una acción de comparar los datos biométricos almacenados de una persona con otros que se capturan en el instante, y automáticamente se certifique o autentifique que efectivamente una persona es quien dice ser, lo anterior mediante la asignación de datos o características únicas de cada individuo, sirviendo lo anterior para que no se presente documentación física que provea la autentificación.

En beneficio las personas registradas o cuyos datos biométricos se almacenan en la base de datos de una organización gubernamental o ente privado, una vez identificados es que pueden celebrar diversos actos jurídicos dentro de la misma o fuera de esta organización, actos como, compraventas, contratación de servicios, adquisición de servicios, realización de operaciones crediticias, y todo lo anterior porque se sustenta en una autenticación y verificación de la identidad de la persona, sin necesidad de estar presente en un lugar específico.

Finalmente, la identificación mediante el uso de los sistemas biométricos constituye una sustitución de la identificación realizada de forma manual, presencial, y sin el alcance de la fiabilidad de un sistema informático, logrando una eficacia y mayor rapidez con la automatización de los sistemas de identidad a través de los sistemas biométricos.

II.1.3. ALCANCE JURÍDICO DE LA IDENTIFICACIÓN POR SISTEMAS BIOMÉTRICOS

Por lo antes mencionado, se debe ocupar la investigación en delimitar el alcance o rigor que tiene identificar a las personas utilizando sus datos biométricos en medios digitales, advirtiéndose que estos ya habían sido utilizados en décadas anteriores,

pero que se efectuaban de forma manual, es decir, mediante el uso de bases de datos en físico, en soporte de papel, donde podían recabarse las huellas dactilares de las personas, pero el ejercicio comparativo no era en automático ni permitía la comparación con demás datos, además que estas debían ser revisadas por un perito en la materia para ser fiables y generar convicción de la identidad, y lo novedoso es la implementación de mecanismos automatizados que almacenan los datos biométricos de las personas con un mayor número de registros y la regulación de estos.

Precisado lo anterior, las repercusiones y alcances de la identificación de las personas mediante el uso de los sistemas biométricos se equipara a una identificación como si se realizara en físico con la documentación autorizada para el fin, como: la credencias para votar, pasaporte, cartilla militar, acta de nacimiento, Clave Única de Registro de Población, además de lo previsto por el artículo 105 de la Ley General de Población vigente que establece que: "la Cédula de Identidad Ciudadana tendrá valor como medio de identificación personal ante todas las autoridades mexicanas ya sea en el país o en el extranjero, y las personas físicas y morales con domicilio en el país,"[44] adicionando que el citado artículo fue materia de reformas con publicación en el Diario Oficial de la Federación de fecha 22 julio del 1992, es decir, hipótesis normativa de hace ya 30 años, y que dicha cédula de identidad que no responde en la realidad a una forma de identificación de la población mexicana.

Actualmente, a pesar de ser una obligación de los ciudadanos mexicanos estar inscritos en el Registro Nacional de Ciudadanos y obtener su Cédula de Identidad Ciudadana, esto es, no es aplicable, porque es una realidad que escasos ciudadanos cuentan con esta, conforme al artículo 98 de la Ley General de Población.[45]

[44] *Cfr.* artículo 105 de la Ley General de Población.
[45] *Cfr*. artículo 98 de la Ley General de Población.
Los ciudadanos mexicanos tienen la obligación de inscribirse en el Registro Nacional de Ciudadanos y obtener su Cédula de Identidad Ciudadana.

En suma que la Cédula de Identidad Ciudadana considera entre los datos y elementos de identificación a algunos: “sistemas biométricos”[46] en el relativo a la huella dactilar, lo anterior en concordancia con lo dispuesto por la fracción VI del artículo 107 de la Ley General de Población, en conclusión, la identidad a través de la Cédula de Identidad Ciudadana, y al contener datos biométricos adquiere el alcance de prueba plena frente a terceros o algún órgano jurisdiccional del Estado.

Aunado a lo anterior, la Ley de Instituciones de Crédito establece en su artículo 52 que:

> Las instituciones de crédito podrán permitir el uso de la firma electrónica avanzada o cualquier otra forma de autenticación para pactar la celebración de sus operaciones y la prestación de servicios con los usuario, mediante el uso de equipos, medios electrónicos, ópticos o de cualquier otra tecnología, sistemas automatizados de procesamiento de datos y redes de telecomunicaciones, ya sean privados o públicos, y establecerán en los contratos respectivos las bases para determinar lo siguiente:
>
> I. Las operaciones y servicios cuya prestación se pacte;
>
> II. Los medios de identificación del usuario y las responsabilidades correspondientes a su uso;
>
> III. Los medios por los que se hagan constar la creación, transmisión, modificación o extinción de derechos y obligaciones inherentes a las operaciones y servicios de que se trate.[47]

De acuerdo con el precepto normativo en referencia, las Instituciones de Crédito dan el rigor jurídico como un medio de identificación del usuario a los sistemas

---

[46] *Cfr.* artículo de la 107 Ley General de Población.
La Cédula de Identidad Ciudadana contendrá cuando menos los siguientes datos y elementos de identificación:
[…]VI. Firma y huella dactilar.

[47] *Cfr.* artículo 52 de la Ley de Instituciones de Crédito.

biométricos, en relación a que se dota de capacidad para acreditar la identidad de las personas con cualquier forma de autenticación y que además puede servir para la celebración de las operaciones.

Siguiendo con el mismo artículo previamente mencionado, en su párrafo segundo establece que las Instituciones de Crédito podrán suspender o cancelar el trámite de operaciones que los usuarios que realicen su autenticación o celebración de operaciones mediante el uso de equipos o medios, siempre que cuenten con elementos suficientes para presumir que los medios de identificación pactados para tal efecto han sido utilizados en forma indebida, robusteciendo que se da el alcance jurídico como un medio de identificación y que se les faculta para determinar sobre la capacidad de una persona de identificarse, toda vez que se permite que dichas instituciones realicen a su juicio el dictamen de si una persona es quien dice ser o no.

Es así como la Ley de Instituciones de Crédito en el artículo 52 establece que el uso de los medios de identificación como lo son los sistemas biométricos que utilizan los usuarios a través de la aplicación o plataformas digitales de la Institución de Crédito se dotan en sustitución de la firma autógrafa, en consecuencia y el alcance jurídico es que producirá los mismos efectos que las leyes otorgan a los documentos correspondientes signados de forma autógrafa, en consecuencia, tendrán el mismo valor probatorio.

Además suman en la presente investigación las Disposiciones Generales establecen los Mecanismos de Identificación Digital y Control de Acceso que deberán observar las dependencias y entidades de la Administración Pública Federal y las empresas productivas del Estado, norma imperativa vigente publicada en el Diario Oficial de la Federación el 10 de mayo del 2018, específicamente en su disposición segunda fracción V establece que los datos biométricos: “Son aquellos rasgos físicos o biológicos de una persona física que la hacen identificable, y que estos hacen las veces de un mecanismo de identidad de las personas para

autenticar la identidad digital."[48] Es decir, es un hecho notorio que el uso de los datos biométricos en la identificación de las personas que se ha tratado de regular en la última década.

La jurisprudencia en el sistema jurídico mexicano, no aporta mayores elementos respecto del uso de los sistemas biométricos como forma de identidad de las personas, lo más cercano de la interpretación de las autoridades jurisdiccionales es la tesis asilada emitida por la Primera Sala del Máximo Tribunal del país, cuyo rubro dice: TARJETAS BANCARIAS. EL NÚMERO DE IDENTIFICACIÓN PERSONAL (NIP) MEDIANTE EL CUAL SE AUTORIZAN OPERACIONES COMERCIALES, TIENE EL CARÁCTER DE UNA FIRMA ELECTRÓNICA. Y entrando al fondo del criterio aislado se tiene que:

> El NIP, Número de Identificación Personal, que advirtiéndose no contiene datos biométricos del usuario, pero tiene similitudes al momento de ingresar a plataformas digitales o directamente en la sucursal de la institución de crédito, la gran mayoría de dichas instituciones optaron por sustituir la firma autógrafa de sus clientes, con el uso obligatorio de un número de identificación personal, y dotaron de carácter jurídico como herramienta de autenticación en las operaciones comerciales. Y en su relativo con el artículo 89 del Código de Comercio, la firma electrónica se constituye por los datos aparejados a un mensaje de datos, el cual debe entenderse como la información generada, enviada, recibida, archivada o comunicada mediante algún medio electrónico, y entre tales medios se encuentra el intercambio de información estructurada bajo

[48] *Cfr.* Disposiciones Generales que establecen los mecanismos de identificación digital y control de acceso que deberán observar las dependencias y entidades de la Administración Pública Federal y las empresas productivas del Estado.
Para los efectos de las presentes Disposiciones Generales, además de las definiciones establecidas en los artículos segundo del Decreto por el que se establece la Ventanilla Única Nacional para los Trámites e Información del Gobierno, y el Acuerdo por el que se modifican las políticas y disposiciones para la Estrategia Digital Nacional, en materia de tecnologías de la información y comunicaciones, y en la de seguridad de la información, así como el Manual Administrativo de Aplicación General en dichas materias, se entenderá por:
[…]V. Datos biométricos: son aquellos rasgos físicos o biológicos de una persona física que la hacen identificable.
[…]

alguna norma técnica o formato convenido; y que dicha información sirve para identificar al firmante, y el criterio se orienta a determinar que la naturaleza jurídica del NIP es la de una firma electrónica simple, en atención a que se trata de datos consignados, adjuntados o asociados en un mensaje de datos, los cuales sirven para identificar al firmante.[49]

Es menester precisar que, para poder implementar correctamente los sistemas de identificación digital mediante el uso de sistemas biométricos, debe existir un marco jurídico regulatorio robusto y que se adecuen a todas las medidas protectoras de los derechos humanos de los usuarios de estos servicios, toda vez que, la identidad es un derecho humano protegido por la Constitución Política de los Estados Unidos Mexicanos y el marco internacional del que el Estado mexicano forma parte.

Al consultar la resoluciones emitidas por el Pleno del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, al ingresar como datos de búsqueda las resoluciones en materia de protección de datos personales tanto en el sector público como en el sector privado, se obtiene que en el ámbito público un total de 65 registros en versión pública, de las cuales de manera directa y expresa no se refieren sobre el particular de los datos biométricos.

Se puede concluir del apartado que, la naturaleza jurídica que tiene el uso de los sistemas biométricos dentro del panorama jurídico nacional; primeramente, lo dota como una prueba plena para identificar a una persona; en segundo término, como un medio de identificación del usuario; por analogía, como datos consignados, adjuntados o asociados en un mensaje de datos, los cuales sirven para identificar al firmante; y como sustitución de la firma autógrafa, siendo que en este apartado la

[49] *Cfr. Gaceta del Semanario Judicial de la Federación, Libro 67, junio de 2019, Tomo II,* página *1029*, Décima Época, 1a. XLIX/2019 (10a.), Registro digital número 2020107. Disponible en: <https://sjf2.scjn.gob.mx/detalle/tesis/2020107> [Consulta: 22-septiembre-2021].

identidad de las personas se tendría como plenamente acreditada y autenticada por el uso de sistemas biométricos como una forma para identificar a una persona.

II.1.3.1. VALIDACIÓN DE LA IDENTIDAD DE LA PERSONA POR MEDIO DE SISTEMA BIOMÉTRICOS

Finalmente, es necesario conocer el proceso de autenticación y la validación de la identidad de una persona que se lleva a cabo para generar certeza o al menos servir de prueba para comprobar que efectivamente una persona es quien dice ser mediante el uso de sistemas biométricos.

La validación de identidad y la autenticación es un tema que se aborda por el Gobierno Mexicano en su página de blog oficial, donde se establecen que:

> Son los mecanismos de identidad digital que permiten verificar la identidad de un usuario, para tener acceso a trámite y servicios que por sus características propias así lo requieren, además estableciendo que cada institución es responsable de los mecanismos de identificación digital que se exijan para la prestación del servicio, por lo que afirman poner a disposición de la ciudadanía cuatro tipos de mecanismos de identidad legal:
>
> 1.- La autenticación con usuario y contraseña: el mecanismo sirve como uno de autenticación básica, porque requiere únicamente un nombre de usuario y contraseña, como la" Llave" utilizada en la Secretaría de Movilidad de la Ciudad de México.
>
> 2.- La autenticación con contraseña dinámica: que es un mecanismo que genera una contraseña dinámica o cambiante al usuario, es decir, que se envía o genera una contraseña por un periodo de tiempo o de un solo uso, y establece que esta contraseña dinámica es exclusiva de las personas físicas y morales que cuenten con la firma electrónica avanzada o conocida como e-firma.
>
> 3.- La autenticación con la firma electrónica avanzada: mecanismo que requiere que el usuario ingre con su firma electrónica avanzada o e-firma y la contraseña.

4.- La autenticación a través de los datos biométricos; mecanismo que exige ingresar a la persona física con su CURP y uno o más datos biométricos para verificar la identidad de las personas. [50]

En el blog de la Secretaría de Gobernación, únicamente se remiten a revisar las Disposiciones Generales que establecen los mecanismos de identificación digital y control de acceso que deberán observar las dependencias y entidades de la Administración Pública Federal y las empresas productivas del Estado, que específicamente establece en su disposición tercera los mecanismos antes precisados. [51]

Pese a que en la Ley Orgánica de la Administración Pública Federal no se establece disposición normativa alguna al respecto, y que en la legislación existe una laguna que subsanar al respecto del uso de los sistemas biométricos como una forma de identificar a las personas, las citadas disposiciones no tienen el rigor ni alcance protector que se requiere el uso de los sistemas biométricos cotidianamente tanto como mecanismos de autenticación como formas de identificación de las

---

[50] SECRETARÍA DE GOBERNACIÓN, *Conoce los mecanismos de identidad digital,* México, Blog Oficial de la Secretaría de Gobernación, 2017, número 1, disponible en: https://www.gob.mx/identidad/es/articulos/identidad-digital> [Consulta: 24-septiembre-2021].

[51] *Cfr*. Disposiciones Generales que establecen los mecanismos de identificación digital y control de acceso que deberán observar las dependencias y entidades de la Administración Pública Federal y las empresas productivas del Estado.

TERCERA. - Los niveles de autenticación relativos a los mecanismos de identificación digital son:

I. Tipo "A" o Usuario anónimo: este mecanismo no requiere de ninguna autenticación, se considera como una interacción donde el usuario mantiene secreta su identidad.

II. Tipo "B" o Autenticación con contraseña: este mecanismo requiere de una autenticación básica, la cual consta de un nombre de usuario y una contraseña proporcionada por el usuario.

III. Tipo "C" o Autenticación con contraseña dinámica: este mecanismo requiere de una contraseña que funciona mediante una clave dinámica de un solo uso, con vigencia determinada y que servirá como mecanismo de acceso en los trámites o aplicativos electrónicos de las instituciones.

IV. Tipo "D" o Autenticación con firma electrónica avanzada: este mecanismo requiere que el usuario ingrese los archivos de su firma electrónica avanzada (e-firma) y su contraseña.

V. Tipo "E" o Autenticación a través de datos biométricos: este mecanismo requiere que una persona física ingrese su CURP y uno o más datos biométricos para que se verifique la identidad de la persona por medio de un aplicativo, mediante el cual las instituciones podrán autenticar la identidad digital.

Las Instituciones deberán contar con registros de trazabilidad de las operaciones realizadas por los usuarios a través de los mecanismos de identificación digital.

personas, conduciéndose a ser una problemática para la protección, promoción, garantía y defensa de los derechos humanos.

II.2. USO DE SISTEMAS BIOMÉTRICOS COMO FORMA DE CONSENTIMIENTO EN LOS ACTOS JURÍDICOS

En este segundo apartado del capítulo segundo, se abordarán las bases de la investigación para la delimitación conceptual y su relación con el plano fáctico de la utilización de los sistemas biométricos como una forma de consentimiento en la celebración de los actos jurídicos realizados de forma electrónica o mediante el uso de medios digitales, por lo que, sería imposible que en este investigación de pretendiera estudiar de forma amplia lo relativo al acto jurídico, entonces de modo de no dejar de lado este estudio en los puntos principales se hará mención en términos generales del acto jurídico y como enfoque principal el consentimiento.

De acuerdo con la teoría general del acto jurídico, en palabras de Rojina Villegas: "El acto jurídico es una manifestación de voluntad que se hace con la intención de producir consecuencias de derecho, las cuales son reconocidas por el ordenamiento jurídico."[52] De la definición citada se debe analizar que todo acto jurídico reconoce la existencia de una manifestación de la voluntad, se habla entonces de la exteriorización de un objetivo o propósito para que se lleven a cabo acciones que en el derecho son reconocidas y con llevan consecuencias de derecho.

Una vez identificado y delimitado el acto jurídico, se deben atender a sus elementos, los cuales Rojina Villegas los enuncia en los siguientes:

1.- Una manifestación de la voluntad que puede ser expresa o tácita. Es expresa cuando se exterioriza por el lenguaje: oral, escrito o mímico. Es tácita, cuando se desprende de hechos u omisiones que de manera necesaria e indubitable revelan

[52] ROJINA VILLEGAS, Rafael, *Compendio de derecho civil, introducción, personas y familia*, México, editorial Porrúa, Vigésimo novena edición, 2000, p. 115.

un determinado propósito, aunque el autor del acto jurídico no exteriorice su voluntad a través del lenguaje.

2.- Objeto física o jurídicamente posible.

3.- El reconocimiento que haga la norma jurídica a los efectos deseados por el autor de acto.[53]

Haciéndose un principal énfasis en el primer elemento señalado, toda vez que es que el importa en lo relativo al trabajo de estudio, en función que como se precisará más adelante el uso de los sistemas biométricos se ha comparado con el de un consentimiento expreso, siendo el principal objetivo delimitar las acepciones que esto conlleva y el estado de indefensión que podría ocasionar.

II.2.1.1. ACTOS JURÍDICOS CELEBRADOS ELECTRÓNICAMENTE

La realidad contemporánea exige métodos y mecanismos más ágiles y más rápidos para la celebración de actos jurídicos, y una solución es la creación de sistemas informáticos que permiten su realización mediante dispositivos móviles con acceso a internet y desde cualquier parte del mundo, en los cuales inmediatamente pueda otorgarse un consentimiento para la celebración de los actos jurídicos. Esto se ha convertido así, en razón de que el acceso al internet y la comunicación han aumentado en los últimos años, ejemplo de ello es el comercio electrónico.

Es el caso de la celebración de actos jurídicos de manera electrónica, en el que todos los avances tecnológicos han tenido una gran influencia, a tal magnitud que para el día de hoy es normal celebrar actos jurídicos y operaciones entre personas ausentes, es decir, que no se encuentran en el mismo espacio, y como se abordará más adelante, los actos jurídicos celebrados electrónicamente son fuente de derechos y de obligaciones, se habla entonces de un verdadero rigor jurídico por el que derivado de la voluntad se actualizan efectos jurídicos que conllevan consecuencias inherentes a la misma.

[53] *Ibidem.,* p. 120.

El acto jurídico mayormente celebrado entre la población mediante medios electrónicos es el contrato, mismo que se puede definir como el acuerdo de voluntades del cual se crean o transmiten derechos y obligaciones, siendo entonces una especie de los convenios, en razón que estos últimos buscan crear, transmitir, modificar o extinguir derechos y obligaciones, es por ello que cómo la mayoría de los actos jurídicos celebrados electrónicamente son los contratos, se abordará por cuestiones de investigación desde esa línea de análisis.

Es indispensable que se distinga el procedimiento por el cual un acto jurídico se efectúa a través de plataformas digitales. Hablamos entonces de un acuerdo de voluntades, donde se realizan dos o más actos que tienen relevancia y efectos para el derecho, un ejemplo claro es que existe una página o plataforma que realiza publicaciones de objetos a la venta, como *Amazon* o *Mercado Libre*, estándose en el supuesto de una oferta al público, y por otra parte se tiene al usuario, o al comprador, que es el sujeto que puede aceptar la oferta, comprar, o decide no aceptar la oferta. Todo este procedimiento si se observa utilizando los medios digitales implica que puede ser rápido, en cambio, si esto se llevara entre presentes o en ofertas realizadas al público como periódicos o revistas no correría con la misma suerte que con la contratación electrónica. Este proceso trae como resultado que ambas partes casi simultáneamente se pongan de acuerdo, precisen sus derechos y obligaciones y surja al instante un acuerdo de voluntades.

Para Doris Oropeza el comercio electrónico es: “la compraventa o intercambio de bienes o servicios a través de medios electrónicos,”[54] como se advierte en su obra donde también cita diversos autores, pero lo coincidente y relevante para la investigación es lo relativo al uso de los sistemas biométricos, toda vez que en estas no se consideran como un elemento por el cual pueda una persona otorgar su

[54] OROPEZA, Doris, *La competencia económica en el comercio electrónico y su protección en el sistema jurídico mexicano,* México, Instituto de Investigaciones Jurídicas UNAM, 2018, p. 2, disponible en: <https://archivos.juridicas.unam.mx/www/bjv/libros/10/4667/4.pdf> [Consulta: 29-septiembre-2021].

consentimiento para la celebración de estos actos de compraventa o de intercambio de bienes o servicios.

Si bien la regulación en materia de comercio electrónico ha avanzado dentro y fuera del país, puede advertirse que no es así con el uso de los sistemas biométricos, en una realidad donde incluso dejan de utilizarse las diversas firmas electrónicas y se sustituyen por una aceptación por medio de insertar la huella digital en una pantalla, o se hace visible el rostro para corroborar la voluntad de propalar contratos, siendo entonces un tema que no se ha superado y que la legislación no incluye en el sistema jurídico.

Por lo que respecta al comercio electrónico, podemos concluir que forma parte de un proceso tecnológico que como también lo considera Doris Oropeza debe ser estudiado como: "Una actividad económico-comercial única."[55] Siendo que es evidente una diferencia entre el comercio tradicional y el comercio electrónico.

Sirviendo entonces de un referente al tópico que nos ocupa la contratación que se efectúa por medios electrónicos, pero no siendo así el tema medular de esta investigación, toda vez que la distinción surge a partir de que se consideran a los sistemas biométricos como una forma de expresión de la voluntad expresa, es decir, como si la voluntad surgiera de manera inequívoca e indubitable del lenguaje.

II.2.1.1.1. EQUIPARACIÓN DE CONSENTIMIENTO EXPRESO Y DIVERSOS MEDIOS DIGITALES

En concordancia con lo anterior, si bien el sistema jurídico mexicano no contempla expresamente el uso de los sistemas biométricos como una forma de otorgar el consentimiento para los actos jurídicos hay normatividad que permite su uso, sin que ello implique que estén limitados y regulados expresamente y de forma correcta, lo anterior es así porque como se ha estudiado su uso implica una comodidad y agilidad frente a la realización de los actos jurídicos.

[55] *Ibidem.,* p. 3.

El referente más cercano y general es el Código Civil Federal que en su artículo 1803, en lo relativo al consentimiento, se establece que: “este puede ser expreso o tácito, y que conforme a su fracción I este será expreso cuando la voluntad se manifiesta verbalmente, por escrito, por medios electrónicos, ópticos o por cualquier otra tecnología, o por signos inequívocos,” [56] sin que necesariamente se mencionen a los sistemas biométricos pero sí que se deje la posibilidad de que estos se encuentren dentro de este supuesto normativo.

Entonces partiendo de un método inductivo, dentro de la legislación mexicana se contempla o se infiere el uso artificioso que se ve de los sistemas biométricos como una forma de manifestar la voluntad expresamente, es decir, como si se tratase de signos del lenguaje que son inequívocos y por lo tanto admiten a ser considerados como plenamente útiles como una equiparación de la manifestación de la voluntad tácitamente.

Además recordando lo dispuesto por el artículo 52 de la Ley de Instituciones de Crédito, las instituciones reguladas por el impero de esa disposición están facultadas para admitir cualquier forma de autenticación para pactar la celebración de sus operaciones y la prestación de servicios con el público mediante el uso de equipos, medios electrónicos, ópticos o de cualquier otra tecnología, sistemas automatizados de procesamiento de datos y redes de telecomunicaciones, ya sean privados o públicos, con la limitante que deberán establecer en los contratos respectivos las bases para su uso, es así, como el uso de los sistemas biométricos como una forma de otorgar el consentimiento para la propalación de actos jurídicos encuentra lugar dentro de la vida jurídica.

II.2.2. CELEBRACIÓN DE ACTOS JURÍDICOS EN PLATAFORMAS DIGITALES

II.2.2.1. CELEBRACIÓN DE ACTOS JURÍDICOS EN EL EXTRANJERO MEDIANTE PLATAFORMAS DIGITALES.

[56] *Cfr*. artículo 1803 del Código Civil Federal.

En virtud de lo analizado hasta este momento, aplicando el método deductivo en conjunto con el legislativo se tiene como premisa general que se admite la celebración de los actos jurídicos mediante el uso de sistemas informáticos y digitales, y es por ello que se deben precisar que ha pasado con la regulación en torno a los datos biométricos y sus implicaciones en el mundo real y actual.

Partiendo de un método comparativo a nivel internacional, en España se tiene que si bien no cuenta con una regulación específica de lo relativo al uso de sistemas biométricos como forma de otorgar el consentimiento en actos jurídicos, si cuenta con una regulación específica relativa al tema de comercio electrónico, que por analogía se puede entender en el mismo sentido, refiriéndose a la Ley de Servicios de la Sociedad de la Información y de Comercio Electrónico, donde principalmente se regula el uso de los sistemas informáticos para la celebración de actos jurídicos, específicamente de los contratos, también conocida como la Ley 34/2002,[57] que ha sido la legislación más próxima en términos de regulación de comercio electrónico.

En la Unión Europea y como lo aborda Tábata Andrea Romero: "Desde el 27 de abril de 2016, el Parlamento Europeo y del Consejo, aprobó el Reglamento (UE) 2016/679 (en adelante, RGPD) con el que se le otorga a algunos datos personales, la calidad de especiales, por concebir que dada su naturaleza, requieren de una protección particular."[58] La autora previamente citada, coincide en decir que: "el impacto y la gravedad del tratamiento de los datos biométricos, por lo que lo considera en la hipótesis del riesgo alto,"[59] por considerarse como un peligro a los derechos fundamentales, ya que a partir de su uso indebido, usurpación de identidad y demás problemáticas que se abordarán en otro capítulo, pueden

[57] *Cfr.* Ley de Servicios de la Sociedad de la Información y de Comercio Electrónico, España.
[58] ROMERO CERDÁN, Tábata Andrea, *La autenticación y verificación de la identidad a través de información biométrica como paradigma del tratamiento de datos personales en México*, Revista del Posgrado de Derecho de la UNAM, México, Ciudad de México, 27 de agosto del 2019, disponible en: http://revistaderecho.posgrado.unam.mx/index.php/rpd/article/view/85/237#toc> [Consultado: 01-octubre-2021].
[59] *Cfr., Idem.*

manifestarse su voluntad sin que ello implique se trata de algún vicio de la voluntad contemplado en la normatividad de la material o en la doctrina.

II.2.3. EL USO DE APLICACIONES Y SU ACCESO MEDIANTE SISTEMAS BIOMÉTRICOS

Los datos biométricos constituyen un nuevo paradigma de la seguridad de las personas, dejando a un lado el panorama conceptual y los procesos de verificación y autenticación, porque la categoría que les otorga la legislación mexicana es de naturaleza indubitable, esto es, que genera certeza de los actos que se celebren con su uso, y existe una tendencia del uso de esta tecnología como una fuente fiable y eficaz para realizar operaciones supuestamente seguras.

Consolidándose como una herramienta que utilizan tanto los particulares como el Estado utilizado en la forma en que los usuarios de las aplicaciones y plataformas digitales puedan manifestar su voluntad para consentir actos jurídicos, ejemplo de esto es que las instituciones de crédito piden recolectar los datos biométricos de las personas, no sólo como mecanismos de identidad sino que también como medios para manifestar su voluntad en el instante para realizar operaciones y consentir movimientos dentro las plataformas de sus instituciones.

Sustentando lo anterior, en estos tiempos no sólo se utiliza algún sistema biométrico para verificar y autenticar nuestra identidad, sino que también se pueden efectuar pagos, depositar a cuentas bancarias, generar la prestación de algún servicio, ordenar que se efectúe alguna actividad mediante el uso de plataformas o medios digitales, que sustituyen la verificación de algún biométrico de las personas en forma de consentimiento expreso de la voluntad de algún usuario.

Ejemplificando, las aplicaciones de Mercado Libre, Mercado Pago, Amazon, Pay Pal y por demás que permiten al usuario que en vez de ingresar al sistema o aplicación con una contraseña o número de identificación personal como forma de autenticar la identidad, también dentro de esta se permite la celebración de

contratación electrónica, generar servicios, con el efecto que surte una firma autógrafa al instante, y sin que ello pudiera ponerse en duda, dejando entonces en incertidumbre al usuario por todas aquellas prácticas que pudieran vulnerar la seguridad el usuario al momento de incorporar sus datos biométricos en el instante que se efectúan las transacciones

II.2.3.1. SERVICIO DE BANCA MÓVIL SOPORTADO POR SISTEMAS BIOMÉTRICOS

Las instituciones de crédito ofrecen entre sus servicios para los usuarios la posibilidad de efectuar operaciones desde sus plataformas digitales y aplicaciones, casi desde cualquier dispositivo, operaciones que en la gran mayoría de los casos refieren a la transferencia electrónica de dinero, se habla entonces del patrimonio de los usuarios, que en diversas ocasiones se ha puesto en peligro por una falta de regulación en la materia, y constantes errores y deficiencias en los sistemas que emplean, entonces resulta de gran utilidad conocer respecto de estas instituciones, su naturaleza jurídica, el marco regulatorio principal de este tipo de operaciones y como se relacionan con el tema que nos ocupa de estudio.

Lo primero que se debe realizar es delimitar el concepto de las instituciones de crédito, la definición legal se otorga en el artículo segundo de la Ley de Instituciones de Crédito que considera al servicio de banca y crédito como: “la captación de recursos del público en el mercado nacional para su colocación en el público, mediante actos causantes de pasivo directo o contingente, quedando el intermediario obligado a cubrir el principal y, en su caso, los accesorios financieros de los recursos captados.”[60]

En el mismo tenor, la definición doctrinal con la que se coincide es la de Elvia Arcelia Quintana Adriano, quien define a un banco como: “una institución que realizar operaciones de banca, es decir, es prestatario y prestamista de crédito;

[60] *Cfr.* artículo 2o. de la Ley de Instituciones de Crédito.

recibe y concentra en forma de depósitos los capitales captados para ponerlos a disposición de quienes puedan hacerlos fructificar."[61] Definición que permite entender cuáles serían los principales objetivos de un banco.

Por lo que hace a las funciones de las instituciones de crédito, en un primer lugar las instituciones de banca múltiple, conforme a los artículos 2o. y 30 de Ley de Instituciones de Crédito respectivamente consisten en:

> La captación los recursos dispersos en la economía, conjuntarlos en ahorro y canalizarlos en forma de financiamiento o créditos hacia personas físicas o morales que generen valor agregado en la economía; en un segundo lugar las instituciones de banca de desarrollo tienen como objeto fundamental facilitar el acceso al crédito y los servicios financieros a personas físicas y morales, así como proporcionarles asistencia técnica y capacitación con el fin de impulsar el desarrollo económico.[62]

Definiendo la naturaleza jurídica de las instituciones de crédito, la Ley de Instituciones de Crédito en su artículo 2o. distingue que el servicio de banco y crédito sólo podrán ser prestados por las instituciones de crédito y que estás podrán

---

[61] QUINTANA ADRIANO, Elvia Arcelia, *Marco jurídico de las finanzas,* México, Instituto de Investigaciones Jurídicas UNAM, 2018, p. 123.

[62] C*fr.* artículo 2o., de la Ley de Instituciones de Crédito.

[…] Para efectos de este artículo y del artículo 103 se entenderá que existe captación de recursos del público cuando: a) se solicite, ofrezca o promueva la obtención de fondos o recursos de persona indeterminada o mediante medios masivos de comunicación, o b) se obtengan o soliciten fondos o recursos de forma habitual o profesional. […]

Artículo 30 de la Ley de Instituciones de Crédito.

Las instituciones de banca de desarrollo son entidades de la Administración Pública Federal, con personalidad jurídica y patrimonio propios, constituidas con el carácter de sociedades nacionales de crédito, en los términos de sus correspondientes leyes orgánicas y de esta Ley.

La Secretaría de Hacienda y Crédito Público expedirá el reglamento orgánico de cada institución, en el que establecerá las bases conforme a las cuáles se regirá su organización y el funcionamiento de sus órganos.

Las instituciones de banca de desarrollo tienen como objeto fundamental facilitar el acceso al financiamiento a personas físicas y morales, así como proporcionarles asistencia técnica y capacitación en términos de sus respectivas leyes orgánicas. En el desarrollo de sus funciones las instituciones referidas deberán preservar y mantener su capital, garantizando la sustentabilidad de su operación, mediante la canalización eficiente, prudente y transparente de recursos.

ser de dos tipos: “instituciones de banca múltiple e instituciones de banca de desarrollo.”[63]

Para Elvia Arcelia Quintana, la naturaleza jurídica de la banca múltiple son: “sociedades anónimas de capital fijo constituidas de acuerdo a lo que dispone en lo relativo a la sociedad anónima la Ley General de Sociedades Mercantiles, y tendrán por objeto la prestación de servicio de banca y crédito, en términos de la Ley de Instituciones de Crédito.”[64] Y que además requieren de la autorización de la Comisión Nacional Bancaria y de Valores, por sus siglas, CNBV para operar delimitación realizada de conformidad con el artículo 8o. de la Ley de Instituciones de Crédito.

En el mismo entendido las instituciones de banca de desarrollo, son entidades de la Administración Pública Federal, con personalidad jurídica y patrimonio propios, constituidas con el carácter de sociedades nacionales de crédito, las cuales forman parte del Sistema Bancario Mexicano que atienden las actividades que el Congreso de la Unión determina, lo anterior de conformidad con los artículos 4o. y 30 de la Ley de Instituciones de Crédito.

Concepciones legales y doctrinales que en sus puntos coincidentes permiten hacer de conocimiento que son entidades totalmente reguladas y autorizadas para operar por autoridades diversas, lo que implicaría un beneficio al usuario de los servicios de banca, y más con la existencia de la Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros, por sus siglas CONDUSEF, pero atendiendo a la fenomenología y en relación con la línea de investigación puede advertirse que el uso de los sistemas biométricos como una forma de manifestación de la voluntad no está regulada.

[63] *Cfr.* artículo 2o. de la Ley de Instituciones de Crédito.
[64] *Op. cit*., QUINTANA ADRIANO, Elvia Arcelia, p. 123.

Sirviendo de un referente porque en este tenor las instituciones de crédito han operado utilizando los sistemas biométricos tanto como una forma de identificar a los usuarios, como en el manifestación de la voluntad para celebrar diversas operaciones, y en coincidencia con los datos personales el tratamiento de la biometría de las personas como datos personales sensibles, la regulación es notoriamente superada por el uso de estas tecnologías, y que son los servicios de banca móvil en los cuales principalmente se implementan.

El sustento jurídico del uso de la banca móvil, plataformas digitales o aplicaciones se encuentra en la Ley para Regular las Instituciones de Tecnología Financiera, legislación que permite a las Instituciones de Crédito operar las contrataciones electrónicas, es decir, se autoriza y regula el uso de la banca en línea así como también de las operaciones y transacciones efectuadas a través de los medios digitales, esta Ley es también conocida como la *Ley Fintech*, ley que fue publicada en el Diario Oficial de la Federación con fecha 9 de marzo de 2018.

La *Ley Fintech* o Ley para Regular las Instituciones de Tecnología Financiera tiene por objeto regular lo relativo a los servicios financieros que prestan las instituciones de tecnología financia, y también sirve como legislación orgánica de las mismas, es decir, cómo se organizan, cómo operan y cómo funcionan, resultando interesante que la legislación prevé que también son objeto de la Ley para Regular las Instituciones de Tecnología Financiera todas aquellas operaciones y servicios financieros que sean ofertados o realizados por medios innovadores,[65] presuponiendo la utilización de medios de autenticación innovadores, como es el caso de los datos biométricos.

[65] *Cfr*. artículo 1o. de la Ley para Regular las Instituciones de Tecnología Financiera.
La presente Ley es de orden público y observancia general en los Estados Unidos Mexicanos y tiene por objeto regular los servicios financieros que prestan las instituciones de tecnología financiera, así como su organización, operación y funcionamiento y los servicios financieros sujetos a alguna normatividad especial que sean ofrecidos o realizados por medios innovadores.

En el mismo orden de ideas y siguiendo la línea legislativa, para la prestación de los servicios de banca en línea se establecen ciertos principios rectores de toda la actividad que regula la Ley para Regular las Instituciones de Tecnología Financiera, los principios son:

> Inclusión e innovación financiera, promoción de la competencia, protección al consumidor, preservación de la estabilidad financiera, prevención de operaciones ilícitas y neutralidad tecnológica, mismos que deberán ser observados por las autoridades financieras y los operadores, de igual forma se establece que el máximo ente de supervisión es la Comisión Nacional Bancaria y de Valores.[66]

En el apartado de definiciones de la Ley para Regular las Instituciones de Tecnología Financiera se establecen conceptos que resultan de gran importancia para las bases teóricas de la investigación, entre ellas la de: "la infraestructura tecnológica y modelo novedoso,"[67] concepciones que predisponen a la existencia de nuevas tecnologías que permitan a las Instituciones de Tecnología Financiera utilizar y operar con nuevas formas de identificación, así como de celebración para los actos jurídicos para los fines y servicios para los que existen.

---

[66] *Cfr*. artículo 3o. de la Ley para Regular las Instituciones de Tecnología Financiera.
La supervisión del cumplimiento de lo dispuesto en esta Ley y las disposiciones que de ella emanen corresponderá a la Comisión Nacional Bancaria y de Valores y al Banco de México, en el ámbito de sus respectivas competencias, en términos de esta Ley y las demás disposiciones jurídicas aplicables.
La Comisión Nacional de Seguros y Fianzas, la Comisión Nacional del Sistema de Ahorro para el Retiro y la Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros tendrán las facultades que en el ámbito de sus respectivas competencias les confiera esta Ley y demás disposiciones jurídicas aplicables.
El Ejecutivo Federal, a través de la Secretaría de Hacienda y Crédito Público, podrá interpretar para efectos administrativos las disposiciones de esta Ley.

[67] *Cfr.* artículo 4o. de la Ley para Regular las Instituciones de Tecnología Financiera.
[…]XV. Infraestructura Tecnológica, a la infraestructura de cómputo, redes de telecomunicaciones, sistemas operativos, bases de datos, software y aplicaciones que utilizan las ITF, las sociedades autorizadas para operar con Modelos Novedosos y las entidades financieras para soportar sus operaciones. […]
XVII. Modelo Novedoso, a aquel que para la prestación de servicios financieros utilice herramientas o medios tecnológicos con modalidades distintas a las existentes en el mercado al momento en que se otorgue la autorización temporal en términos de esta Ley; […]

De igual forma, se establece en la *Ley Fintech* que la facultad para que las Autoridades Financieras emitan disposiciones para regular los procedimientos y formas de cumplimiento aparte que las que la propia ley les establece, dejando al arbitrio y ambigüedad que dichas normas podrán justificarse con simplemente aducir que no se tratan riesgos, como se deprende del artículo 7 de la ley en cita.

En el mismo orden de ideas de la aplicación de la Ley para Regular las Instituciones de Tecnología Financiera se encuentra el aspecto relativo la aceptación de los riesgos en las operaciones que se efectúen a través de los medios digitales o tecnologías aplicadas y este, pues se les exigen a las Instituciones de Tecnología Financiera que aparte de la serie de requisitos y obligaciones de la misma ley, que también deben: "tomar medidas para evitar las difusión de información falsa o engañosa, y que adicionalmente deben difundir la información que permita los clientes o usuarios identificar los riesgos de las operaciones que se celebren con ellas."[68]

Es muy importante lo precisado con anterioridad porque establece desde este momento la bases de uno de los puntos medulares de la investigación, que es el riesgo y responsabilidad de los usuarios, pues del mismo artículo antes citado se establece que ni el Gobierno Federal ni las entidades de la administración pública

[68] *Cfr.* artículo 11 de la Ley para Regular las Instituciones de Tecnología Financiera.
Para organizarse y operar como ITF se requiere obtener una autorización que será otorgada por la CNBV, previo acuerdo del Comité Interinstitucional, en términos del Capítulo I del Título III de la presente Ley.
Las ITF, además de cumplir con las obligaciones establecidas en esta Ley y en las disposiciones que de ella emanen, deberán tomar medidas para evitar que se difunda información falsa o engañosa a través de ellas. Adicionalmente, las ITF deberán difundir la información que permita a sus Clientes identificar los riesgos de las Operaciones que celebren con o a través de ellas, conforme a lo previsto en esta Ley.
Ni el Gobierno Federal ni las entidades de la administración pública paraestatal podrán responsabilizarse o garantizar los recursos de los Clientes que sean utilizados en las Operaciones que celebren con las ITF o frente a otros, así como tampoco asumir alguna responsabilidad por las obligaciones contraídas por las ITF o por algún Cliente frente a otro, en virtud de las Operaciones que celebren. Las ITF deberán señalar expresamente lo mencionado en este párrafo en sus respectivas páginas de internet, en los mensajes que muestren a través de las aplicaciones informáticas o transmitan por medios de comunicación electrónica o digital que utilicen para el ofrecimiento y realización de sus Operaciones, así como en la publicidad y los contratos que celebren con sus Clientes.

serán responsables de los riesgos que repercutan en las operaciones, de igual forman tampoco podrán garantizar los recursos de los clientes que utilicen en las operaciones que se celebren con las Instituciones de Tecnología Financiera, precepto que deja toda la responsabilidad al usuario de las tecnología novedosas, por lo que, de ninguna forma se remite expresamente la responsabilidad a la Institución y dado el riesgo que presuponen, es notorio el estado de incertidumbre en el que colocan al usuario y cliente.

Dentro de la misma legislación existe una categoría para estas Instituciones de Información Financiera y en las que destacan las Instituciones de Fondos de Pago Electrónico, cuyos servicios son los que ofrezcan al público consistentes en la emisión, administración, redención y transmisión de fondos de pago electrónico, a través de aplicaciones informáticas, interfaces, páginas de internet o cualquier otro medio de comunicación electrónica o digital, solo podrán prestarse por las personas morales autorizadas por la Comisión Nacional Bancaria y de Valores, previo acuerdo del Comité Interinstitucional, como se establece en el artículo 22 de la Ley para Regular las Instituciones de Tecnología Financiera y cuyos servicios se enlistan en la propia ley.

Los fondos de pagos electrónicos son definidos en el artículo 23 de la Ley para Regular las Instituciones de Tecnología Financiera que establece que serán aquellos fondos contabilizados o contenidos en un registro electrónico de cuentas tradicionales, por lo tanto al ingresar y obtener los servicios de banca electrónica y al estar las los registros como cuentas tradicionales al tener acceso a estos desde un dispositivo móvil o aplicación es posible realizar un pago electrónico, y finalmente dichas plataformas admiten a los datos biométricos tanto como una forma de identificación del cliente como también una forma de otorgar el consentimiento en los actos y servicios que prestan.

Finalmente, de las Instituciones de Tecnología Financiera es importante mencionar que para que puedan operar como tal, requieren obtener la autorización

ante la Comisión Nacional Bancaria y de Valores, con previo acuerdo del Comité Interinstitucional, sin que a lo largo de la Ley para Regular las Instituciones de Tecnología Financiera se advierta un mayor requisito relativo al uso de datos biométricos o ciberseguridad, por lo tanto exclusivamente se ciñe al aspecto institucional y facultativo y no operacional.

En lo relacionado a los fondos de pagos electrónico, la Comisión Nacional Bancaria y de Valores tiene la facultad de emitir disposiciones generales para preservar la estabilidad y correcto funcionamiento de la Instituciones de Tecnología Financiera, y tratándose de instituciones de fondo de pago electrónico, conjuntamente la Comisión citada y el Banco de México deben emitir conjuntamente las disposiciones de carácter general en materia de seguridad de información, el uso de medio electrónicos, ópticos o de cualquier otra tecnología, sistemas automatizados de procesamiento de datos, atribuciones que tiene conforme al artículo 48 de la Ley para Regular las Instituciones de Tecnología Financiera.

De lo expresado en el párrafo que antecede el 28 de enero del 2021 se publicaron en el Diario Oficial de la Federación, la Secretaría de Hacienda y Crédito Público, la Comisión Nacional Bancaria y de Valores y el Banco de México, emitieron las Disposiciones aplicables a las Instituciones de Fondos de Pago Electrónico a que se refiere los artículos 28, segundo párrafo; 54, primer párrafo, y 56, primer y segundo párrafos de la Ley para Regular las Instituciones de Tecnología Financiera.

Disposiciones regulatorias de la *Ley Fintech* que permiten celebrar actos jurídicos mediante los denominados por la propia ley como canales de instrucción, en su artículo 2 estable la facultad de estas instituciones para pactar la celebración de operaciones y la prestación de servicios a través de los denominados canales de Instrucción,[69] para este fin las instituciones de crédito deben requerir el

[69] *Cfr.* artículo 2o. de las Disposiciones aplicables a las Instituciones de Fondos de Pago Electrónico a que se refiere los artículos 28, segundo párrafo; 54, primer párrafo, y 56, primer y segundo párrafos de la Ley para Regular las Instituciones de Tecnología Financiera.

consentimiento expreso de los clientes o usuarios de estos servicios de banca móvil, consentimiento expreso que se puede obtener mediante un proceso de autenticación, proceso que se remite al estudio del artículo 7.[70]

El proceso de autenticación refiere que las instituciones de crédito o denominadas por la propia ley como instituciones de fondos de pago electrónico deberán recabar y validar, lo siguiente:

I. El Identificador de Cliente y;
II. Un Factor de Autenticación.

En el sentido que establece que el denominado Identificador de Cliente deberá ser único para cada cliente y deberá asociarse a todas las Operaciones realizadas por el usuario.

De igual forma establece la obligación de las Instituciones de Crédito de guardar evidencia de la autenticación, a lo que se remite al artículo 29, fracción IV de las Disposiciones de la Ley para Regular las Instituciones de Tecnología Financiera en cita, donde mandata la creación de registros que permitan vigilar, auditar y rastrear los accesos y actividades realizadas por los usuarios, en el entendido que los registros deben cumplir con prerrogativas que son:

a) Fecha, hora, minuto y segundo de las actividades realizadas por los clientes.
b) Números de las cuentas involucradas en la operación.
c) Datos de identificación del canal de instrucción utilizado por el cliente o por quien haya usado el medio de disposición respectivo para realizar la operación de que se trate, así como los factores de autenticación utilizados para su instrucción.

Las instituciones de fondos de pago electrónico, al pactar la celebración de Operaciones y la prestación de servicios a través de Canales de Instrucción, deberán requerir el consentimiento expreso de sus Clientes para dichos efectos, el cual se podrá obtener a través del proceso de Autenticación referido en el artículo 7 de las presentes Disposiciones. Adicionalmente, las instituciones de fondos de pago electrónico deberán: […]

[70] *Cfr.* artículo 7o. de las Disposiciones aplicables a las Instituciones de Fondos de Pago Electrónico a que se refiere los artículos 28, segundo párrafo; 54, primer párrafo, y 56, primer y segundo párrafos de la Ley para Regular las Instituciones de Tecnología Financiera.

d) Direcciones de los protocolos de Internet o similares, es decir, el número de la línea de teléfono o demás datos, de acuerdo con el canal de instrucción utilizado por el cliente o usuario del medio de disposición.

Ahora bien, esa información generada por los registros deberá ser almacenada de forma segura por un periodo mínimo de 180 días naturales a partir de su generación, mediante mecanismos previamente determinados para evitar su alteración, así como mantener procedimientos de control interno para su acceso y disponibilidad.

También se establece que la información deberá ser proporcionada a los clientes o usuarios del medio de disposición que así lo requieran expresamente a la institución de fondos de pago electrónico mediante sus canales de atención al cliente, en un plazo que no exceda de 10 días hábiles, siempre que se trate de operaciones realizadas en las propias cuentas de los clientes o usuarios del medio de disposición durante los ciento ochenta días naturales previos al requerimiento de la información de que se trate.

En suma, deviene de importante para esta investigación conocer los requisitos que establece la legislación para las instituciones de crédito o denominadas por las disposiciones de la Ley para Regular las Instituciones de Tecnología Financiera, lo siguientes requisitos: primero, que se cuente con una contratación entre la institución de crédito y el cliente de manera clara y precisa, que tipo de operaciones y servicios que podrán realizar y proporcionar a través de dichos canales de instrucción, los procedimientos para la autenticación y las responsabilidades respecto de la celebración de operaciones y la prestación de servicios, los mecanismos para la notificación al cliente de las operaciones realizadas y servicios prestados, los procedimientos de cancelación de la contratación de servicios y las restricciones operativas aplicables, todas celebradas a través de los denominados canales de instrucción; segundo; se debe informar a los usuarios, los términos y condiciones para el uso de los canales de instrucción; tercero, la obligación de

informar a los riesgos inherentes a la utilización de los canales de instrucción, así como hacer de su conocimiento sugerencias para prevenir la realización de actos no autorizados por ellos o cualesquier otros irregulares.

En relación con los párrafos anteriores debe precisarse que se entiende por canales de instrucción, que en el artículo 1o. de las Disposiciones referidas establece a los canales de instrucción como: “los equipos, medios electrónicos, ópticos o de cualquier otra tecnología, sistemas automatizados de procesamiento de datos y redes de telecomunicaciones que forman parte de la infraestructura tecnológica de la institución de fondos de pago electrónico de que se trate y que, a través de ellos, esta permite al cliente realizar operaciones.”[71]

Desprendiéndose de las porciones legales invocadas que se deja en un estado de completa indefensión al usuario de los servicios y operaciones efectuadas por las instituciones de tecnologías financieras, toda vez que de la simple lectura se advierte una regulación insuficiente y que no sirve de forma directa en defensa del usuario, por el contrario evidencia vulnerabilidades del uso de los canales de instrucción, reconociendo el riesgo de su uso y dejando la responsabilidad de su uso al cliente, quienes al final están inconscientes de esta regulación y responsabilidad por un beneficio de prontitud, evitar acudir a sucursales, el ahorro del tiempo y facilidad de efectuar los actos jurídicos.

Del tema que nos ocupa, el uso de los sistemas biométricos esta regulación citada no le basta para su limitación, toda vez que conforme al artículo 5o. de las Disposiciones de la Ley para Regular las Instituciones de Información Financiera, los establece como una categoría para la autenticación que deberán utilizar las instituciones de fondos de pago electrónico, limitándose a referirse que:

[71] *Cfr.* artículo 1o. de las Disposiciones aplicables a las Instituciones de Fondos de Pago Electrónico a que se refiere los artículos 28, segundo párrafo; 54, primer párrafo, y 56, primer y segundo párrafos de la Ley para Regular las Instituciones de Tecnología Financiera.

> Formarán parte de la información perteneciente a la categoría más alta de la autenticación del usuario, señalada con la fracción III, respecto de la autenticación por la información derivada de características propias del cliente, encontrándose en ellas el carácter biométrico, huellas dactilares, geometría de la mano o de la cara, patrones en iris o retina y reconocimiento de voz.[72]

Pese a lo anterior y que se considera a los sistemas biométricos como la categoría más alta de información del usuario para autenticar en la celebración de los actos jurídicos, establece que para el uso de esta información las instituciones de fondos de pago electrónico deberán contar con la previa autorización de la Comisión Nacional Bancaria y de Valores y del Banco de México y que en todo caso, se considerará que dos o más factores de autenticación son independientes si la vulneración de uno de los factores de autenticación no compromete la fiabilidad de los demás, por lo anterior, admite una duda de la fiabilidad de la información contenida dentro de los factores de autenticación.

Adicionalmente, las referidas Disposiciones de la Ley para Regular las Instituciones de Tecnología Financiera establecen que las instituciones de fondos de pago electrónico tienen la obligación de cifrar la información personal y la información sensible recibida, generada, almacenada o transmitida en la infraestructura tecnológica propia o de terceros contratados, incluyendo en el presupuesto normativo las imágenes de documentos de identificación expedidos por autoridades oficiales e información biométrica de los clientes, y en el caso de los sistemas biométricos, como se estableció en el primer capítulo de la investigación, al tener el carácter de datos personales sensibles, el artículo hace la excepción del cifrado la información relativa a las operaciones, siempre y cuando dicha información esté almacenada en tablas o repositorios distintos a los utilizados para almacenar el resto de la información personal e información sensible, y trata de subsanar el error de tratamiento de los datos personales y de la protección de

[72] *Cfr.* artículo 5o. de las Disposiciones aplicables a las Instituciones de Fondos de Pago Electrónico a que se refiere los artículos 28, segundo párrafo; 54, primer párrafo, y 56, primer y segundo párrafos de la Ley para Regular las Instituciones de Tecnología Financiera.

los derechos de acceso, rectificación, cancelación y oposición, estableciendo que estos podrán ser tratados siempre que se cuente con mecanismos de seguridad que permitan su disociación y eviten el acceso a dicha información, en caso de no estar autorizado para ello.

Así mismo, refiere la existencia de mecanismos y procedimientos para cifrar la información referida en el párrafo anterior, por lo se incorpora el uso de las claves criptográficas, la cuales conforme al artículo precitado deberán estar bajo el control exclusivo del oficial en jefe de seguridad de la información de la institución de fondos de pago electrónico de que se trate, mecanismo que en nada beneficia al usuario y tampoco a la facultad del Estado para regular los actos celebrados entre los particulares, porque ello no implica una verificación de seguridad por las autoridades competentes de regular las instituciones de crédito, es el caso que se deja fuera del poder de vigilancia y protección a la Comisión Nacional Bancaria y de Valores y al Banco de México, dejando claro que las Disposiciones de la Ley para Regular las Instituciones de Tecnología Financiera exclusivamente atiente los intereses de las instituciones de crédito.

En concordancia con lo anterior, lo único que establece la Ley para Regular las Instituciones de Tecnología Financiera y sus Disposiciones en lo relativo al uso de los sistemas biométricos y su vigilancia o autorización de la Comisión Nacional Bancaria y de Valores y del Banco de México es en términos del artículo 44 de las Disposiciones de la Ley para Regular las Instituciones de Tecnología Financiera:

> La contratación de la prestación de servicios con terceros que presten servicios que impliquen la transmisión, almacenamiento, procesamiento, resguardo o custodia de información personal o información sensible, imágenes de documentos de identificación expedidos por autoridades oficiales o información biométrica de los clientes, en el caso que el tercero tenga privilegios de acceso

para conocer dicha información o la información de configuración de seguridad, o bien, a la administración de control de accesos.[73]

Dejando de lado los derechos inherentes a los datos personales, específicamente de la Ley Federal de Protección de Datos Personales en Posesión de Particulares.

En la misma línea de omisión regulatoria protectora de derechos humanos, las Disposiciones de la Ley para Regular las Instituciones de Tecnología Financiera en su anexo 3 establecen la forma en que se tramitan los incidentes en materia de seguridad de la información, estableciendo la posibilidad de una vulnerabilidad de la seguridad informática de las instituciones de pago electrónico, mecanismos que no colman una posible violación de los derechos del usuario, toda vez que no se brinda una solución, procedimiento o mecanismo que permita al titular de dicha información ejercer los derechos de acceso, rectificación, cancelación y oposición respecto de sus datos personales sensibles, además de poner en discusión la vulnerabilidad y por ende la fiabilidad del uso de los sistemas biométricos como una forma de otorgar el consentimiento para la celebración de actos jurídicos.

En el apartado del uso de los sistemas biométricos en los servicios y operaciones entre las instituciones de crédito, y de pago electrónico, desde la realidad de los usuarios se destacan los contratos de adhesión, contratos que los usuarios suscriben en la mayoría de los casos casi sin leerlos ni mucho menos entender el sentido y repercusiones de los mismos, derivado de diversos factores como: la falta de tiempo, una creencia de confianza en la institución, contratos confusos y extensos, hechos que hacen que el usuario al momento de celebrar contratos de adhesión no revisen las cláusulas insertas, y cuanto menos el apartado del uso y responsabilidades de la banca móvil o denominado servicio de pagos electrónicos, resultando que de desconozcan los procesos de autenticación mediante el uso de

[73] *Cfr.* artículo 44 de las Disposiciones aplicables a las Instituciones de Fondos de Pago Electrónico a que se refiere los artículos 28, segundo párrafo; 54, primer párrafo, y 56, primer y segundo párrafos de la Ley para Regular las Instituciones de Tecnología Financiera.

datos personales sensibles como el caso de la biometría de las personas y los alcances de las estipulaciones a que se adhieren.

En el mismo orden de ideas, los contratos de adhesión no son susceptibles de negociación, es decir, se habla de una imposibilidad de modificar sus cláusulas, términos y condiciones de uso, por lo que el usuario se ve en la necesidad de suscribirlo, sobre todo porque en la actualidad y con diversas políticas públicas el uso de las instituciones de crédito va en aumento, dejándose de incentivar el uso y manejo de efectivo, por lo anterior es que la banca móvil y la suscripción de contratos de adhesión aumenta, resaltando que estos contratos contienen o al menos deberían contener el tratamiento de los datos personales sensibles, que en especie se actualiza, pero no en favor de los usuarios, sino en materia de transferencia de datos a terceros.

Pese a la regulación de los contratos de adhesión por las autoridades del Estado mexicano, no se atienden en un plano fáctico a las necesidades y protección de los usuarios de los servicios financieros y sistema de pagos electrónicos, por el contrario propician la falta de seguridad y protección de los mismos, toda vez que no subsanan los vacíos legales, y la voluntad no es libre por los factores inherentes a cada individuo antes descritos, y en el tema medular de la investigación deriva de la premisa que los usuarios no conocen de los alcances del uso de los sistemas biométricos tanto como una forma de identidad, como su valor como datos personales sensibles, y dentro de los procesos como una forma de autenticación y de forma de manifestar su voluntad para producir efectos dentro del ámbito del derecho.

Una vez expresado lo anterior, se debe estudiar a la Ley de Instituciones de Crédito, legislación que regula las actividades de estas instituciones que celebran los contratos de adhesión, que al caso concreto conviene precisar que uno de los requisitos para operar como institución de crédito en el territorio nacional es el establecido por el artículo 8 de la citada ley donde establece la obligación de: “contar

con la autorización del Gobierno Federal, autorización que compete otorgar discrecionalmente a la Comisión Nacional Bancaria y de Valores, previo acuerdo de su Junta de Gobierno y opinión favorable del Banco de México."[74]

Las facultades de las Instituciones de Crédito delimitadas por el artículo 46 de la misma ley y por lo que hace al uso de los sistemas biométricos puede caber en supuesto de la fracción XXVIII que deja en el entendido que también serán facultades todas las que les confiera la Secretaría de Hacienda y Crédito Público, "oyendo la opinión del Banco de México y de la Comisión Nacional Bancaria y de Valores,"[75] posibilidad que apertura un amplio catálogo de facultades entre ellas pudiendo atribuirles competencia en materia de tratamiento de datos personales e incluso de materias que no regula la propia ley.

La Ley de Instituciones de Crédito no abunda en el tópico regulatorio del uso de los sistemas biométrico tanto como forma de identidad o como forma de manifestar expresamente la voluntad del usuario, lo único que se debe resaltar por analogía es facultad que confiere el artículo 52 para permitir el uso de cualquier forma de autenticación para pactar la celebración de sus operaciones y la prestación de servicios con el público mediante el uso de equipos, medios electrónicos, ópticos o de cualquier otra tecnología, sistemas automatizados de procesamiento de datos y redes de telecomunicaciones, ya sean privados o públicos, disposición normativa que no protege los derechos de los usuarios y no establece más en su regulación, reservándose a permitir su uso sin mayor limitación, por lo que puede concluirse este apartado que la legislación de la materia en México no es suficiente, sin que se deje de lado lo dispuesto por las leyes en materia de protección de datos personales.

El uso de la biometría de las personas como datos personales que permiten la autenticación de las personas, no sólo es una problemática que remonta a la

[74] *Cfr.* artículo 8o. de la Ley de Instituciones de Crédito.
[75] *Cfr.* artículo 46 de la Ley de Instituciones de Crédito.

identidad de las personas, sino que es también un tema de certeza y seguridad en la celebración de actos jurídicos, toda vez que en diversas ocasiones y como se analizó en el capítulo se contempla la posibilidad de ingreso a las bases de datos biomédicos de los usuarios y la transferencia de los mismos, resultando en la vulnerabilidad de estos, dado que deberá equipararse al consentimiento expreso a los actos que se celebren por las Instituciones de Crédito e Instituciones de Tecnología Financiera mediante el uso de factores de autenticación incluidos los datos biométricos.

Temática que se ha abordado desde el pasado, extendiéndose desde el uso de NIP, Número de Identificación Personal, desde el cual y en conjunto con la tarjeta de crédito o débito en físico o digital pueden celebrarse actos con las instituciones de crédito, tanto pasivas como activas, y actualmente en un avance tecnológico y conociendo las vulnerabilidades y robos de identidad, las instituciones han creado contraseñas dinámicas, concebidas como números que cambian en cierto periodo de tiempo o que se proporcionan al momento de pretender realizar operaciones con las Instituciones de Crédito, porque se conocía y aceptaba la existencia de deficiencias en los sistemas informáticos, así como delitos relacionados con el tema, mismos que serán objeto de estudio de esta investigación.

Desprendiéndose en conclusión que la utilización de los sistemas biométricos de los usuarios si bien implica beneficios en rapidez, inmediatez y comodidad en la celebración de los actos jurídicos, presupone riesgos a los usuarios, y conforme a las legislaciones estudiadas estos riesgos se estipulan en perjuicio del usuario, responsabilidad que delegan al mayor interesado de la seguridad de sus datos, y que por vulneraciones en los sistemas informáticos de las Instituciones de Crédito e Instituciones de Tecnología Financiera, esta aceptación en la legislación de la responsabilidad del usuario es notoriamente violatoria a los derechos de identidad y los derechos de acceso, rectificación, cancelación y oposición, derechos fundamentales que se instituyen para su protección, promoción, defensa y garantía,

que en el plano fáctico no se actualizan derivado de falta de supervisión de las autoridades competentes para regular su uso.

II.2.4. SERVICIOS DE CERTIFICACIÓN EN MÉXICO

Hablar de celebración de actos jurídicos mediante el uso de datos biométricos y que estos se efectúen principalmente a través del comercio electrónico obliga a realizar un estudio de las firmas electrónicas en el sistema jurídico mexicano, mismo en el que actualmente hay diferentes leyes que sustentan la base jurídica de la firma electrónica, que comúnmente se utiliza en actos de comercio y para realizar cualquier trámite, ya sea entre particulares o frente al gobierno, en virtud que la firma electrónica tiene los mismos efectos jurídicos que la firma autógrafa, marco normativo que remite a consultar la Ley de Firma Electrónica Avanzada y el Código de Comercio específicamente en su Título Segundo denominado Del Comercio Electrónico.

Respecto de la Ley de la Firma Electrónica Avanzada su regulación es de interés público, y tiene como objetivo normar lo relativo a: "el uso de la firma electrónica avanzada en los actos y la expedición de certificados digitales a personas físicas, la regulación de los servicios relacionados con la firma electrónica avanzada, y la homologación de la firma electrónica avanzada con las firmas electrónicas avanzadas reguladas por otros ordenamientos legales dentro de México."[76]

La utilidad de la firma electrónica avanzada es: "signar en documentos electrónicos y, en su caso, en mensajes de datos, produciendo los mismos efectos que los presentados con firma autógrafa es decir, que se les dota del mismo valor probatorio,"[77] como si fuera un consentimiento expreso, para esto la ley exige que la firma electrónica cumpla los principios rectores de: "equivalencia funcional, autenticidad, integridad, neutralidad tecnológica, no repudio, y confidencialidad,"[78]

[76] *Cfr.* artículo 1o. de la Ley de la Firma Electrónica Avanzada.
[77] *Cfr.* artículo 7o. de la Ley de la Firma Electrónica Avanzada.
[78] *Cfr.* artículo 8o. de la Ley de la Firma Electrónica Avanzada.
Para efectos del artículo 7 de esta Ley, la firma electrónica avanzada deberá cumplir con los principios rectores siguientes:

al respecto y para que se le confiera el valor probatorio como el de una firma autógrafa la propia ley estable dos requisitos para los servidores públicos y particulares que utilicen la firma electrónica: "primero, la existencia de un certificado digital vigente, emitido u homologado en términos de la Ley de la Firma Electrónica y; segundo, que exista una clave privada, generada bajo su exclusivo control."[79]

De lo precisado en el párrafo que antecede, se advierte que es posible la celebración de actos de comercio de forma electrónica, así como celebración de actos jurídicos diversos, como son, la realización de trámites, contratación de servicios profesionales, trámites y servicios que ofrece el gobierno, por lo tanto, es viable que se efectúe la contratación y se otorgue el consentimiento mediante la firma electrónica, la cual tiene el mismo rigor jurídico que la firma autógrafa, pero no ocurre así para disposiciones del uso de datos biométricos utilizados como una forma de otorgamiento de consentimiento, y que como se observó en el primer capítulo, su uso se ha comparado con el consentimiento expreso, por lo que se llega a la conclusión que la Ley de Firma Electrónica tampoco aplica para el caso del uso de datos biométricos, toda vez que la misma además de no contener disposiciones

---

I. Equivalencia Funcional: Consiste en que la firma electrónica avanzada en un documento electrónico o en su caso, en un mensaje de datos, satisface el requisito de firma del mismo modo que la firma autógrafa en los documentos impresos;
II. Autenticidad: Consiste en que la firma electrónica avanzada en un documento electrónico o, en su caso, en un mensaje de datos, permite dar certeza de que el mismo ha sido emitido por el firmante de manera tal que su contenido le es atribuible al igual que las consecuencias jurídicas que de él deriven;
III. Integridad: Consiste en que la firma electrónica avanzada en un documento electrónico o, en su caso, en un mensaje de datos, permite dar certeza de que éste ha permanecido completo e inalterado desde su firma, con independencia de los cambios que hubiere podido sufrir el medio que lo contiene como resultado del proceso de comunicación, archivo o presentación;
IV. Neutralidad Tecnológica: Consiste en que la tecnología utilizada para la emisión de certificados digitales y para la prestación de los servicios relacionados con la firma electrónica avanzada será aplicada de modo tal que no excluya, restrinja o favorezca alguna tecnología en particular;
V. No Repudio: Consiste en que la firma electrónica avanzada contenida en documentos electrónicos garantiza la autoría e integridad del documento y que dicha firma corresponde exclusivamente al firmante, y
VI. Confidencialidad: Consiste en que la firma electrónica avanzada en un documento electrónico o, en su caso, en un mensaje de datos, garantiza que sólo pueda ser cifrado por el firmante y el receptor.

[79] *Cfr.* artículo 9o. de la Ley de la Firma Electrónica Avanzada.
Para que los sujetos obligados puedan utilizar la firma electrónica avanzada en los actos a que se refiere esta Ley deberán contar con: I. Un certificado digital vigente, emitido u homologado en términos de la presente Ley, y II. Una clave privada, generada bajo su exclusivo control.

normativas inherentes, tampoco advierte interpretación que pueda ser aplicable para el uso de los datos biométricos.

Del Código de Comercio, las disposiciones inherentes al comercio electrónico se establecen desde el artículo 89 al 114, correspondientes al Título Segundo, para efectos de la investigación resulta importante citar el rigor de la firma electrónica que se establece en términos del artículo 89 Bis, además de la presunción de que:

> Un mensaje de datos proviene del emisor si ha sido enviado; por el propio emisor, es decir, si se autenticó su identidad en el envío; usando medios de identificación, tales como claves o contraseñas del emisor, que al igual que en el tópico de los datos biométricos están sujetos a vulnerabilidad y riesgos, o que hayan sido enviados por un sistema de información programado por el emisor o en su nombre para que opere automáticamente, que de igual forma guarda relación con la investigación por los proceso automatizados que ejecutan la autenticación.[80]

En ese sentido de las dos legislaciones en cita se advierte que en el caso de mensajes de datos, relacionados con actos de comercio que se realizan en el país, estos pueden firmarse electrónicamente utilizando certificados digitales que emiten las autoridades certificadoras que están subordinadas a la Autoridad Certificadora Raíz de la Secretaría de Economía, en lo relativo a firmas electrónicas y firmas electrónicas avanzadas, no siendo así la aplicabilidad para procesos de autenticación o en su caso de identificación mediante el uso de datos biométricos, pero de alguna forma pueden servir como guía para una posible regulación y tarea legislativa en materia de datos biométricos como forma de otorgar el consentimiento en la celebración de actos jurídicos mediante el uso de sistemas informáticos.

Ahora bien, lo importante es lo relativo a los prestadores de servicios de certificación, mismos que por la estrecha relación que guardan frente a la autenticación, identidad y en su caso para la celebración de actos jurídicos son

[80] *Cfr.* artículo 90 del Código de Comercio.

importantes para una visión legislativa a futuro de los datos biométricos aplicados como símil de una firma electrónica, a estos prestadores les es aplicable además de lo dispuesto por la Ley de Firma Electrónica y el Código de Comercio el Reglamento del Código de Comercio en Materia de Prestadores de Servicios de Certificación y las demás reglas a las que deberán sujetarse los Prestadores de Servicios de Certificación.

Un servicio de certificación es para la Ley de la Firma Electrónica Avanzada: "aquellos servicios relacionados con la firma electrónica avanzada y, en su caso, expedición de certificados digitales."[81] Por lo que, al ser la firma electrónica avanzada una forma de otorgar el consentimiento expreso para el momento de la celebración de actos jurídicos, y la estrecha relación que guarda el uso de los datos biométricos que en ocasiones se pretender usar y equiparar con la firma electrónica, será necesario mencionar lo relativo a los certificados digitales.

Para poder definir a los certificados digitales es necesario remitirse a la concepción de los documentos digitales que son:

> Aquellos en los cuales la información está registrada en formato electrónico, sobre un soporte electrónico, y que requiere de dispositivos informáticos para la consulta. El documento digital se concibe entonces como un medio de expresión de la voluntad con efectos de creación, modificación o extinción de derechos y obligaciones por medio de la electrónica, informática y telemática.[82]

Lo anterior en palabras de Anselma Vicente, que abundan a la investigación realizada porque una firma electrónica es un documento digital en sentido estricto, y que permite autenticar un proceso de firma o consentimiento para la celebración de actos jurídicos y que principalmente buscan generar efectos de derecho.

---

[81] *Cfr.* Artículo 2 de la Ley de la Firma Electrónica Avanzada.
[82] GÓMEZ FRÖDE, Carina y Marco Ernesto Briseño García Carrillo, coords., *Nuevos paradigmas del derecho procesal*, México, Instituto de Investigaciones Jurídicas UNAM, 2016, p. 611.

En el mismo tenor, Melecio Juárez establece que el documento electrónico es un:

> Documento cuyo soporte material es algún dispositivo electrónico o magnético, cuyo contenido está codificado mediante algún tipo de código digital que pueda ser leído, interpretado, reproducido, visualizado, que también se puede extraer o no, mediante el auxilio de detectores magnetizados o también mediante medios magnéticos sofisticados.[83]

Por lo tanto, de las dos definiciones se puede hacer un aproximado hacia la definición de los servicios de certificación, por lo que a continuación se estudiará una definición legal.

El Código Federal de Procedimientos Civiles dota de valor probatorio a todos aquellos documentos digitales que encuadran en las definiciones proporcionadas, toda vez que en el Código en cita se le da el carácter como prueba a la información generada o comunicada que conste en medios electrónicos, ópticos o en cualquier otra tecnología. Pero establece:

> Un parámetro para el momento de su valor probatorio, estudiando la fiabilidad del método en que haya sido generada, comunicada, recibida o archivada y, en su caso, si es posible atribuir a las personas obligadas el contenido de la información relativa y ser accesible para su ulterior consulta. Cuando se exija que un documento sea conservado y presentado en su forma original, ese requisito quedará satisfecho si se acredita que la información generada, comunicada, recibida o archivada por medios electrónicos, ópticos o de cualquier otra tecnología, es decir, que la información del documento se ha mantenido íntegra

[83] JUÁREZ PÉREZ, Melecio Honorio, *Análisis legal de documentos electrónicos,* México, Instituto de Investigaciones Jurídicas UNAM, número 55, enero-febrero 2020, disponible en: <https://revistas.juridicas.unam.mx/index.php/hechos-y-derechos/article/view/14360/15524> [Consulta: 21- febrero-2022].

e inalterada a partir del momento en que se generó por primera vez en su forma definitiva y ésta pueda ser accesible para su ulterior consulta.[84]

Desde este punto siendo importantes los servicios de certificación para los documentos digitales, como es el caso de las firmas electrónicas, de una metodología inductiva se puede considerar parte de la definición lo establecido por el Código Federal de Procedimientos Civiles, siendo que principalmente los servicios de certificación sirven para la conservación de los documentos digitales, es decir, autentican que el documento signado mediante la firma electrónica no ha sido alterado y que conserva las mismas características que en el momento que se firmó.

Ahora bien, es importante saber quién ofrece los servicios de certificación en México, siendo la Ley de Firma Electrónica Avanzada establece que:

Serán prestadores de los servicios de certificación las instituciones públicas, así como los notarios y corredores públicos y las personas morales de carácter privado que de acuerdo a lo establecido en el Código de Comercio sean reconocidas con tal carácter para prestar servicios relacionados con la firma electrónica avanzada y, en su caso, expedir certificados digitales.[85]

Cita que estima la posibilidad que no sólo tengan fe pública para certificar documentos digitales las autoridades identificadas, sino que también se deja en la posibilidad personas morales de carácter privado tengan a bien determinar sólo la autenticidad de los documentos.

Derivado de lo anterior, se debe remitir el estudio legislativo al artículo 95 bis 3 del Código de Comercio,[86] mismo que hace referencia al artículo 102 del mismo

[84] *Cfr.* artículo 210 A del Código Federal de Procedimientos Civiles.
[85] *Cfr.* fracción XIX del Artículo 2º de la Ley de Firma Electrónica Avanzada.
[86] Artículo 95 bis 3.- del Código de Comercio.

Código, y establece en el artículo 100 del Código de Comercio que podrán ser prestadores de servicios de certificación, previa acreditación ante la Secretaría de Economía:[87]

I. Los notarios públicos y corredores públicos;
II. Las personas morales de carácter privado, y
III. Las instituciones públicas.

Así mismo, del artículo en cita se resuelve la problemática de la fe pública que fue objeto de planteamiento anterior, porque se estiman que las facultades conferidas para expedir certificados o de prestar servicios relacionados, como la conservación de mensajes de datos, el sellado digital de tiempo, o la digitalización de documentos impresos, no conllevan fe pública por sí mismas, así, los notarios y corredores públicos podrán llevar a cabo certificaciones que impliquen o no la fe pública, en documentos en papel o mensajes de datos, párrafo del artículo 100 del Código de Comercio que fue objeto de reformas publicadas en el Diario Oficial de la Federal el 07 de abril del 2016, por lo que a pesar de ser considerados como prueba plena, no se estima como un documento indubitable o susceptible de reputarse como falso, porque sigue la naturaleza de una documental, teniendo los mismos efectos jurídicos.

Los requisitos para ser prestador de servicios de certificación son:

Primero, que las instituciones y personas identificadas en el artículo 100 del Código de Comercio hayan obtenido la acreditación de la Secretaría de Economía; segundo, deberán notificar a ésta la iniciación de la prestación de los servicios a que hayan sido autorizados, dentro de los 45 días naturales siguientes al comienzo de dicha actividad. Y conforme al artículo 100 para que puedan ser prestadores de servicios de certificación, se requiere:

En el caso de documentos digitalizados o almacenados por prestadores de servicios de certificación, se necesitará que éstos cuenten con acreditación para realizar sus actividades a que hace referencia el artículo 102 de este Código.

[87] *Cfr.* artículo 100 del Código de Comercio.

I. Contar con los elementos humanos, materiales, económicos y tecnológicos requeridos para prestar los servicios, a efecto de garantizar la seguridad de la información y su confidencialidad;

II. Contar con procedimientos definidos y específicos para la prestación de los servicios, y medidas que garanticen la seriedad de los certificados, la conservación y consulta de los registros, si es el caso;

III. Quienes operen o tengan acceso a los sistemas de certificación de los prestadores de servicios de certificación no podrán haber sido condenados por delito contra el patrimonio de las personas o que haya merecido pena privativa de la libertad, ni que por cualquier motivo hayan sido inhabilitados para el ejercicio de su profesión, para desempeñar un puesto en el servicio público, en el sistema financiero o para ejercer el comercio;

IV. Contar con fianza vigente por el monto y condiciones que se determinen en forma general en las reglas generales que al efecto se expidan por la Secretaría de Economía

V. Establecer por escrito su conformidad para ser sujeto a auditoría por parte de la Secretaría de Economía, y

VI. Registrar su certificado ante la Secretaría de Economía. [88]

Estableciendo que opera en favor del peticionario la figura de la afirmativa ficta, es decir, si la Secretaría de Economía no ha resuelto respecto a la petición del solicitante, para ser acreditado conforme al artículo 100 previamente citado, dentro de los 45 días siguientes a la presentación de la solicitud, se tendrá por concedida la acreditación. Requisitos y figura jurídica que sin lugar a dudas dejan en un estado de indefensión a las personas usuarias de los servicios de certificación.

[88] *Cfr.* artículo 102 del Código de Comercio.
Los Prestadores de Servicios de Certificación que hayan obtenido la acreditación de la Secretaría deberán notificar a ésta la iniciación de la prestación de los servicios a que hayan sido autorizados, dentro de los 45 días naturales siguientes al comienzo de dicha actividad.
[…]
B) Si la Secretaría no ha resuelto respecto a la petición del solicitante, para ser acreditado conforme al artículo 100 anterior, dentro de los 45 días siguientes a la presentación de la solicitud, se tendrá por concedida la acreditación.

Por lo que respecta a las obligaciones y responsabilidades de los prestadores de servicios de certificación se establece en el artículo 104 del Código de Comercio que deben:

> Comprobar la identidad de los solicitantes, poner a disposición del firmante los dispositivos de generación de los datos de creación y de verificación de la firma electrónica; informar de las condiciones precisas para la utilización del certificado, de sus limitaciones de uso y, en su caso, de la forma en que garantiza su posible responsabilidad; mantener un registro de certificados, a dicho registro podrá accederse por medios electrónicos, ópticos o de cualquier otra tecnología y su contenido público estará a disposición de las personas que lo soliciten, guardar confidencialidad respecto a la información que haya recibido para la prestación del servicio de certificación, asegurar las medidas para evitar la alteración de los certificados y mantener la confidencialidad de los datos en el proceso de generación de los datos de creación de la firma electrónica.[89]

Obligaciones que en ningún momento derivan su responsabilidad de la autenticidad de los documentos digitales que certifican, así como tampoco se obligan a contar con servicios de protección de sistemas de seguridad informática y cuanto menos contemplan que se les obliguen a informar el tratamiento de los datos personales que pudieran contener, así como tampoco se establece fehacientemente los casos de responsabilidad, dejando entonces al arbitrio de un contrato de prestación de servicios de certificación la responsabilidad del firmante, que es evidente transgrede los principios de proporcionalidad entre las partes y que deja en estado de incertidumbre al usuario ante los riesgos y delitos que serán precisados.

Conforme con lo precisado en los párrafos que anteceden, es necesario realizar la consulta a las Reglas Generales a las que deberán sujetarse los Prestadores de Servicios de Certificación, cuyo principal objetivo es:

[89] *Cfr.* artículo 104 del Código de Comercio.

> Abundar en las disposiciones normativas que deberán cumplir los interesados en obtener la acreditación por parte de la Secretaría de Economía para poder ser Prestadores de Servicios de Certificación y ofrecer los servicios de emisión de Certificados Digitales, Sellos Digitales de Tiempo, Conservación de Mensajes de Datos, Digitalización de Documentos en Soporte Físico, así como para actuar como Tercero Legalmente Autorizado, de acuerdo con lo establecido en el artículo 100 del Código de Comercio y la NOM-151-SCFI-2016, publicada en el Diario Oficial de la Federación el 30 de marzo de 2017.[90]

De las Reglas Generales a las que deberán sujetarse los Prestadores de Servicios de Certificación principalmente destaca lo dispuesto por su artículo 8 en el que establecen que aquellos candidatos a prestar el servicio de certificación podrán optar por tener su equipo de cómputo y comunicación, software y sistemas e infraestructura informática en uno o más centros de datos, principal y alternos, pudiendo utilizar para cualquiera de ellos, cómputo en la nube, de esto último establece ciertos requisitos que en general tratan aspectos en materia de normatividad internacional y de estandarización en normativas y procesos internacionales, sin que ello implique que los sistemas informáticos sean inviolables o que no sean susceptibles de los delitos en materia de informática que se verán en el último capítulo.

Ahora bien, en lo relativo al apartado de seguridad y protección de datos el Reglamento citado prevé que sea posible la utilización de una nube privada, es decir, que:

> Las bases de datos pueden contenerse en sistemas o infraestructura será administrada, operada y asegurada por el propio Prestador de Servicios de Certificación, así como se admite la posibilidad que la administración de la infraestructura para los servicios de emisión de Certificados Digitales,

[90] *Cfr.* artículo 1o. de las Reglas Generales a las que deberán sujetarse los Prestadores de Servicios de Certificación.

Sellos Digitales de Tiempo, Conservación de Mensajes de Datos y Digitalización de Documentos en Soporte Físico podrá realizarse a través de un tercero contratado por el Prestador de Servicios de Certificación. [91]

Dejando de establecerse requisito adicional para este rubro, ordenado que únicamente deberán los terceros dar cumplimiento con lo especificado en sus documentos de seguridad informática.

Finalmente respecto de las Reglas Generales a las que deberán sujetarse los Prestadores de Servicios de Certificación, si bien en su cuerpo normativo de 230 artículos no establece disposiciones expresas en materia del uso de datos biométricos, si hace mención y remite a la Ley Federal de Protección de Datos Personales en Posesión de Particulares, por lo tanto, a pesar que el Reglamento emplea cuestiones técnicas de la informáticas y telemática, no regula lo relativo a la inviolabilidad de los sistemas informáticos, por lo que resulta en una norma que carece de relevancia en aspectos de efectos y naturaleza jurídica para esta investigación pero que sirven de panorama para establecer las disposiciones relativas a seguridad informática y aplicabilidad de estándares internacionales en los procesos de certificación de documentos digitales.

Existe el Reglamento a la Ley de la Firma Electrónica, constante de 27 artículos, entre los cuales destacan la responsabilidad que remiten al usuario o titular del certificado digital, estableciendo que: “la Clave Privada deberá ser resguardada y controlada por el titular del Certificado Digital, en un Medio Electrónico, óptico o magnético que sea de su uso exclusivo.”[92] y también que se permite la transferencia de datos en términos de lo dispuesto por el artículo 23, en el que se facultan para que la Secretaría de Economía, el Servicio de Administración Tributaria y las demás

[91] *Cfr.* artículo 8o. fracción VII de las Reglas Generales a las que deberán sujetarse los Prestadores de Servicios de Certificación.
[92] *Cfr.* artículo 15 del Reglamento de la Ley de la Firma Electrónica.
La Clave Privada deberá ser resguardada y controlada por el titular del Certificado Digital, en un Medio Electrónico, óptico o magnético que sea de su uso exclusivo.

Autoridades Certificadoras puedan convenios de colaboración que suscriban para la prestación de Servicios relacionados con la Firma Electrónica Avanzada, es decir, que se advierte la posibilidad que los documentos digitales puedan ser certificados por dependencias con convenios con las autoridades certificadoras, sin que en la legislación se haya ordenado algún requisito o en su caso limitante para la celebración de dichos convenios, que en un punto final inciden en la seguridad de los datos proporcionados a las entidades certificadoras.

Respecto de la validez y rigor jurídico de estos documentos digitales certificados, Anselma Vicente dice que: "Se ha establecido lo que se denomina la equivalencia funcional, que instaura que los documentos digitales y firma electrónica que garanticen la integridad del documento producirán los mismos efectos que la leyes otorgan a los documentos de papel y firma autógrafa que no fueron objetados, teniendo el mismo valor probatorio."[93] Esta cita y el apartado abierto en la investigación para estudiar lo relativo a la firma electrónica y los servicios de certificación, son importantes porque pueden delimitar un punto de partida para el uso de datos biométricos como una forma de identidad y de consentimiento para la celebración de actos jurídicos, es decir, como un proceso automatizado para firmar documentos digitales.

Sin perjuicio de lo anterior, se señala que no todo es ideal dentro de los servicios de certificación puesto que actualmente hay muchas plataformas que intentan engañar a los usuarios diciendo que prestan servicios de certificación, cuando en México son pocos y delimitados los particulares que cuentan con la autorización de la Secretaría de Economía para operar como Prestadores de Servicios de Certificación, además de las diversas autoridades como el Sistema de Administración Tributaria.

[93] O*p. cit.* GÓMEZ FRÖDE, Carina y Marco Ernesto Briseño García Carrillo, coords., *Nuevos paradigmas del derecho procesal*, p. 613.

Siendo unos de los problemas más generales que plataformas y páginas pretendan dar valor a lo que denominan firmas digitales, pretendiendo dotarles de equivalencia a una firma electrónica avanzada y como una firma autógrafa a la imágenes de una firma autógrafa, actividades no reguladas que generan incertidumbre jurídica para los usuarios que acostumbran a utilizar las aplicaciones y plataformas que mediante una cuenta, un correo electrónico y en su caso hasta datos biométricos pretenden autenticar la identidad de una persona y en su caso hasta otorgar su consentimiento para la celebración de diversos actos jurídicos.

En relación con lo anterior, siendo la Firma Electrónica Avanzada certificada por un Prestador de Servicios de Certificación la única que produce efectos jurídicos y que permitiría en caso de una contienda judicial ser ofrecida como prueba y que tenga el valor probatorio como documento base de una acción o como prueba que pretenda acreditar algún hecho.

Esta firma electrónica también es susceptible de ser alterada o en su caso la cadena de bloques violada, como se analizará en el apartado de los delitos informáticos en cualquier medio tecnológico que contenga y almacene datos cabe la posibilidad de ser objeto de ataques informáticos y por consecuencia que los datos almacenados puedan ser utilizados por cualquier otra persona o en su caso se utilicen para la comisión de delitos como la usurpación de identidad.

La vulneración de los sistemas informáticos que contienen las bases de datos con firmas electrónicas avanzadas no implicaría que se tengan que dejar de utilizar, por el contrario es evidente que se han acelerado los procesos mediante el uso e implementación de servicios de línea y que permiten la automatización de los mismos.

Por otro lado, el tema toral de investigación yace en la responsabilidad y falta de regulación que perjudican en el caso de los riesgos de estos sistemas informáticos directamente a los usuarios, porque son a quienes la legislación les asume la

responsabilidad de su uso y en su caso la seguridad y vulnerabilidad de los mismos, resultando que dentro de una controversia judicial donde se incorporen documentos digitales como prueba la carga probatoria de acreditar la vulneración del mismo será del usuario y titular de la firma electrónica.

Es importante añadir a esta investigación lo relativo a la Firma Electrónica Avanzada y los Prestadores de Servicios de Certificación, porque los mismos guardan y en donde los datos biométricos se han utilizado como una forma de identificar a las personas y ejecutar los procesos de autenticación, sirven de un panorama regulatorio y de espíritu legislativo, en la inteligencia que se tiene que pensar que actualmente y como en muchas plataformas se han incorporado el uso de los datos biométricos para la firmar documentos digitales o en su caso la realización de actos jurídicos y contratación de servicios, por lo tanto resulta viable observar la legislación en materia de firmas electrónicas y como se han aplicado en la realidad en México para marcar la pauta que deberá seguir el legislador para incorporar el uso de datos biométricos como una forma de otorgar el consentimiento, es decir, como si se tratase de una firma electrónica.

También como lo considera Rosa del Carmen Rascón:

> De acuerdo con la Ley Modelo de la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional sobre Firmas Electrónicas (CNUDMI), se entiende que una firma electrónica no es solamente aquélla que dicho documento menciona como “firma numérica”, que es la basada en la criptografía de clave pública, sino que el documento busca tener un concepto más amplio de mecanismos de “firma electrónica”, en los cuales se podría cumplir con una o más funciones de firmas manuscritas que para la CNUDMI son: identificar a una persona, proporcionar certidumbre en cuanto a su participación personal en el

acto de la firma, y vincular a esa persona con el contenido de un documento, ambos supuestos se cumplen con el dato.[94]

Al respecto de la cita realizada también se menciona que el dato biométrico como forma de otorgar el consentimiento se encuentra en la Ley Modelo de la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional (UNCITRAL) sobre Firmas Electrónicas, legislación internacional que establece como:

Los principios fundamentales que rigen el comercio electrónico: la no discriminación, la neutralidad respecto de los medios técnicos y la equivalencia funcional. Ley que su objeto son generar los criterios de fiabilidad técnica para la equivalencia entre las firmas electrónicas y las firmas manuscritas, y determinar la responsabilidad del signatario, de la parte que se fía de la firma y de otros terceros que intervienen en el proceso de firma y en quienes se confía. De igual forma la Ley Modelo contiene disposiciones regulan el reconocimiento de los certificados extranjeros y las firmas electrónicas sobre la base de un principio de equivalencia sustantiva como una firma autógrafa.[95]

En relación con los dos párrafos que anteceden dentro de las:

Ciertas técnicas se basarían en la autenticación mediante un dispositivo biométrico basado en las firmas manuscritas. Con este dispositivo el firmante firmaría de forma manual utilizando un lápiz especial en una pantalla de computadora o en un bloc numérico. La firma manuscrita sería luego analizada por la computadora y almacenada como un conjunto de valores numéricos que se podrían agregar a un mensaje de datos y que el receptor podría recuperar en pantalla para autenticar la firma. Este sistema de autenticación exigiría el análisis

[94] RASCÓN CASTILLO, Rosa del Carmen, *Uso de datos biométricos como método para otorgar el consentimiento en la contratación electrónica, algunos aspectos a considerar*, México, INFOTEC Centro de Investigación e Innovación en tecnologías de la información y comunicación, 2019, p. 26.
[95] *Cfr.* artículos 1, 2, 3, 4, 5, 6, 10 y 12 Ley Modelo de la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional (UNCITRAL) sobre Firmas Electrónicas.

previo de muestras de firmas manuscritas y su almacenamiento utilizando el dispositivo biométrico. Otras técnicas entrañan el uso de números de identificación personal (NIP), versiones digitalizadas de firmas manuscritas y otros métodos, como la selección de un signo afirmativo en la pantalla electrónica mediante el ratón.[96]

Realizando el ejercicio comparativo del dato biométrico como una firma manuscrita contra una firma o incluso un proceso de autenticación entre la firma electrónica y el dato biométrico que se emplee para ese fin.

De igual forma la Ley Modelo de la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional sobre Firmas Electrónicas establece que puede utilizarse un dato biométrico como una clave privada, y lo regula en los siguientes términos: “Esa clave privada probablemente se mantendrá en una tarjeta inteligente, o se podrá acceder a ella mediante un número de identificación personal o mediante un dispositivo de identificación biométrica, por ejemplo, mediante el reconocimiento de una huella digital.”[97] De la cita se tiene al dato biométrico como si se tratase de una clave privada o contraseña, o un número de identificación personal que ya se ha utilizado en México por Instituciones de Crédito, por lo que resulta que el dato biométrico podría utilizarse con el rigor y símil de una contraseña, quedando a aspectos técnicos de ingeniería informática determinar cuál es más fiable.

Los artículos de la Ley Modelo de la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional sobre Firmas Electrónicas citados atendieron a la tarea del legislador internacional ante la evolución de las innovaciones tecnológicas para la regulación de reconocimiento de la naturaleza jurídica de las firmas electrónicas independientemente de la tecnología utilizada en los dispositivos biométricos, que de una interpretación sistemática y funcional y conforme a lo

[96] *Cfr.* artículo 33 Ley Modelo de la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional (UNCITRAL) sobre Firmas Electrónicas.
[97] *Cfr.* artículo 38 Ley Modelo de la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional (UNCITRAL) sobre Firmas Electrónicas.

expresado en el primer capítulo la investigación permiten la identificación de personas por sus características físicas únicas como su: geometría de la mano o facial; las huellas dactilares, el reconocimiento de la voz o el escáner de la retina; la utilización de números de identificación personal; la utilización de contraseñas privadas para autenticar mensajes de datos mediante una tarjeta inteligente u otro dispositivo en poder del firmante; versiones digitalizadas de firmas manuscritas.

Del presente apartado se concluye que la regulación de las Firmas Electrónicas Avanzadas y los Prestadores de Servicios de Certificación, puede servir como punto de partida para la observancia de una posible legislación del uso de datos biométricos con el mismo fin, y que ambas tendrían las mismas problemáticas en torno al derecho humano a la identidad, protección de datos y certeza jurídica en los actos que celebren con su uso, esto último porque los sistemas informáticos serán vulnerables y advierten los riesgos dentro de sus sistemas derivados de los delitos informáticos que previamente fueron objeto de análisis.

II.2.4.1. CONSTANCIA DE CONSERVACIÓN Y CERTIFICACIÓN DE FIRMAS OBTENIDAS POR SISTEMAS BIOMÉTRICOS

Como se analizó en el punto anterior, para que un documento digital pueda ser valorado como prueba plena ante una autoridad jurisdiccional o que produzca efectos de derecho, es necesario cubra con los requisitos que las legislaciones prevén en la material, y de este apartado, a manera de precisar cómo será posible que un dato biométrico pueda cubrir con los requisitos previstos se harán mención de la constancias de conservación y certificación de las firmas que se obtengan por el uso de los datos biométricos, como un proceso de autenticación e identidad de la persona que signa un documento digital.

Primero, de conformidad con el artículo 38 del Código de Comercio: “se obligan a los comerciantes a conservar los comprobantes originales de sus operaciones,”[98] pudieron ser esta conservación en formato impreso o electrónico, siempre y cuando

[98] *Cfr.* artículo 38 del Código de Comercio.

se observe lo relativo a la Norma Oficial Mexicana, NOM, aplicable, y como también señala el artículo 46 bis del Código de Comercio: “esta conservación o digitalización sostenida en medios electrónicos, ópticos o cualquier otra tecnología se deberá efectuar observando lo establecido en la Norma Oficial Mexicana sobre digitalización y conservación de mensajes de datos que para tal efecto emite la Secretaría de Economía,”[99] resultando aplicable la NOM-151-SCFI-2016, “Requisitos que deben observarse para la conservación de mensajes de datos y digitalización de documentos”, la cual cancela la NOM-151-SCFI-2002.

La NOM-151-SCFI-2016 mencionada tiene como objeto establecer los requisitos que deben observarse para la conservación de mensajes de datos y la digitalización de documentos en términos de lo dispuesto en los artículos 33, 38 y 49 del Código de Comercio: “aquellos documentos que se derivan que los mensajes de datos generados de la celebración de actos jurídicos deberán resguardarse en un repositorio que permita cumplir con los requisitos de ayudar a que el documento se mantenga íntegro y disponible para su ulterior consulta,”[100] es decir, un: “repositorio certificado.”[101]

Para la emisión de la firma electrónica avanzada, el Prestador de Servicios de Certificación o la Autoridad Certificadora, debe observar los requisitos que la normatividad aplicable señale para su operación, remitiendo se a lo que se analizó en el apartado anterior, la constancia emitida por el Prestador de Servicios de Certificación, acreditado para tales efectos, deberá observar los términos establecidos en el Apéndice Normativo A de la NOM-151-SCFI-2016 y el almacenamiento de las constancias de conservación, así como los documentos

[99] *Cfr.* artículo 46 bis del Código de Comercio.
[100] *Cfr.* artículo 1o. de la NORMA OFICIAL MEXICANA NOM-151-SCFI-2016, REQUISITOS QUE DEBEN OBSERVARSE PARA LA CONSERVACIÓN DE MENSAJES DE DATOS Y DIGITALIZACIÓN DE DOCUMENTOS (CANCELA LA NOM-151-SCFI-2002).
[101] *Cfr.* artículo 6o. de la NORMA OFICIAL MEXICANA NOM-151-SCFI-2016, REQUISITOS QUE DEBEN OBSERVARSE PARA LA CONSERVACIÓN DE MENSAJES DE DATOS Y DIGITALIZACIÓN DE DOCUMENTOS (CANCELA LA NOM-151-SCFI-2002).

digitalizados quedarán en control del usuario pudiendo contratar para su administración a terceros.

Ahora bien, de conformidad con el apéndice A de la NOM-151-SCFI-2016, para brindar seguridad respecto de la integridad del mensaje de datos se atienten a las siguientes reglas:

Primera:

La integridad será dada cuando el mensaje de datos sea cifrado usando la función hash, ya que dicha función matemática permite detectar cuándo existen alteraciones a los documentos resguardados, el *Hash* sirve en la obtención por primera vez de un sello digital de tiempo como constancia de conservación de mensajes de datos, ya que el interesado genera una solicitud de sello digital de tiempo de acuerdo al RFC 3161, empleando alguna función hash avalada por la Secretaría de Economía y el Identificador de Objeto referente a la política del Prestador de Servicios de Certificación a la que se apegará la emisión del sello digital de tiempo.[102]

Segunda, se sabe que no es importante sólo obtener un sello digital de tiempo que permita consultar posteriormente el documento, sino también es importante mantener: "la inmutabilidad del documento y esto se realiza al obtener una constancia de conservación del mismo, por lo que para la verificación de la constancia con un sello digital de tiempo contra un mensaje de datos, se obtiene del sello digital de tiempo la huella digital del documento generada con la función *hash* indicada en el sello digital de tiempo."[103]

[102] *Cfr.* artículo A.8.2 de la NORMA OFICIAL MEXICANA NOM-151-SCFI-2016.
[103] *Cfr.* artículo.8.3 NORMA OFICIAL MEXICANA NOM-151-SCFI-2016.
Verificación de la constancia con un sello digital de tiempo contra un mensaje de datos:
a) Se obtiene del sello digital de tiempo la huella digital del documento generada con la función hash indicada en el sello digital de tiempo.

De las reglas anteriores y conforme al apéndice A de la NOM-151-SCFI-2016 el procedimiento para su obtención queda de la siguiente forma cuando se obtiene por primera vez de un sello digital de tiempo como constancia de conservación de mensajes de datos; primero, genera una solicitud de sello digital de tiempo empleando alguna función hash avalada por la Secretaría de Economía y el Identificador de Objeto referente a la política del Prestador de Servicios de Certificación a la que se apegará la emisión del sello digital de tiempo; segundo, se envía la solicitud al Prestador de Servicios de Certificación a través del mecanismo previamente establecido entre el Prestador de Servicios de Certificación y el interesado; tercero, el Prestador de Servicios de Certificación valida que la longitud de la huella corresponda al algoritmo empleado en su generación y emite el sello digital; cuarto, el Prestador de Servicios de Certificación envía el sello digital de tiempo a través del mismo mecanismo por el cual recibió la solicitud; quinto finalmente el sello digital de tiempo obtenido es la evidencia de que el documento existe desde la fecha asentada en el sello digital de tiempo.

Con el sello digital es posible determinar el estado de conservación de un documento digital o un mensaje de datos, es decir, con el sello digital de tiempo es posible garantizar la integridad del documento que se conserva en sistema informático de la empresa o de un tercero.

Las reglas y directrices establecidas en la NOM 151-SCFI- 2016, consolidan el panorama general para que a través de documentos digitales que empleen el uso de datos biométricos como forma de identidad y proceso de autenticación permitan a un usuario por analogía y que el legislador prevea como los requisitos mínimos para que un contrato firmado mediante datos biométricos cumpla con los requisitos normativos asociados al proceso de conservación y los mismos tengan como resultado que el documento firmado utilizando datos biométricos pueda tener efectos en el campo del derecho, obligue a las partes signatarias y que otorgaron su consentimiento a través del uso de sus datos biométricos y que se brinde la certeza jurídica a los contratantes respecto la validez del contrato, así como la

protección de sus derechos sustantivos, porque conforme a esta investigación los datos biométricos tienen una doble acepción, como dato personal y forma de identificarse y como forma de otorgar su consentimiento para la celebración de actos jurídicos.

Por último, el certificado de conservación, así como el sello de tiempo digital son emitidos por la Prestadora de Servicios de Certificación, y ambos servicios sirven para dar certeza a los documentos firmados a través de la firma electrónica y que los mismos no han sido alterados o modificados desde el tiempo que fueron sellados, por lo que, conforme a la Ley de la Firma Electrónica, Código de Comercio y la NOM 151-SCFI- 2016.

Así como otras fuentes indirectas del derecho como la Ley Modelo de la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional sobre Firmas Electrónicas revisada en el apartado anterior todas las regulaciones han tenido como objetivo validar la certeza y brindar seguridad al usuario de estos servicios, y dejando a un lado los riesgos y vulnerabilidades de los sistemas informáticos, estos servicios permiten generar rigor jurídico a los actos celebrados digitalmente, pero esto no ocurre para el caso de los datos biométricos pero sirven de sustento para la futura labor legislativa y de igual forma para el establecimiento de mecanismos que permitan su implementación y correcta regulación a modo de beneficiar al titular de los datos.

II.2.5. DISPOSICIONES INTERNACIONALES EN MATERIA DE SISTEMAS BIOMÉTRICOS RESPECTO DEL CONSENTIMIENTO EN ACTOS JURÍDICOS.

Conforme a los anteriores apartados, y derivado de una conclusiva falta de legislación y vacíos legales dentro del sistema jurídico mexicano, en un tema actual de incorporación de los tratados internaciones en materia de derechos humanos y de desarrollo de materia de identificación de las personas en diversos países, es obligado el estudio de las diversas disposiciones internaciones, que si bien no son aplicables en el territorio mexicano, pero forman parte de un acervo jurídico que

permitirá visualizar que sucede con los sistemas jurídicos en el mundo en materia del uso de los sistemas biométricos, resultando en el análisis que se avocará este apartado y que cobra importancia como espíritu para la regulación interna.

Del estudio de la legislación internacional, se comenzará por el análisis realizado por Tábata Andrea Romero Cerdán, que en una publicación de la revista de derecho estudiando lo relativo al marco jurídico de la Unión Europea respecto al tratamiento de datos biométricos que: "[…]el 27 de abril de 2016, el Parlamento Europeo y del Consejo, aprobó el Reglamento (UE) 2016/679 con el que se le otorga a algunos datos personales, la calidad de especiales, por concebir que dada su naturaleza, requieren de una protección particular."[104]

En el entendido que el referido reglamento dota de categoría de datos personales a la biometría de las personas, lo anterior como se corrobora por el propio Reglamento General de Protección de Datos, que la misma autora cita y que efectivamente es el fundamento de la prohibición del tratamiento de los sistemas biométricos, en el tenor del artículo 9 en su numeral 1 establece que: quedan prohibidos el tratamiento de datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o las orientación sexuales de una persona física, esto en lo referente al tratamiento de categorías especiales de datos personales.

Pero en el articulado citado admite excepciones para el tratamiento de estos datos, conforme a el numeral 3 del artículo referido del Reglamento (UE) 2016/679 ordena que el tratamiento podrá hacerse cuando: su tratamiento sea realizado por un profesional sujeto a la obligación de secreto profesional, o bajo su responsabilidad, de acuerdo con el Derecho de la Unión o de los Estados miembros

[104] *Op. cit.* ROMERO CERDÁN, Tábata Andrea, *La autenticación y verificación de la identidad a través de información biométrica como paradigma del tratamiento de datos personales en México*.

o con las normas establecidas por los organismos nacionales competentes, o por cualquier otra persona sujeta también a la obligación de secreto de acuerdo con el Derecho de la Unión o de los Estados miembros o de las normas establecidas por los organismos nacionales competentes, en suma en el numeral 4 establece la facultad de los Estados parte de este reglamento la posibilidad de legislar con respecto al tratamiento de datos genéticos, datos biométricos o datos relativos a la salud, por lo que se admiten regulaciones internas de cada país.

Del citado Reglamento de Protección de Datos de la Unión Europea debe aclararse que actualmente se encuentra derogado, y se sustituye por el actualmente vigente Reglamento (UE) 2016/679 del parlamento europeo y del consejo de 27 de abril de 2016 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,"[105] pero con la concordancia en los artículos citados en cuanto a la hipótesis normativa y toda vez que no presentan cambios en los mismos no será necesario realizar las citas correspondientes.

Del estudio de las regulaciones internas de algunos Estados miembros de la Unión Europea, se encuentran adelantados en materia de regulación de los sistemas biométricos España, que con la Agencia Española de Protección de Datos es de los países con un mayor acervo legislativo y protector en materia de protección de datos, entre las cuales se encuentran al ser parte de la Unión Europea el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas en lo que respecta al tratamiento de datos personales y el tratamiento estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos), y de las legislación interna la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y

[105] REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016 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 (Reglamento general de protección de datos), disponible en: <https://www.boe.es/doue/2016/119/L00001-00088.pdf> [Consulta: 10 -noviembre-2021].

garantía de los derechos digitales; el Real Decreto 389/2021, de 1 de junio, por el que se aprueba el Estatuto de la Agencia Española de Protección de Datos.

En lo referente a la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, de España resalta lo ordenado por el apartado 1 del artículo 15, por cuanto a la los datos personales establece que:

> Solicitados que revelen la ideología, afiliación sindical, religión o creencias, el acceso únicamente se podrá autorizar en caso de que se contase con el consentimiento expreso y por escrito del afectado, a menos que dicho afectado hubiese hecho manifiestamente públicos los datos con anterioridad a que se solicitase el acceso. Si la información incluyese datos personales que hagan referencia al origen racial, a la salud o a la vida sexual, incluyese datos genéticos o biométricos o contuviera datos relativos a la comisión de infracciones penales o administrativas que no conllevasen la amonestación pública al infractor, el acceso solo se podrá autorizar en caso de que se cuente con el consentimiento expreso del afectado o si aquel estuviera amparado por una norma con rango de ley.[106]

Lo anterior dentro del sistema jurídico español, y en la misma línea legislativa de la Unión Europea, con el punto destacable que para el caso de los datos biométricos de las persones se requiere de una autorización expresa del usuario para permitir su tratamiento, rango que sirve para su protección y garantizar los derechos de los titulares de los datos, sirviendo de referencia para una posible aplicación legislativa en el sistema jurídico mexicano.

Regresando a sistemas jurídicos más cercanos a nuestro país, se debe mencionar a la Red Iberoamericana de Protección de Datos, por sus siglas RIPD, la normatividad establece entre sus objetivos el promover programas de

[106] *Idem.*

capacitación entre sus miembros, así como la información a los ciudadanos sobre el uso de sus datos personales, y de los derechos que pueden ejercer frente al manejo que se haga de los mismos, por lo que no es vinculante lo realizado de la Red Iberoamericana de Protección de Datos, toda vez que de sus objetivos y facultades no se desprende alguna que permita jurisdicción dentro de los Estados miembro.

De la Red Iberoamericana de Protección de Datos debe señalarse lo establecido por la disposición segunda de los Estándares de Protección de Datos Personales, en la que establece una definición de los datos personales sensibles, que para tal fin se consideran:

> Aquellos que se refieran a la esfera íntima de su titular, o cuya utilización indebida puedan dar origen a discriminación o conlleve un riesgo grave para éste. De manera enunciativa, se consideran sensibles los datos personales que puedan revelar aspectos como origen racial o étnico; creencias o convicciones religiosas, filosóficas y morales; afiliación sindical; opiniones políticas; datos relativos a la salud, a la vida, preferencia u orientación sexual, datos genéticos o datos biométricos dirigidos a identificar de manera unívoca a una persona física.[107]

Estándares que consideran a los datos biométricos como datos personales sensibles y por consiguiente su tratamiento como tal, y de un punto muy relevante se establece una prohibición del responsable de los datos personales a llevar a cabo tratamientos automatizados de datos personales que tengan como efecto la discriminación de los titulares por su origen racial o étnico, creencias o convicciones religiosas, filosóficas y morales, afiliación sindical opiniones políticas, datos relativos a la salud, a la vida, preferencia u orientación sexual, así como datos genéticos o

[107] RED IBEROAMERICANA DE PROTECCIÓN DE DATOS PERSONALES, *Estándares de Protección de Datos Personales*, RIPD, p. 13, disponible en: <https://www.redipd.org/sites/default/files/inline-files/Estandares_Esp_Con_logo_RIPD.pdf> [Consulta: 15-noviembre-2021].

datos biométricos, conforme a la disposición 29.4, que habla sobre un derecho de los titulares de los datos a no ser objeto de decisiones individuales automatizadas.

Así mismo del marco regulatorio antes mencionado, se dice que el titular tendrá derecho a no ser objeto de decisiones que le produzcan efectos jurídicos o le afecten de manera significativa que se basen únicamente en tratamientos automatizados destinados a evaluar, sin intervención humana, determinados aspectos personales del mismo o analizar o predecir, en particular, su rendimiento profesional, situación económica, estado de salud, preferencias sexuales, fiabilidad o comportamiento, artículo 29.1.

Sin embargo el artículo 29.2 admite una acotación a este derecho cuando esta actividad esté autorizada por el derecho interno de los Estado, o que se base en el consentimiento del titular de los datos, hipótesis normativas que se actualizan en México y por tanto no podrían ser aplicables, pero que significan un avance conceptual y protector en favor del usuario o titular, sustentando entonces un estándar que debería seguirse en los Estados Iberoamericanos.

En conclusión, el mayor avance legislativo en materia del uso de sistemas biométricos, es en los países conformantes de la Unión Europea, por la aplicabilidad del Reglamento (UE) 2016/679 del parlamento europeo y del consejo de 27 de abril de 2016 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, por ser de aplicación para todos los países miembro, y resaltando el caso de España que dentro de su legislación interna incorpora en el mismo sentido que la legislación internacional la protección y defensa de los datos personales de las personas incluyendo y considerando a los datos biométricos.

II.3. PROBLEMÁTICA DE LOS SISTEMAS BIOMÉTRICOS EQUIPARABLE AL CONSENTIMIENTO EXPRESO

En último lugar de este capítulo, se resaltarán las principales problemáticas que conllevan la utilización de los sistemas biométricos tanto como una forma de autenticación que permiten a una persona identificarse y celebrar actos jurídicos como una forma equiparable al otorgamiento del consentimiento expreso, por lo que en este apartado se abordarán los principales riesgos que implican su uso para los usuarios, así como de forma general se mencionarán los riesgos del uso de los sistemas informáticos que contienen almacenados los datos biométricos de los usuarios.

El consentimiento expreso se define por el artículo 1803 del Código Civil Federal como: “aquel en el que la voluntad se manifiesta verbalmente, por escrito, por medios electrónicos, ópticos o por cualquier otra tecnología, o por signos inequívocos,”[108] definición que posibilita la adecuación a la hipótesis normativa de cualquier forma o medio que permita saber que una persona otorgue su voluntad para celebrar un acto jurídico, acepción que advierte la utilización de diversos sistemas informáticos que logran manifestar la voluntad de una persona.

Las aplicaciones o plataformas electrónicas que permiten consentir los actos jurídicos mediante el uso de botones o enlaces que sostienen que una persona está manifestado su voluntad para celebrar y producir efectos de derecho, con el uso de los datos biométricos, incluso se puede concebir como una forma más segura o con mayores datos que pueden corroborar que efectivamente una persona desea manifestar su voluntad.

Por lo tanto, en términos generales su uso no es novedoso, pero hasta cierto modo se puede decir que generan un mayor sentimiento de seguridad en el usuario, por el respaldo de las bases de datos con su biometría, sentimiento que dista de la realidad de la seguridad de los sistemas informáticos, toda vez que estos al igual que una contraseña pueden ser vulnerados desde cualquier parte del mundo.

[108] *Cfr.* artículo 1803 del Código Civil Federal.

Luego entonces, la interrogante es si realmente existe una manifestación expresa de la voluntad cuando se confirma o autentica la identidad de una persona mediante el uso de sistemas informáticos automatizados utilizando los datos biométricos de las personas, para la legislación mexicana sí, como se observó en el desarrollo del capitulado este se equipara al consentimiento expreso, es decir, que no admiten signos equívocos o dubitables, pero no se toman en consideración las vulnerabilidades que la propia legislación contempla, por lo que esta problemática concierne principalmente a la denominada ciberseguridad o seguridad cibernética, así como los medios de protección de la información contenida en bases de datos.

Problemática que se aborda por los delitos informáticos o también denominados delitos cibernéticos, que dentro de la doctrina se estudia desde la rama del Derecho Informático, definido por Julio Téllez como: "una rama de las ciencias jurídicas que contemplan a la informática como instrumento (informática jurídica) y como objeto de estudio (derecho de la informática). En función de lo anterior, es notorio que la clasificación de dicho Derecho Informático obedecerá a dos vertientes fundamentales: la informática y el derecho de la informática."[109]

Derivado de la anterior definición se debe mencionar que existe una reiterada relación del Derecho con la informática, y de igual forma se deben atender para estas problemáticas como el uso de los sistemas biométricos en diversas disciplinas, como la biología, la genética, la medicina, la informática, y demás ramas de la ciencia que comprenden en alguno de sus ámbitos a los sistemas biométricos.

El tema y problemática que nos ocupa será motivo de estudio de capítulo final, del que deberán abordarse los principales delitos informáticos, una clasificación de estos delitos para efectos de esta investigación podrían ser, las falsificaciones informáticas, los daños o modificaciones de programas o datos almacenados en los sistemas informáticos y los fraudes cometidos mediante manipulación de los sistemas en soporte físico como en computadoras.

[109] TÉLLEZ VALDÉS, Julio, *Derecho informático*, México, Cuarta Edición, Mc Graw-Hill, 1998, p. 22.

Advirtiéndose desde este momento, que existen hechos constitutivos de delitos y su existencia por sí misma contempla su adecuación a la realidad, es decir, que los ilícitos se comenten y siguen perpetuándose en nuestra sociedad, entonces el uso de medios tecnológicos o sistemas informáticos que contengan datos biométricos no están garantizados como infalibles o inviolables, por el contrario, el derecho que siempre trata de ajustarse a la realidad alcanza en sus hipótesis normativas para regular el uso de estas tecnologías, en consecuencia el riesgo de los sistemas informáticos siempre estará vigente.

Ahora bien, en un panorama hipotético de un gran avance en la seguridad informática, y más allá del uso de sistemas antivirus y consejos se seguridad extrema, como comunicaciones encriptadas, uso de firmas electrónicas avanzadas, en México se debe dar mayor importancia a regular el uso de estos sistemas biométricos, creando una regulación en específico del tema, lo anterior porque los delitos informáticos advierten una mayor diversidad de circunstancias de modo, forma, tiempo y lugar, al momento de la ejecución del ilícito, elementos que son distintos a los delitos que no involucran el uso de los medios electrónicos.

Finalmente, una vez que se han reconocido vulnerabilidades de los sistemas informáticos que contienen los datos personales sensibles como datos biométricos, convendría señalar cualquier dato que admita una posible falsificación, usurpación, error, no podría ser considerado como una forma expresa de consentimiento, dada la naturaleza jurídica de lo expreso, es decir, los signos inequívocos, ni tampoco elevarse a la categoría de prueba plena o indubitable, en un marco de protección de los derechos sustantivos, los delitos informáticos y las vulnerabilidades, así como la fiabilidad del uso de los datos biométricos de las personas como forma de consentir expresamente actos jurídicos debería ser un tema prioritario por su mayor uso en nuestra sociedad.

Por lo tanto su función, rapidez y eficacia no se pone en duda, lo que se pone en interrogante es el deber de regular en su uso, brindar una mayor certeza y seguridad en los usuarios, dado que como ha quedado precisado el consentir efectos de derecho no es un tema menor, y cuanto menos lo es la identidad de los seres humanos.

III. CAPÍTULO III DE LA PROTECCIÓN DE DATOS PERSONALES Y BASES DE DATOS DE SISTEMAS BIOMÉTRICOS.

En el tercer capítulo se abordará la temática de los datos biométricos de las personas como datos personales sensibles, en función que su tratamiento dentro del marco jurídico mexicano en los últimos años ha avanzado y son tutelados por la legislación, los datos biométricos como datos personales sensibles deben tener un tratamiento especial para su uso y dentro de la perspectiva de sistemas de autenticación, formas de identidad y una manera en que las personas manifiestan su consentimiento, resultando de gran importancia su protección y regulación como datos personales sensibles.

En este capítulo no se pretende estudiar todo lo relativo a datos personales y su protección, porque sería imposible intentarlo, pero de forma toral y en los puntos que interesan para la investigación se hace referencia y conceptualizan algunos aspectos de los datos personales.

III.1. LOS SISTEMAS BIOMÉTRICOS, USO Y DISPOSICIÓN EN BASES DE DATOS

Recordando la definición de los sistemas biométricos alcanzada en el primer capítulo del trabajo de investigación, se tiene como datos biométricos a todos aquellos rasgos físicos y conductuales que se derivan de la biología única de cada individuo, los cuales al ser medibles hacen posible que una persona se distinga del resto de las personas, y que estos rasgos a través de la tecnología y la automatización de los procesos de comparación de los datos biométricos previamente almacenados en una base de datos permiten el ejercicio comparativo en cuestión de segundos.

Definición de la que deductivamente se llegó a la premisa que los datos biométricos de las personas pueden catalogarse como datos personales sensibles,

por lo que será necesario precisar qué se entiende por un dato personal sensible y sus implicaciones en el mundo jurídico.

Comenzando la conceptualización con las definiciones legales, los datos personales en la fracción IX del artículo 3o. de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados establecen que los datos personales son: “cualquier información concerniente a una persona física identificada o identificable.”[110] Se considera que una persona es identificable cuando su identidad pueda determinarse directa o indirectamente a través de cualquier información que proporcione rasgos que permitan hacer distinguible a un individuo dentro del resto de la población.

En el misma tesitura la Ley Federal de Protección de Datos Personales en Posesión de Particulares específicamente la fracción V del artículo 3º define a los datos personales como: “cualquier información concerniente a una persona física identificada o identificable.”[111]

Por lo que de estás dos legislaciones una de carácter general y otra federal se advierte que existe una coincidencia en la definición que proporcionan, dejando un amplío concepto al incluir la palabra cualquier, que abre la posibilidad de admitir que en la hipótesis normativa encuadre toda aquella que permita a una persona identificarse o ser identificable frente a la sociedad, y en la inteligencia, los datos biométricos encuadran en ambos presupuestos normativos.

Doctrinalmente y conforme a la Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, por sus siglas INAI, los datos personales son: ”Cualquier información relativa a una persona física que la identifica o hace identificable. Es la información que nos describe, que nos da identidad, nos

[110] *Cfr.* artículo 3o. de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.
[111] *Cfr.* artículo 3o. de la Ley Federal de Protección de Datos Personales en Posesión de Particulares.

caracteriza y diferencia de otros individuos."[112] Concepto coincidente con las definiciones legales proporcionadas, y que añade la característica de describir y caracterizar a una persona del resto, que conforme a la identidad es reiterativo.

En la doctrina, para Javier Corral Jurado y Jacqueline Peschard los datos personales:

> Se refieren a toda aquella información relativa al individuo que lo identifica o lo hace identificable. Entre otras cosas, le dan identidad, lo describen, precisan su origen, edad, lugar de residencia, trayectoria académica, laboral o profesional. Además de ello, los datos personales también describen aspectos más sensibles o delicados sobre tal individuo, como es el caso de su forma de pensar, estado de salud, sus características físicas, ideología o vida sexual, entre otros. Los datos personales son necesarios para que un individuo pueda interactuar con otros o con una o más organizaciones sin que sea confundido con el resto de la colectividad y para que pueda cumplir con lo que disponen las leyes. Asimismo, hacen posible la generación de flujos de información que redunda en crecimiento económico y el mejoramiento de bienes y servicios.[113]

Concepto que adiciona cualidades a los datos personales, deduciendo que los datos personales son fundamentales para que un individuo pueda interactuar con otros individuos u organizaciones sin que sea confundido, un aspecto que como se indicó en el segundo capítulo involucra un carácter social, derecho que no se limita a la identidad, si no que abarca su aspecto más amplio que es reconocer a las personas como parte integrantes de la sociedad y de una colectividad, además que añade el flujo de información, que como se precisará más adelante corresponde a

---

[112] INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES, *Conceptos Generales de la Protección de Datos Personales*, México, INAI, volumen 1, p. 6.

[113] CORRAL JURADO, Javier y Beatriz Solís Leree, *Protección de Datos Personales, Compendio de lecturas y legislación*, México, Tiro Corto Editores, 2010, p. 10.

la transferencia de los datos personales, definición que en mucho aporta a esta investigación.

Por lo tanto, se puede aseverar que un dato personal es toda aquella información que identifica o hace identificable a una persona, en adición, a que está sólo corresponde a las personas físicas, es decir, las personas morales no cuentan con datos personales, derivado de lo establecido podemos decir que un dato biométrico es un dato personal, porque en él se contienen características únicas que pueden ser medibles y que permiten reconocer a una persona de las demás, y que en todo caso con el uso de medios tecnológicos, con las limitantes de la cantidad de personas en una base de datos o de los problemas externos para su medición nos permiten hacer identificable a una persona.

Las anteriores definiciones relacionan a los datos biométricos de las personas como datos personales, pero la clasificación de los mismos como sensibles, se realiza a partir de los siguientes conceptos, que permitirán diferenciar y clasificar a los datos biométricos como datos personales sensibles.

La primera definición de los datos personales sensibles, es la definición legal que proporciona la Ley General de la materia, en la fracción X del artículo 3º definiéndolos como:

> Aquellos que se refieran a la esfera más íntima de su titular, o cuya utilización indebida puedan dar origen a discriminación o conlleve un riesgo grave para éste. De manera enunciativa más no limitativa, se consideran sensibles los datos personales que puedan revelar aspectos como origen racial o étnico, estado de salud presente o futuro, información genética, creencias religiosas, filosóficas y morales, opiniones políticas y preferencia sexual.[114]

[114] *Cfr.* fracción X del Artículo 3 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

En el mismo sentido, el artículo 3º de la Ley Federal referida, en su fracción VI, los distingue de los datos personales como: “aquellos datos personales que afectan a la esfera más íntima de su titular, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para éste.”[115]

En particular se deja en claro que se consideran sensibles aquellos que puedan revelar aspectos como origen racial o étnico, estado de salud presente y futuro, información genética, creencias religiosas, filosóficas y morales, afiliación sindical, opiniones políticas, preferencia sexual, que de la simple lectura constituyen los mismos elementos que los de la Ley General mencionada, por lo que son similares y sus características y elementos son compartidos.

Conforme a los conceptos históricos conviene destacar lo analizado por Julio Huerta Anguiano que fundamentalmente establece que:

> El 14 de diciembre de 1990, la Asamblea General de la Organización de las Naciones Unidas (ONU) adoptó los Principios Rectores para la Reglamentación de los Ficheros Computarizados de Datos Personales de las Naciones Unidas (ONU, 1990), cuyo artículo relativo al “principio de no discriminación” estableció la prohibición de registrar datos que pudieran originar una discriminación ilícita o arbitraria, en particular información sobre el origen racial o étnico, color, vida sexual, opiniones políticas, convicciones religiosas, filosóficas o de otro tipo, o sobre la participación en una asociación o la afiliación a un sindicato. En un sentido similar, la Directiva 95/46/CE, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (Parlamento Europeo y Consejo de la Unión Europea, 1995), estableció en su artículo 8(1) que los Estados miembros debían prohibir el tratamiento de los datos personales que revelaran el origen racial o étnico, las opiniones políticas, las convicciones religiosas o filosóficas, la pertenencia a

[115] *Cfr.* fracción VI del artículo 3o. de la Ley Federal de Protección de Datos Personales en Posesión de Particulares.

sindicatos, así como el tratamiento de los datos relativos a la salud o a la sexualidad de las personas.[116]

Conceptos que interesa conocer por las fechas y especialmente porque de las definiciones contenidas se tiene un parteaguas de las principales problemáticas que conlleva el tratamiento de los datos sensibles de las personas.

La contextualización de los datos personales como sensibles corresponden a una realidad de discriminación y problemas que se pueden asociar con los propios datos personales de las personas, y conforme a las definiciones citadas del derecho positivo, al ser una disposición normativa vigente, su fin es el regular la conducta de las personas, referente a los sujetos obligados y de particulares, y la responsabilidad del tratamiento de los datos personales sensibles, constituyendo un régimen impositivo e imperativo de su tratamiento específico.

De las anteriores definiciones se desprende que las diferencias entre los datos personales y los datos personales sensibles se encuentran en el grado de afectación a la esfera íntima de privacidad de las personas, de acuerdo con las situaciones que pueden propiciar en lo presente y en lo futuro que una persona pueda sufrir discriminación por sus datos más íntimos, concepto que advierte un problema social mayor, la discriminación, por lo tanto debe considerarse a los datos personales sensibles en su sentido amplio como todos aquellos que se relacionan en la privacidad y en lo más íntimo de las personas y en su sentido social como aquellos que puede propiciar o vulnerar que se discrimine a una persona por sus propios datos personales.

En el mismo sentido la doctrina, para Huerta Anguiano considera que:

---

[116] HUERTA ANGUIANO, Julio Alberto, *Naturaleza intrínseca, "contexto" o "finalidad" en la determinación del carácter sensible de los datos personales*, en Revista del Instituto de Investigaciones Jurídicas, México, junio-diciembre 2020, p. 5, disponible en: <https://revistas.juridicas.unam.mx/index.php/derecho-informacion/article/view/14658/15717> [1-diciembre-2021]>

> La distinción entre datos personales sensibles y no sensibles es fundamental porque reconoce que el procesamiento de datos personales puede tener distintos niveles de impacto en la vida privada de las personas, así como en diversos valores protegidos por el derecho. La dicotomía presupone que el tratamiento de cierto tipo de información puede implicar riesgos y afectaciones importantes para sus derechos y libertades fundamentales. Así lo expone el autor Sabah Al-Fedaghi, para quien la sensibilidad de los datos personales es uno de los factores más importantes para determinar la percepción de privacidad de un individuo, reconociendo que el grado de sensibilidad influye en la decisión sobre el nivel de seguridad que se establece para controlar el acceso a dicha información.[117]

Definiendo entonces que, los datos personales sensibles implícitamente guardan una relación de los principios constitucionales de no discriminación, dignidad humana, derecho a la identidad, y que en sí mismos podrían encontrarse con la justificación de clasificar a los datos personales como sensibles o no, elemento que podría ser considerado como subjetivo y que el carácter imperativo normativo permite que se actualice la hipótesis normativa de ser tratados como sensibles.

Por lo que el legislador mexicano decide otorgarle esta categoría y con ello una mayor tutela, pero podría advertirse una laguna interpretativa, toda vez que puede entenderse que cada persona define cuáles serán sus datos personales sensibles, y en este tenor presuponen la existencia de problemáticas interpretativas del concepto.

Una de las problemáticas en torno a la materia es que las hipótesis normativas admiten supuestos normativos amplios, como todo aquél que puede afectar en lo presente o en el futuro la esfera jurídica más íntima de las personas, primer problema interpretativo que presupone el conocimiento y delimitación de la esfera jurídica íntima de las personas, como privacidad, el segundo problema interpretativo

[117] *Ibidem.* p. 3.

surge que los datos sensibles supongan una discriminación, problemática que hace las definiciones pueden ser interpretadas de múltiples formas.

Si bien el interés del legislador fue dotar de una mayor protección a los datos personales sensibles, establece un problema que por sí sólo no crea un estado de inseguridad y vacío jurídico, pero si hace complicada la labor interpretativa y de encuadrar los datos personales con la categoría de sensibles.

Precisado lo anterior, así como la dicotomía entre los datos personales sensibles o los no sensibles, en términos de este trabajo y con las interpretaciones más favorables a las personas como derecho humano, los biométricos son datos personales sensibles, porque forman parte de la persona, es decir, son parte integrante de la naturaleza del ser humano, el iris, la geometría de la mano, la huella dactilar, la cara, forma de escritura, son rasgos únicos que forman parte de la esfera más íntima de las personas, en la razón que los mismos son parte del ser humano, y derivado de ellos también podría presuponer un elemento que los pudiera colocar en discriminación por función de sus propias características físicas.

Los datos biométricos encuadran en el supuesto normativo de ser datos personales sensibles, más aún si conocemos la importancia de estos, a simple vista parecieran como un rasgo o particularidad de cada individuo, pero con la tecnología y como forma de identidad, proceso de autenticación de la identidad, se comprende su necesidad de incluirlos como parte de la esfera íntima de las personas, además que en algún momento pueden ser utilizados para discriminar a las personas, recordando lo estudiado en el primer capítulo y relacionándolo con este apartado, conclusivamente por su importancia y su relación directa como datos personales de las personas son datos sensibles, y de ahí su importancia de ser protegidos con esa cualidad.

Continuando la línea argumentativa y conforme a la premisa que los datos biométricos son datos personales sensibles, bajo el método deductivo se infiere que

si bien en el sistema jurídico no existe una regulación directa o específica respecto del uso de los datos biométricos.

Para el caso de los datos personales sensibles no ocurre así, en virtud que además de la Ley General y de la Ley Federal, en cada entidad federativa se cuenta con regulación al respecto, por lo anterior conforme a la metodología se señala que contrario a la regulación para el uso de los datos biométricos como un proceso de autenticación o inclusive como una forma de identidad que no está regulado, si lo está para el caso de datos personales.

Por lo anterior, y conforme al acervo legislativo en materia de datos personales sensibles, se infiere que la legislación en materia de datos biométricos exclusivamente como datos personales sensibles es amplia.

Ahora bien, conforme al estudio de los datos personales sensibles se vuelve indispensable definir qué se entiende por el tratamiento de los datos, la Ley Federal de Protección de Datos Personales en Posesión de Particulares en su artículo 3o. lo define el tratamiento como a obtención, uso, divulgación o almacenamiento de datos personales, por cualquier medio.

El uso abarca cualquier acción de acceso, manejo, aprovechamiento, transferencia o disposición de datos personales, lo anterior conforme a la fracción XVIII, y en el mismo sentido la Ley General referida lo define como cualquier operación o conjunto de operaciones efectuadas mediante procedimientos manuales o automatizados aplicados a los datos personales, relacionadas con la obtención, uso, registro, organización, conservación, elaboración, utilización, comunicación, difusión, almacenamiento, posesión, acceso, manejo, aprovechamiento, divulgación, transferencia o disposición de datos personales, establecido en el artículo 3o., fracción XXXIII.

De las definiciones legales se advierten dos aspectos: el primero, que el tratamiento puede definirse como el acceso, el manejo, uso, obtención, registro, organización, elaboración, posesión, aprovechamiento, transferencia, divulgación y almacenamiento de los datos personales y; el segundo, que la Ley General citada considera este tratamiento mediante el uso de procedimientos automatizados.

El tema de los datos biométricos como datos personales sensibles abarca todo lo relativo al tratamiento, pero es limitado para el uso de los datos biométricos como forma de identidad y consentimiento para actos jurídicos, y en relación con el primer apartado, para su uso en lo relativo al tratamiento, las principales problemáticas se localizan en el uso, manejo, almacenamiento, transferencia, posesión y obtención.

Una vez que se han recabado los datos biométricos de su titular, estos pasan a ser manejados y almacenados en bases de datos del responsable, y las bases de datos por sí mismas no implicarían un problema en el tratamiento de los datos biométricos, pero las transferencias, uso, disposición, acceso y divulgación si presuponen un problema no sólo del derecho a la información, y de la protección de datos personales, sino un problema de identidad.

Las bases de datos, al ser la propia limitante para un sistema de autenticación o de automatización de reconocimiento de identidad, admiten vulneraciones de delitos informáticos, que como se precisará, las propias disposiciones normativas admiten su vulnerabilidad y realización de delitos en materia de ciberseguridad.

Las bases de datos se constituyen por los datos que permiten identificar a una persona, en consecuencia cuando se efectúa la captura de los datos biométricos con el fin de hacer a una persona identificable del resto a través de bases de datos almacenados, se encuentran en los supuestos de máximo cuidado y tratamiento específicos de estos datos sensibles, pero en el plano fáctico, en materia de datos personales tanto en posesión de sujetos obligados como de particulares, los datos

no están totalmente protegidos en lo referente a su transferencia y vulneraciones a los sistemas informáticos que contienen las bases de datos.

Derivado de las problemáticas, y en el encuadramiento de delitos cibernéticos, los datos biométricos no son completamente tutelados, en función que con el robo o manipulación de las bases, casi desde cualquier punto del mundo se podría autenticar la identidad de una persona, sin necesidad de que sea la persona misma, esto porque a pesar la existencia de grandes barreras y sistemas de seguridad de los sistemas informáticos, siguen aconteciendo problemas de certeza y seguridad en los mismos.

Problemáticas que atienden factores técnicos de ciberseguridad, cuya rama de la ciencia es la informática, y la estrecha relación con la comisión de delitos informáticos que repercuten al mundo jurídico por las implicaciones y efectos a los derechos que podrían llegar a acontecer con el mal uso de las bases de datos que contengan datos biométricos, y la regulación en ese sentido es nula o la existente no es suficiente con sus presupuestos normativos para su protección, y continúa sin resolverse la problemática que sucede con las bases de datos que contienen datos biométricos de los usuarios, y que la propia responsabilidad de su tratamiento se traslada al usuario.

III.2. TRATAMIENTO DE LOS SISTEMAS BIOMÉTRICOS COMO DATOS PERSONALES SENSIBLES

Los datos biométricos de las personas como datos personales sensibles presuponen un tratamiento especial que la propia legislación aplicable involucra, por lo que será importante precisar qué es el tratamiento de datos y qué implicaciones jurídicas protectoras trae consigo, temáticas que se cubren por la protección de datos personales.

Para Ana Garriaga Domínguez el tratamiento de datos es:

> Cualquier operación o procedimiento técnico, de carácter automatizado o no, que permita la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos, ya se produzcan éstas a través de consultas, comunicaciones, interconexiones o de transferencias. Nos permite inferir que el concepto legal de fichero en relación con el de tratamiento de datos es un concepto dinámico que no se entiende como un simple depósito de datos, sino como el conjunto de procesos y aplicaciones informáticas que se llevan a cabo con los datos registrados, susceptibles en caso de interrelación, de configurar el perfil de una persona.[118]

El Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales define que: "el tratamiento de datos personales implica la obtención, uso, divulgación o almacenamiento de datos personales. El uso de los datos personales abarca cualquier acción de acceso, manejo, aprovechamiento, transferencia, comunicación o disposición de datos personales."[119]

Para Concepción Conde Ortiz el tratamiento de los datos personales contempla:

> Las operaciones que se realizan con los datos y a efectos de la Ley se define el "tratamiento de datos" en el artículo 3.) como las "operaciones y procedimientos técnicos de carácter automatizado o no, que permitan la recogida, grabación, conservación, elaboración, modificación, bloqueo, y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias.[120]

---

[118] GARRIAGA DOMÍNGUEZ, Ana, *Tratamiento de datos personales y derechos fundamentales*, Madrid, segunda edición, editorial Dykinson, 2009, p. 74.
[119] *op.cit.* INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES, *Guía para titulares de los datos personales, Conceptos Generales de la Protección de Datos*, p.10.
[120] CONDE ORTIZ, Concepción, *La Protección de Datos Personales: Un Derecho Autónomo Con Base En Los Conceptos de Intimidad y Privacidad*, Madrid, editorial Dykinson, 2005.

Conviene hacer una mención en las definiciones legales del tratamiento de datos, en este tenor la Ley Federal referida establece al tratamiento como la obtención, uso, divulgación o almacenamiento de datos personales, por cualquier medio. El uso abarca cualquier acción de acceso, manejo, aprovechamiento, transferencia o disposición de datos personales y en el mismo sentido lo hace la Ley General anteriormente referida.

En cuanto a qué implica este tratamiento la ley hace su distinción en el sentido que se establecen los principios de: licitud, consentimiento, información, calidad, finalidad, lealtad, proporcionalidad y responsabilidad, además de lo establecido por el artículo 7 de la Ley Federal en cita mandata que en todo tratamiento de datos personales se presume que existe la expectativa razonable de privacidad, que se puede traducir como la confianza que deposita cualquier persona en otra, respecto de que los datos personales proporcionados entre ellos serán tratados conforme a lo que acordaron las partes en los términos establecidos por la legislación aplicable.

También se ordena que todo tratamiento de datos personales estará sujeto al consentimiento de su titular, que el tratamiento deberá limitarse al cumplimiento de las finalidades previstas en el aviso de privacidad.

Aunado a la obligación de todo responsable del tratamiento de datos a establecer y mantener medidas de seguridad administrativas, técnicas y físicas que permitan proteger los datos personales contra daño, pérdida, alteración, destrucción o el uso, acceso o tratamiento no autorizado.

En lo relativo a los datos personales sensibles y su tratamiento la Ley Federal de Protección de Datos en Posesión de Particulares establece que: “el responsable deberá obtener el consentimiento expreso y por escrito del titular para su tratamiento, a través de su firma autógrafa, firma electrónica, o cualquier mecanismo de autenticación que al efecto se establezca,”[121] así mismo respecto de los datos

[121] *Cfr*. artículo 9o. de la Ley Federal de Protección de Datos Personales en Posesión de Particulares.

personales sensibles existe la prohibición de crear bases de datos que contengan datos personales sensibles, sin que se justifique la creación de las mismas para finalidades legítimas, concretas y acordes con las actividades o fines explícitos que persigue el sujeto regulado, restricción que para el uso de datos biométricos en México aplica y debiera servir de limitante para las bases de datos actuales.

La antes referida protección de la Ley Federal pese a estar regulada no se aplica, toda vez actualmente las bases de datos sensibles son manejadas por particulares y su uso no se encuadra en finalidades legítimas, concretas y acordes con las actividades de las mismas, por ejemplo, *Google* y sus servidores, de igual forma diversas aplicaciones que manejan datos personales sensibles, de las cuales no se logra advertir que se traten de actividades explícitas y perfectamente limitadas que impliquen la creación y manejo de estas bases de datos, y en realidad su actividad podría seguir operando sin necesariamente tener que crear sus propias bases de datos que contienen datos biométricos de sus usuarios

Si bien la Ley General y la Ley Federal en materia de Protección de Datos hacen restricciones para el caso de los datos biométricos como datos personales sensibles, la protección no es suficientemente clara y extensa para que su uso sea controlado, en función de lo anterior, en un marco de avance y crecimiento informático la regulación se ve superada, además que la normatividad protectora positiva no es suficiente para exigir al responsable del tratamiento una mayor responsabilidad.

La protección especial a los datos sensibles también se observa en el capítulo XI de la Ley Federal citada en lo relativo a los Delitos en Materia del Tratamiento Indebido de Datos Personales que en la razón que implica una: “agravante en la

---

Tratándose de datos personales sensibles, el responsable deberá obtener el consentimiento expreso y por escrito del titular para su tratamiento, a través de su firma autógrafa, firma electrónica, o cualquier mecanismo de autenticación que al efecto se establezca.
No podrán crearse bases de datos que contengan datos personales sensibles, sin que se justifique la creación de las mismas para finalidades legítimas, concretas y acordes con las actividades o fines explícitos que persigue el sujeto regulado.

comisión de los delitos adicionando en comparación con los datos personales que, tratándose de datos personales sensibles, las penas se duplican.”[122]

La Ley General referida es coincidente con las hipótesis normativas relativas al tratamiento de datos personales, y en comparación con la Ley Federal reconoce cualquier tratamiento de datos personales que obren en soportes físicos o electrónicos, con independencia de la forma o modalidad de su creación, tipo de soporte, procesamiento, almacenamiento y organización.[123]

Acotado a la protección de los datos personales sensibles de conformidad con el artículo 7 de la Ley General precitada se establece como excepción a la reglas general de la prohibición de los sujetos obligados a tratar de los datos sensibles que: “se cuente con el consentimiento expreso del titular para que se traten sus datos,”[124] y se relaciona con lo ordenado con el artículo 22 de la misma ley, en lo relativo a excepciones a el otorgamiento del consentimiento expreso al tratamiento de los datos personales sensibles, del artículo en referencia se advierte que de las 10 fracciones previstas la hipótesis normativas para su adecuación es muy amplia, concluyéndose que faculta el tratamiento de los datos sin requerir el consentimiento expreso del titular de los datos sensibles.[125]

La Ley General referida también dota con la naturaleza jurídica de un tratamiento intensivo o relevante de datos personales, al que se efectúa de conformidad con la fracción II del artículo 75,[126] en lo relativo a los datos personales sensibles, por lo

---

[122] *Cfr.* artículo 69 de la Ley Federal de Protección de Datos Personales en Posesión de Particulares.
[123] *Cfr.* artículo 4o. de la Ley de General de Protección de Datos Personales en Posesión de Sujetos Obligados.
[124] *Cfr.* artículo 7o. de la Ley de General de Protección de Datos Personales en Posesión de Sujetos Obligados.
[125] *Cfr.* artículo 22 de la Ley de General de Protección de Datos Personales en Posesión de Sujetos Obligados.
[126] *Cfr.* artículo 75 de la Ley de General de Protección de Datos Personales en Posesión de Sujetos Obligados.
Para efectos de esta Ley se considerará que se está en presencia de un tratamiento intensivo o relevante de datos personales cuando:
I. Existan riesgos inherentes a los datos personales a tratar;
II. Se traten datos personales sensibles, y

que se da apertura a una categoría de tratamiento de datos y de los cuales se desprenden disposiciones específicas como la evaluación de impacto en la protección de datos personales.

Siguiendo con la idea de la protección de los datos personales sensibles, con la introducción en nuestro sistema jurídico de los denominados derechos ARCO, derechos de acceso, rectificación, cancelación y oposición, derechos que se consideran básicos para la protección del derecho fundamental de los datos personales.

De la delimitación conceptual de los derechos de acceso, rectificación, cancelación y oposición, en lo general se pueden definir como: "el conjunto de acciones a través de las cuales una persona física puede ejercer el control sobre sus datos personales,"[127] recapitulando de la definición que los datos personales son exclusivamente de la titularidad de las personas físicas, y cuya finalidad es la Protección de los Datos Personales, al mismo tiempo que se garantizan un control por parte de su titular de los datos personales, en el mismo sentido existen pronunciamientos al respecto del órgano garante en México, el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales.

El Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, establece que: "como titular de tus datos personales, tienes derecho a acceder a ellos, rectificarlos, a solicitar que se eliminen o cancelen, así como a ponerte a su uso. A estos derechos se le conoce como ARCO y están reconocidos en el artículo 16 de la Constitución Política de los Estados Unidos Mexicanos."[128]

III. Se efectúen o pretendan efectuar transferencias de datos personales.

[127] *Cfr*. PÉREZ SERNA, Jesús Mayo, *Los derechos ARCO (Acceso, Rectificación, Cancelación y Oposición)*, México, 12 mayo del 2010, disponible en: <https://ayudaleyprotecciondatos.es/derechos-arco/> [Consulta: 02-enero-2022].

[128] *Cfr.* INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES, *Guía para Titulares de los Datos Personales*, *op.cit.*, página 5.

Se tiene entonces que el objetivo de los derechos de acceso, rectificación, cancelación y oposición es la tutela que ejerce un titular de sus datos personales, poder de control sobre los mismos, y con ello garantizar su protección en el tratamiento que estos tengan, una vez sentadas la bases se vuelve necesario precisar específicamente cada control que ejerce el titular sobre sus datos personales.

Del acceso, por parte de la teoría en la materia en España la autora López-Vidriero y el autor Efrén Santos lo definen como: "aquel derecho que deberá ejercitarse cuando el afectado quiera conocer con exactitud los datos personales de que un tercero- responsable del fichero- dispone, dónde fueron recabados- de una tercera empresa, del propio afectado, y si dichos datos personales o parte de ellos han sido comunicados o van a ser comunicados a un tercero."[129]

En el mismo sentido se pronuncia Osvaldo Gozaini, quien refiere que el derecho de acceso es: "el derecho a solicitar y obtener información de un archivo o registro, para saber si el mismo contiene o no información personal que a alguien concierne; contribuye el fundamento esencial del habeas data. Es el derecho de entrada a los bancos de datos y la garantía principal que tiene una persona para conocer qué información existe sobre ella."[130]

Finalmente, el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, refiere a este derecho como: "el derecho que tienes de solicitar el acceso a tus datos personales que están en las bases de datos, sistemas, archivos, registros o expedientes del responsable que los posee,

[129] LÓPEZ-VIDRIERO, Tejedor y Efrén Pascual Santos, *Protección de datos personales. manual práctico para empresas*, España, Editorial Fundación Confemetal, 2005, p. 91.
[130] GOZAINI, Osvaldo Alfredo, *Habeas data. Protección de datos personales*, Argentina, Rubinzal-Culzoni Editores, 2001, pp. 357-359.

almacena o utiliza, así como de conocer información relacionada con el uso que se da a tu información personal."[131]

Conforme a las definiciones expresadas el derecho de acceso se puede entender como una potestad de control de una persona a saber y conocer específicamente sí sus datos están siendo tratados y modo se realiza, así como conocer cuales datos recaban y para qué fin, y en su caso conocer el almacenamiento de los mismos, transferencias de los mismos, a fin de que conozca y pueda hacer valer sus demás derechos de protección, por lo que se puede considerar con el carácter de primogénito frente a los demás, toda vez que una vez que se tiene acceso por parte del titular de acceder a su información propia puede ejercer los demás.

De la rectificación, en palabras de Carranza Torres: "es la facultad legal que posee toda persona a la cual no se le han mantenido actualizados los datos o no han sido sometidos a la confidencialidad que les corresponde, siendo los mismos en consecuencia inexactos, erróneos o incompletos o indebidos en su difusión, de acuerdos a la situación actual o al marco legal que les correspondiere."[132]

En la misma tesitura la autora Rocío Ovilla define al derecho de rectificación como:

> Derecho que se aplica a las informaciones inexactas, incompletas, equivocadas o caducas. El responsable o usuario de la base de datos, debe proceder a la rectificación, supresión o actualización de los datos personales del afectado, realizando las operaciones necesarias. Es decir, este derecho de rectificación se

[131] *Cfr.* INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES, *Guía para Titulares de los Datos Personales*, *op.cit.,* p. 6.

[132] CARRANZA TORRES, Luis, *Habeas data. La protección jurídica de los datos personales*. Argentina, Editorial Alveroni, 2001, pp. 94 y 95.

convierte en una obligación de rectificación para el responsable de los archivos personales.[133]

De las dos definiciones insertadas se puede concluir que el derecho de rectificación de los datos personales es aquél por el cual el titular de los datos puede solicitar o hacer correcciones de sus datos personales, mismos que pueden modificarse en función de su realidad social, adecuándose a su plano fáctico, ya sea porque son incorrectos, incompletos o desactualizados.

El Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales lo define como: “el derecho que tienes de solicitar la rectificación o corrección de tus datos personales, cuando éstos sean inexactos o incompletos o no se encuentren actualizados. En otras palabras, puedes solicitar a quien posea o utilice tus datos personales que los corrija cuando los mismos sean incorrectos, desactualizados o inexactos.”[134]

Conforme a diversos criterios judiciales se tiene que:

“La adecuación a la realidad social de los datos personales a la persona, es un derecho fundamental y que relaciona directamente con el derecho a la identidad.”[135]

“El derecho de identidad consagrado el artículo 4 de la Constitución Política de los Estados Unidos Mexicanos, toda vez que los datos personales registrados de una persona deben concordar con su realidad y situación actual y social, por medio de la cual se identifique una persona.”[136]

---

[133] OVILLA BUENO, Rocío, *La protección de los datos personales en México*, México, Editorial Porrúa, 2005, p. 37.

[134] C*fr.* INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES, *Guía para Titulares de los Datos Personales*, *op. cit.*, p. 6.

[135] *Cfr.* Gaceta del Semanario Judicial de la Federación, libro 8, diciembre de 2021, Tomo II, página 1141, Undécima Época, 1a./J. 29/2021 (10a.), Número de registro digital: 2023890. Disponible en: <https://sjf2.scjn.gob.mx/detalle/tesis/2023890>

[136] *Cfr.* Gaceta del Semanario Judicial de la Federación, libro 43, junio de 2017, Tomo I, página 580, Décima época, 1a. LXXIII/2017 (10a.), número de registro digital: 2014646. Disponible en: <https://sjf2.scjn.gob.mx/detalle/tesis/2014646>

"Además que la identidad atiene a diversos factores psíquicos y sociales."[137]

Una vez definido el derecho a la rectificación, se debe atender lo relativo al tratamiento que tienen los datos personales, es decir, analizar qué derecho le asiste a un titular a cancelar el tratamiento que tienen sus datos personales.

De la cancelación, la doctrina argentina en la materia en palabras de Osvaldo Gozaini establece que este derecho: "exige el borrado físico de los datos, sin que sea suficiente a estos efectos una marca lógica o el mantenimiento de otro fichero alternativo en el que se registren las bajas producidas,"[138] quien también refiere que este derecho: "confiere una potestad de reclamar la eliminación de toda información que violenta la esfera jurídica del gobernado, y un poder de excluir o suprimir o pedir estas acciones a través de la persona que esté tratando los datos personales."[139]

También se puede definir este derecho como: "la facultad de eliminar de un fichero aquellos datos de carácter personal que no deban figurar en él, ya sea porque nunca debieron ser registrados, ya sea porque habiéndose recogido legalmente, diversas causas exigen su supresión."[140] De lo que se desprende que el titular no necesariamente necesitaría una causa legítima para pedir la cancelación del tratamiento de sus datos, si no que por el simple hecho de ser titular de estos datos debería ser procedente el ejercicio de la cancelación del tratamiento de sus datos personales.

En la misma forma el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales establece que:

---

[137] *Cfr.* Semanario Judicial de la Federación y su Gaceta. libro VI, marzo de 2012, Tomo 1, página 273, Décima Época, 1a. XLV/2012 (10a.). número de registro digital: 2000340. Disponible en: <https://sjf2.scjn.gob.mx/detalle/tesis/2000340>

[138] *Op.cit.* GOZAINI, OSVALDO ALFREDO, Habeas data. Protección de datos personales, p. 373.

[139] *Cfr., Ibidem.,* pp. 364 y 365.

[140] *Op.cit.* GARRIDA DOMÍNGUEZ, ANA, *Tratamiento de datos personales y derechos fundamentales*, p. 133.

> Es el derecho que tienes de solicitar que tus datos personales se eliminen de los archivos, registros, expedientes, sistemas, bases de datos del responsable que los posee, almacena o utiliza. Aunque hay que tomar en cuenta que no en todos los casos se podrán eliminar tus datos personales, principalmente cuando sean necesarios por alguna cuestión legal o para el cumplimiento de obligaciones.[141]

En seguimiento con las definiciones de conforme lo estipula la Ley Federal de Protección de Datos Personales en Posesión de Particulares, se establece una forma de ejercer este derecho, considerando: "la existencia de la figura del bloqueo de datos, pudiéndose interpretar como un antecesor a para la obstrucción del tratamiento de los datos personales, toda vez que la cancelación de datos personales dará lugar a un periodo de bloqueo tras el cual se procederá a suprimir los datos,"[142] por lo que no se constituye el bloqueo como un derecho autónomo a la cancelación, si no como un medio de preparación o fase antes de la cancelación, pero desde esta etapa los datos no pueden ser tratados, por lo que durante el bloqueo ya se ejercita el derecho de cancelación.

De la oposición, la doctrina en palabras de la autora Isabel Davara lo define como: "Consiste en que el titular, en aquellos casos en los que no resulte necesario su consentimiento para el tratamiento de sus datos, y siempre que una ley no disponga lo contrario, podrá oponerse al tratamiento de los mismos cuando existan motivos fundados y legítimos."[143]

Abunda en el tema que nos ocupa Jesús Mayo Pérez quien lo define como:

---

[141] *Cfr.* INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES, *Guía para Titulares de los Datos Personales*, *op.cit.,* p. 7.

[142] *Cfr.* artículo 25 de la Ley Federal de Protección de Datos Personales en Posesión de Particulares.

[143] FERNÁNDEZ DE MARCOS, Isabel Davara. *Breve análisis de la reforma al artículo 6° constitucional en lo relativo a protección de datos personales*, en Carbonell, Miguel y Bustillos, Jorge (coord.), Hacia una democracia de contenidos: la reforma constitucional de transparencia, México, Instituto de Investigaciones Jurídicas, UNAM, México, 2007, p. 85.

El derecho del afectado a que no se lleve a cabo el tratamiento de sus datos de carácter personal o se cese en el mismo en los supuestos en que no sea necesario su consentimiento para el tratamiento, que se trate de ficheros de giro comercial o que tengan la finalidad de adoptar decisiones referidas al interesado y basadas únicamente en el tratamiento automatizado de sus datos.[144]

En la misma tesitura, los autores antes citados López-Vidrieto y Efrén Santos mencionan que:

El derecho de oposición reconoce al afectado la posibilidad de negarse al tratamiento de sus datos de carácter personal por un tercero, siempre y cuando no exista una base legal que obligue al tratamiento de dichos datos como relación contractual, administrativa, etc. Así, cuando no existan motivos legales y legítimos, el afectado podrá oponerse al tratamiento de sus datos.[145]

Así mismo el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales aporta lo siguiente a la definición:

El derecho que tienes de solicitar que tus datos personales no se utilicen para ciertos fines, o de requerir que se concluya el uso de los mismos a fin de evitar un daño a tu persona. También en este caso, como en el anterior, no siempre se

[144] *Op. cit.* PÉREZ SERNA, JESÚS MAYO, *Los derechos ARCO (Acceso, Rectificación, Cancelación y Oposición)*.
[145] *Op.cit.* LÓPEZ- VIDRIERO TEJEDOR, ICIAR Y Efrén Santos Pascual, *Protección de datos personales. manual práctico para empresas*, pp. 92 y 93.

podrá impedir el uso de tus datos personales, cuando sean necesarios por alguna cuestión legal o para el cumplimiento de obligaciones.[146]

Del derecho de oposición se puede concluir que es aquel derecho que consiste en la facultad que un titular de datos tiene frente a un poseedor de sus datos para que se prohíba que sus datos personales tengan un tratamiento específico, es decir, la libertad de determinar cómo quiere limitar el tratamiento de sus datos.

Conclusivamente respecto de los derechos de acceso, rectificación, cancelación y oposición se pueden advertir características únicas, primordialmente que son derechos que pertenecen únicamente a su titular, es decir, que pueden ejercitarse por el gobernado que tiene interés jurídico para este fin, se habla entonces de un ejercicio directo sobre estos derechos respecto de su titular, de igual forma no son derechos absolutos, toda vez que como se ha advertido en este capítulo se encuentran regulados por disposiciones inherentes en la materia, además de las que a continuación de describen.

La legislación aplicable en materia de protección de derechos humanos, se encuentra desde la disposición constitucional que establece que toda persona tiene derecho a la protección de sus datos personales: “al acceso, rectificación y cancelación de los mismos, así como manifestar su oposición,”[147] en términos artículo 16 de la Constitución Política de los Estados Unidos Mexicanos.

---

[146] *Cfr.* INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES, Guía para Titulares de los Datos Personales, *op.cit.,* p. 7.

[147] *Cfr.* párrafo segundo del artículo 16 de la Constitución Política de los Estados Unidos Mexicanos.
[…]
Toda persona tiene derecho a la protección de sus datos personales, al acceso, rectificación y cancelación de los mismos, así como a manifestar su oposición, en los términos que fije la ley, la cual establecerá los supuestos de excepción a los principios que rijan el tratamiento de datos, por razones de seguridad nacional, disposiciones de orden público, seguridad y salud públicas o para proteger los derechos de terceros.
[…]

Por lo que son reconocidos como derechos humanos y el correlativo a la identidad, que en términos de la argumentación vertida en este apartado se relaciona con el artículo 4o. en su párrafo octavo de la Constitución Política de los Estados Unidos Mexicanos. [148] Y por lo que respecta a la legislación internacional de la que el Estado mexicano forma parte están reconocidos por el artículo 18 del correlativo derecho a la identidad y nombre de la Convención Americana sobre Derechos Humanos, Pacto de San José.

De lo anterior se desprende que cualquier violación a estos derechos de acceso, rectificación, cancelación y oposición, implica una vulneración a los derechos humanos de las personas, por lo que la protección a estos derechos sustantivos admiten un control de constitucionalidad y convencionalidad donde se reclame de un acto de autoridad, la protección de los datos personales implica el ejercicio de los derechos humanos del sujeto, y conclusivamente se puede afirmar que los derechos de acceso, rectificación, cancelación y oposición forman parte de la esfera de las personas y ameritan su protección más amplia en favor de su titular.

Por lo que respecta al uso de los datos biométricos de las personas como una forma en la que pueden ser susceptibles de ser vulnerados los derechos humanos de las personas, se deben tomar en consideración los riesgos que implican su almacenamiento así como el rigor jurídico y naturaleza que se les dotan al ser utilizados como una forma de identificarse y de consentir actos jurídicos, involucran un riesgo en el ejercicio de los derechos de acceso, rectificación, cancelación y oposición, toda vez que presuponen vulneraciones a los mismos por su propia naturaleza por la responsabilidad que se remite al usuario o titular de los datos personales y no al responsable del tratamiento.

---

[148] *Cfr.* párrafo octavo del artículo 4 Constitución Política de los Estados Unidos Mexicanos.
[...]
Toda persona tiene derecho a la identidad y a ser registrado de manera inmediata a su nacimiento. El Estado garantizará el cumplimiento de estos derechos. La autoridad competente expedirá gratuitamente la primera copia certificada del acta de registro de nacimiento.
[…]

III.2.1. POSESIÓN Y USO DE BASES DE DATOS CON SISTEMAS BIOMÉTRICOS

Para precisar el uso de las bases de datos que contengan datos biométricos se necesita remontarse al inicio de las bases de datos, los avances científicos y grandes cambios económicos y alteraciones en el ámbito jurídico, toda vez que como se delimitó en el primer capítulo del presente trabajo, en palabras de Concepción Conde Ortiz: “a la sociedad informatizada la definen los bancos de datos y las redes de información. Las bases de datos o bancos de datos jurídicos constituyen una de las modalidades más relevantes del sector, por su importancia social y política y amplitud de la documentación que elaboran.”[149]

Ahora bien, las implicaciones que conlleva el tratamiento de las bases de datos que contienen datos sensibles como se incluyen los datos biométricos, presuponen un posible índice alto de vulneración a los derechos sustantivos de los seres humanos, porque involucran su protección y además de derechos más íntimos del individuo, derecho a la identidad, derecho a la intimidad.

Por otra parte, es indispensable delimitar la figura de los responsables del tratamiento de los datos personales, en este tenor la Ley Federal de Protección de Datos en Posesión de Particulares los define como: “la persona física o moral de carácter privado que decide sobre el tratamiento de datos personales,”[150] así mismo, la LGPDPPSO establece que son los sujetos obligados a que se refiere el artículo 1 de la ley en comento que: “deciden sobre el tratamiento de datos personales,”[151]

---

[149] *Op. cit.* CONDE ORTIZ, Concepción, *La protección de datos personales: un derecho autónomo con base en los conceptos de intimidad y privacidad*, p.16.

[150] *Cfr.* artículo 3 fracción XIV de la Ley Federal de Protección de Datos Personales en Posesión de Particulares.

[…]

XIV. Responsable: Persona física o moral de carácter privado que decide sobre el tratamiento de datos personales.

[…]

[151] *Cfr.* artículo 3 fracción XXVIII de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

[…]

XXVIII. Responsable: Los sujetos obligados a que se refiere el artículo 1 de la presente Ley que deciden sobre el tratamiento de datos personales;

[…]

definiciones legales que permiten identificar los aspectos comunes, que serán las personas físicas o jurídicas colectivas que deciden sobre el tratamiento de los datos personales.

El Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales los define como:

> La persona física o moral o la institución de gobierno que decide sobre el tratamiento de los datos personales, es decir, la que establece las finalidades del tratamiento o el uso que se le dará a los datos personales, el tipo de datos que se requieren, a quién y para qué se comparten, cómo se obtienen, almacenan y suprimen los datos personales, y en qué casos se divulgarán, entre otros factores de decisión.[152]

El Instituto de Transparencia, Acceso a la Información Pública, Protección de Datos Personales y Rendición de Cuentas de la Ciudad de México, por sus siglas, INFOCDMX, define al responsable como: "la persona servidora pública que decide sobre el tratamiento de los datos personales, su finalidad es la protección y seguimiento de las medidas de seguridad de los mismos."[153]

Distinguiéndose el responsable de la figura del encargado, que la LFPDPPP lo define como: "la persona física o jurídica que sola o conjuntamente con otras trate datos personales por cuenta del responsable."[154]

---

[152] *Cfr.* INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES, *Guía para Titulares de los Datos Personales*, *op.cit.,* p. 10.

[153] *Cfr*. INSTITUTO DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN PÚBLICA, PROTECCIÓN DE DATOS PERSONALES Y RENDICIÓN DE CUENTAS DE LA CIUDAD DE MÉXICO, *Designación de responsables de datos personales y de enlaces en sujetos obligados,* Disponible en: < www.infocdmx.org.mx >

[154] *Cfr.* artículo 3 fracción IX de la Ley Federal de Protección de Datos Personales en Posesión de Particulares.

De igual forma, la Ley General estipula que es: “la persona física o jurídica, pública o privada, ajena a la organización del responsable, que sola o conjuntamente con otras trate datos personales a nombre y por cuenta del responsable.”[155] Distinción se menciona por la estrecha relación que guarda el encargado con el responsable, siendo que el responsable es quien decide sobre el tratamiento y el encargado es quien ejecuta el tratamiento de los datos personales.

Conviene precisar las diferencias entre la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados y la Ley Federal de Protección de Datos en Posesión de Particulares, siendo su vértice distintivo el ámbito de aplicación y los sujetos que regulan, es decir a las personas que limitan en materia de datos personales, la Ley Federal con un ámbito aplicativo en toda la República Mexicana como una entidad federada, cuyo objeto de regulación son los particulares que poseen datos personales; y la segunda con aplicación general, que sirve como ley modelo o parámetro para regulación dentro del poder legislativo de cada Entidad Federativa en su potestad de creación y modificación de las leyes.

En seguida se realiza un estudio de los conceptos contenidos anteriormente, particulares y sujetos obligados, a efecto de distinguir las implicaciones del tratamiento conforme a cada uno de los responsables, primero en lo relativo a los sujetos obligados y segundo de los particulares.

Los particulares en materia de datos personales como responsables, en la misma metodología seguida la Ley Federal hace referencia desde su denominación a los particulares, es decir, que la legislación es aplicable para la protección de los datos personales en posesión de los particulares, y por lo tanto son los sujetos a regular, entendiéndose estos particulares como los encargados de los datos.

Los responsables particulares, según la Ley Federal referida son:

[155] *Cfr.* artículo 3 fracción XV de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

Personas físicas o morales de carácter privado que lleven a cabo el tratamiento de datos personales, así mismo se exceptúan de este tratamiento a las sociedades de información crediticia y a las personas que lleven a cabo la recolección y almacenamiento de datos personales, que sea para uso exclusivamente personal, y sin fines de divulgación o utilización comercial.[156]

En el mismo sentido la doctrina, estable que estas excepciones que hace la ley es primero, por una parte, su regulación jurídica respecto al tratamiento de los datos que manejen historial crediticio se encuentra en una ley particular, a saber, la Ley para Regular las Sociedades de Información Crediticia, en cuanto a que dispone reglas claras respecto a la prestación de dicho servicio, el manejo de sus bases de datos, la protección de los intereses del cliente, y sanciones respectivas en caso de contravenir tales disposiciones de la Ley para Regular las Sociedades de Información Crediticia; segunda, de las consideraciones sobre las cuales se fundamenta la exclusión de dichas instituciones tiene que ver con lo relativo a la institución del secreto bancario, la cual ha resguardado la relación de confianza entre los usuarios y las instituciones bancarias, con respecto a las relaciones de confidencialidad y la presencia del respeto al secreto.

La segunda de las excepciones finalmente se refiere a la exclusión del ámbito de aplicación de la Ley Federal mencionada de aquellas personas que aun cuando recolecten o almacenen datos de particulares, lo hagan con el ánimo exclusivamente personal sin la finalidad de su lucro posterior.

---

[156] *Cfr.* artículo 2o. de la Ley Federal de Protección de Datos Personales en Posesión de Particulares. Son sujetos regulados por esta Ley, los particulares sean personas físicas o morales de carácter privado que lleven a cabo el tratamiento de datos personales, con excepción de:
I. Las sociedades de información crediticia en los supuestos de la Ley para Regular las Sociedades de Información Crediticia y demás disposiciones aplicables, y
II. Las personas que lleven a cabo la recolección y almacenamiento de datos personales, que sea para uso exclusivamente personal, y sin fines de divulgación o utilización comercial.

En la misma sintonía de investigación, la Ley General mencionada los define como: “sujetos obligados a aquellos que, en el ámbito federal, estatal y municipal, cualquier autoridad, entidad, órgano y organismo de los Poderes Ejecutivo, Legislativo y Judicial, órganos autónomos, partidos políticos, fideicomisos y fondos públicos.”[157] De esta definición legal es importante soslayar el cúmulo de sujetos que se pueden encuadrar en el supuesto normativo, principalmente en lo relativo a la autoridades, quienes son el objetivo regulatorio, en el entendido que no sólo se trata de autoridades, si no, de entidades, órganos y organismos, cuya naturaleza jurídica son distintas.

De igual forma los sujetos obligados pueden entenderse como:

> El Estado en su sentido estricto, por lo tanto, se puede entender como el Gobierno o el ente potestativo, entendido o englobado en su ámbito estructural político más pequeño, el municipio y hasta el más grande el federal, así como la consideración respecto del poder al que pertenecen, ejecutivo, legislativo y judicial, por lo que abarca todo un cúmulo de autoridades, entidades y organismos, incluidos los OCA´S, Organismos Constitucionales Autónomos. [158]

Así mismo la Ley General en cita ordena que:

> Deberán dotarse de esta categoría a los sindicatos y cualquier otra persona física o moral que reciba y ejerza recursos públicos o realice actos de autoridad en el ámbito federal, estatal y municipal serán responsables de los datos personales,

---

[157] *Cfr.* párrafo 5 del Artículo 1º de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.
[…]
Son sujetos obligados por esta Ley, en el ámbito federal, estatal y municipal, cualquier autoridad, entidad, órgano y organismo de los Poderes Ejecutivo, Legislativo y Judicial, órganos autónomos, partidos políticos, fideicomisos y fondos públicos.
[…]

[158] *Cfr.* LÓPEZ-AYLLÓN, Sergio y David Arellano Gault, *Estudio en materia de transparencia de otros sujetos obligados por la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental*, México, colaboración IFAI, CIDE, UNAM, 2019.

de conformidad con la normatividad aplicable para la protección de datos personales en posesión de los particulares.[159]

Por lo tanto, a pesar de su naturaleza en específico se remite a la multicitada Ley Federal, siendo que cubre la totalidad de los sujetos que deben respetar los datos personales, dejando entonces en el entendido que cualquier persona debe obedecer las leyes protectoras de datos personales porque cualquiera puede estarse tanto en el supuesto de ser particular o en su caso y si lo permite de sujeto obligado, con la anotación que los titulares y personas que laboren como sujetos obligados, cuando no estén en ejercicio de su cargo deberá ser regulados como particulares.

Concluyendo lo anterior y en la relación de los datos biométricos, en los apartados siguientes se abordarán los aspectos legales y repercusiones en el tratamiento de los datos biométricos respecto de los particulares y de los sujetos obligados, por lo tanto, se tendrá una visión de cada uno de los responsables del tratamiento de los datos personales sensibles de las personas

III.2.1.1. POSESIÓN Y USO DE BASES DE DATOS DE SISTEMAS BIOMÉTRICOS POR EL ESTADO

En este apartado principalmente se estudiará lo relativo a la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, toda vez que es la legislación que se encarga de regular lo relativo a los sujetos obligados, mismos que como previamente se analizó conforman un cúmulo de entes gubernamentales que por su simple jerarquía y relación con los particulares, los titulares de los datos personales, deben estar en perfecta limitación y tutela, toda vez que el Estado por su naturaleza debe ser el principal promotor y defensor de los derechos de acceso, rectificación, cancelación y oposición, así como de la protección de los derechos humanos a la intimidad e identidad.

[159] *Cfr.* artículo 1º Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

Conforme al párrafo 4 del artículo 1o. de la LGPDPPSO, se establece que el principal objetivo es establecer las bases, procedimientos, principios, para garantizar el derecho que tiene toda persona a la protección de sus datos personales, artículo que debe ser interpretado y aplicado en sintonía con el artículo 1º de la Constitución Política de los Estados Unidos Mexicanos, en cuanto a la interpretación conforme, el control convencional y constitucional, así como el principio pro persona, entendiendo que el ámbito de sus atribuciones y facultades las autoridades tienen la obligación de promover, garantizar, respetar los derechos a la protección de los datos personales, por lo tanto a la luz de los tratados internaciones y las leyes internas más favorables las personas titulares deben gozar plenamente de la mayor protección que se otorguen a sus datos.

Para el tratamiento de los datos personales la Ley General que nos ocupa establece ciertos objetivos rectores, que son:

> El distribuir competencias entre los Organismos garantes de la Federación y las Entidades Federativas, establecer las bases mínimas y condiciones homogéneas que regirán el tratamiento de los datos personales y el ejercicio de los derechos de acceso, rectificación, cancelación y oposición, mediante procedimientos sencillos y expeditos, además de garantizar la observancia de los principios de protección de datos personales, proteger los datos personales en posesión de cualquier autoridad, entidad, órgano y organismo de los Poderes Ejecutivo, Legislativo y Judicial, órganos autónomos, partidos políticos, fideicomisos y fondos públicos, de la Federación, las Entidades Federativas y los municipios, con la finalidad de regular su debido tratamiento; garantizar que toda persona pueda ejercer el derecho a la protección de los datos personales; promover, fomentar y difundir una cultura de protección de datos personales; establecer los mecanismos para garantizar el cumplimiento y la efectiva aplicación de las medidas de apremio que correspondan para aquellas conductas que contravengan las disposiciones previstas en esta Ley, y regular los medios de

> impugnación y procedimientos para la interposición de acciones de inconstitucionalidad y controversias constitucionales por parte de los Organismos garantes locales y de la Federación; de conformidad con sus facultades respectivas.[160]

De los objetivos en cita se entiende que se brindará la protección más amplia a los datos personales, objetivos que en la mayoría de los casos en la práctica no acontecen, como se analizó en el primer capítulo de este trabajo.

Se establece una acotación a estos derechos de protección de datos por razones de: “seguridad nacional, disposiciones de orden público, seguridad y salud pública o para proteger los derechos de terceros,”[161] limitante que se considera es contraria a los principios constitucionales de proporcionalidad y racionalidad, por lo tanto, dado que como hemos visto en los últimos años en el país, por el simple hecho de argüir que existe un tema de seguridad nacional pueden violarse derechos humanos.

Las hipótesis imperativas por las cuales un sujeto obligado puede tratar datos personales se limitan a dos aspectos:

> Primero que se respeten los principios de licitud, finalidad, lealtad, consentimiento, calidad, proporcionalidad, información y responsabilidad en el tratamiento de datos personales; y segundo, que el tratamiento de datos personales por parte del responsable deberá sujetarse a las facultades o atribuciones que expresamente estén conferidos por la legislación orgánica que se los permita, desde esta vértice el tratamiento de los mismos no sólo debería estarse a lo dispuesto por estos artículo citados, sino que también debería

[160] *Cfr.* artículo 2 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.
[161] *Cfr.* artículo 6 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

observarse que estén previstos entre las facultades de la autoridad, ente, organismo o institución considerada como sujeto obligado.[162]

El tratamiento de los datos biométricos debe atender lo relativo al documento basal para la autorización de tratarlos por parte de su titular, se habla del aviso de privacidad, en el que deberán estar justificadas por finalidades concretas, lícitas, explícitas y legítimas, relacionadas con las atribuciones que legalmente tengan, recordando que este aviso de privacidad deberá contener la finalidad del tratamiento, así como lo relativo a los derechos de acceso, rectificación, cancelación y oposición.

La Ley General que se estudia si bien es avanzada, no es completa para la protección de los datos biométricos como datos sensibles, porque a pesar que menciona medidas de seguridad técnicas como son el conjunto de acciones y mecanismos que se valen de la tecnología relacionada con *hardware* y *software* para proteger el entorno digital de los datos personales y los recursos involucrados en su tratamiento. Y se enlistan las siguientes actividades:

a) Prevenir que el acceso a las bases de datos o a la información, así como a los recursos, sea por usuarios identificados y autorizados;
b) Generar un esquema de privilegios para que el usuario lleve a cabo las actividades que requiere con motivo de sus funciones;
c) Revisar la configuración de seguridad en la adquisición, operación, desarrollo y mantenimiento del software y hardware, y
d) Gestionar las comunicaciones, operaciones y medios de almacenamiento de los recursos informáticos en el tratamiento de datos personales;[163]

[162] *Cfr.* artículos 16 y 17 Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.
[163] *Cfr.* fracción XXIII artículo 3o. de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

Considerando que la mayoría de las bases de datos que contienen datos biométricos son almacenados de forma digital y dada la vulnerabilidad que ha sido ventilada en esta investigación, en la legislación suena bastante protector, pero en la práctica y dados los ilícitos en materia de ciberseguridad.

Después, se destaca que si bien el tratamiento de los datos en manos de los sujetos obligados, debe ser exactamente como la Ley General lo establece, también deben obedecerse diversas legislaciones, principalmente orgánicas o administrativas, y esto tiene su justificación, que es el poder que tiene el Estado frente a los particulares, como doctrinalmente se conoce como la relación de subordinación que se guarda entre el Estado y el gobernado, las medidas deben ser robustas y a favor del equilibro, por lo que la Ley General que se analiza debería tener un marcado interés al titular, como la Ley Federal del Trabajo lo hace en favor de los trabajadores.

Bajo el mismo argumento en los procedimientos que establece, la solicitud de ejercicio de los derechos de acceso, rectificación, cancelación y oposición, así como los recursos de inconformidad y revisión, y finalmente para sustanciación del juicio de amparo, estos deberían estar dotados de la suplencia de la queja en favor del titular, dado que el Estado al tener el monopolio del registro de los datos de las personas, acceso a los datos personales sensibles, fotografía, recolección de huellas digitales, iris, geometría de la mano, por formar parte de un registro nacional de población debe existir un balance entre las partes, dada la relación que es evidente.

Una vez precisado lo anterior, se advierte que existe una evidente justificación de una regulación que debería de ser excesivamente exhaustiva para los sujetos obligados, no sólo que se doten de atribuciones y facultades, si no que expresamente se establezcan limitaciones al tratamiento de los datos biométricos, que como se analizó forman parte de la identidad y esencia de los seres humanos, y que las autoridades y el Estado permiten tener almacenados, a través del Registro

Nacional de Población, y como se sabe: “los datos se permiten trasferir, como en caso del Instituto Nacional Electoral como ejemplo de un órgano constitucional autónomo, el Sistema de Administración Tributaria como un órgano desconcentrado de la Secretaría de Hacienda y Crédito Público.”[164]

III.2.1.2. POSESIÓN Y USO DE BASES DE DATOS DE SISTEMAS BIOMÉTRICOS POR PARTICULARES

De este apartado se destacarán las principales disposiciones relativas al tratamiento de los datos personales en posesión de los particulares y sus diferencias con las de los sujetos obligados, remitiéndose principalmente a la Ley Federal de Protección de Datos Personales en Posesión de Particulares, retomando algunos argumentos vertidos en los capítulos anteriores.

La Ley Federal mencionada establece los principios rectores que: “se deben observar en el momento de tratar los datos personales que son: licitud, consentimiento, información, calidad, finalidad, lealtad, proporcionalidad y responsabilidad,”[165] en este entendido los datos personales son tutelados.

La limitante para los particulares que traten datos personales, además del aviso de privacidad, es que se limiten al cumplimiento de las finales que se suscribieron en el aviso de privacidad, y por lo que respecta a la seguridad de los datos personales que ya recabaron y que lleve a cabo tratamiento de datos personales deberá: “establecer y mantener medidas de seguridad administrativas, técnicas y físicas que permitan proteger los datos personales contra daño, pérdida, alteración, destrucción o el uso, acceso o tratamiento no autorizado.”[166]

---

[164] *Cfr.* LÓPEZ SÁNCHEZ, Rogelio y José Luis Leal Espinoza, *El derecho a la información y datos personales en México, una visión comparada con el sistema interamericano y europeo de derechos humanos,* México, Editorial Dykinson, 2018.

[165] *Cfr.* artículo 6 de la Ley Federal de Protección de Datos Personales en Posesión de Particulares. Los responsables en el tratamiento de datos personales, deberán observar los principios de licitud, consentimiento, información, calidad, finalidad, lealtad, proporcionalidad y responsabilidad, previstos en la Ley.

[166] *Cfr.* artículo 19 de la Ley Federal de Protección de Datos Personales en Posesión de Particulares. Todo responsable que lleve a cabo tratamiento de datos personales deberá establecer y mantener medidas de seguridad administrativas, técnicas y físicas que permitan proteger los datos personales

Se estima que la legislación no cubre las vulnerabilidades de los sistemas informáticos que llegaren a contener datos biométricos, por ende resulta una porción normativa que se queda en la hipótesis y que en la realidad no provee de mecanismos de defensa reales frente a las vulneraciones a la protección de los datos personales.

Con referencia a lo anterior debe destacarse lo dispuesto por el párrafo final del artículo mencionado, donde evidentemente el legislador previó los daños y vulneraciones para las medidas de seguridad, refiriendo que los responsables no adoptarán medidas de seguridad menores a aquellas que mantengan para el manejo de su propia informa información y advierte el denominado el riesgo existente, las posibles consecuencias para los titulares, la sensibilidad de los datos y el desarrollo tecnológico.

En el mismo sentido el artículo 20 de la Ley Federal en cita manda que las vulneraciones de seguridad ocurridas en cualquier fase del tratamiento que afecten de forma significativa los derechos patrimoniales o morales de los titulares, serán informadas de forma inmediata por el responsable al titular, y que el titular es quien debe optar por las medidas correspondientes a la defensa de sus derechos, consolidando una vulneración y menoscabo a su defensa y protección de datos, dado que el titular es quien en la mayoría de los casos menor conocimiento de seguridad y sistemas informáticos tiene.

La LFPDPPP establece un mecanismo que debe ejercitarse frente al Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, el procedimiento de protección de datos, y el procedimiento de verificación, y como forma de la ejecución y poder coercitivo el procedimiento de

---

contra daño, pérdida, alteración, destrucción o el uso, acceso o tratamiento no autorizado. Los responsables no adoptarán medidas de seguridad menores a aquellas que mantengan para el manejo de su información. Asimismo se tomará en cuenta el riesgo existente, las posibles consecuencias para los titulares, la sensibilidad de los datos y el desarrollo tecnológico.

imposición de sanciones, que son procedimientos que sin lugar a dudas son garantistas y protectores de los derechos de acceso, rectificación, cancelación y oposición y de la protección de los datos personales, pero se entiende que estos procedimientos se ejercitar por solicitud del interesado, pero que sucedería en el caso que una persona no supiera que existen vulneraciones a sus datos personales, o para aquellas personas que nunca se han enterado de los derechos frente a sus datos.

De las diferencias principales del tema de los datos biométricos se destacan que al ser datos personales sensibles por una parte en posesión de los sujetos obligados, estos son limitados conforme a la atribuciones de la autoridad que se trate y que los mismos deben ser expresamente justificados y con finalidades muy específicas, mientras que en posesión de particulares su tratamiento puede remitirse a un aviso de privacidad donde expresamente y con la formalidad de ser por escrito donde se consienta su tratamiento.

Por último, la diferencia entre el tratamiento que se le den a los datos en posesión de particulares y de sujetos obligados depende directamente con la calidad del sujeto responsable, es decir, la relación que guarda este frente al titular, llámese una relación entre iguales, particulares, o entre subordinados o bajo la facultad de imperio. Relaciones que en mucho tienen que ver con la forma y limitación para tratar los datos personales, ejemplo de ello, es que uno simplemente puede remitirse a un consentimiento otorgado en un aviso de privacidad y el otro tiene que limitarse a sus atribuciones, así como exactamente delimitar cual es el propósito para tratar los datos.

Finalmente se concluye que si existen diferencias en el tratamiento de los datos personales sensibles de los titulares en función del sujeto que es responsable de su tratamiento, y por lo argumentado en párrafos anteriores la rigurosidad se encuentra justificada, lo que se destaca en los apartados es que en la realidad las responsabilidad del tratamiento se refiere al titular sobre todo en los riesgos que

advierten y por lo tanto al que le corresponde que sean seguros y protegidos es al propio titular, mismo que cuenta con procedimientos que le permiten el ejercicio de los derechos de acceso, rectificación, cancelación y oposición.

III.2.2. EL VALOR COMERCIAL DE LOS DATOS PERSONALES

Una vez que se ha definido el tratamiento de los datos personales sensibles, conformados también por los datos biométricos de los titulares conforme a la metodología de esta investigación se hablará del valor que tienen estos datos personales en el mundo, entendiendo que su importancia se encuentra en los datos contenidos en las bases de datos y que permiten acceder como un usuario, autenticándose o en su caso que permiten la celebración de actos jurídicos con esos datos.

Para Lorena Pichardo Flores: “en la era digital los datos personales son un activo de valor económico, razón por la cual es necesario ser cuidadosos a la hora de hacer uso de las redes socio digitales e internet, así como corroborar su ciclo de vida.”[167] Cita que permite presuponer que el valor de los datos biométricos como datos personales sensibles tienen un valor económico, y esto también se deriva del tratamiento de estos, principalmente por las grandes bases de datos, mismas que contienen datos personales que permiten generar perfiles de las personas con aplicaciones de mercado, salud, economía, consumidores, por lo que, estas aplicaciones por sí mismas dotan de un valor agregado a los datos personales, por lo que deductivamente se demuestra que existe un valor que se puede cuantificar por el tratamiento de los datos personales.

Además del valor económico de los datos personales se reconoce que existe poder dentro de ellos, es decir, al controlar la identidad y formas de autenticación,

---

[167] PICHARDO FLORES, Lorena, *El valor de los datos se relaciona con su vulnerabilidad*, México, Dirección General de Comunicación Social, Universidad Nacional Autónoma de México, 28 de julio del 2021, disponible en: < https://www.dgcs.unam.mx/boletin/bdboletin/2021_613.html#:~:text=En%20la%20era%20digital%20los,Personales%2C%20de%20la%20Unidad%20de > [Consulta: 08-enero-2022].

es decir, se deja latente la posibilidad de manejar bases de datos que permiten controlar la forma en que se manejan las masas, por ejemplo de control de elecciones celebrados por medios electrónicos y que utilicen mecanismos de autenticación con datos personales de los ciudadanos.

Al hablar del valor comercial de los datos biométricos es obligado pretender dar cantidades líquidas o estimaciones de los mismos, para este tenor Pichardo Flores Lorena dice que:

> En el caso de Latinoamérica IBM obtuvo el costo 1.68 millones de dólares, esto es, aproximadamente, 35 millones de pesos por una vulneración de datos personales a una organización; es decir, el promedio del costo en el mundo es más alto que en Latinoamérica. Un solo dato personal, por ejemplo, una Clave Única de Registro de Población, domicilio o Registro Federal de Contribuyentes cuesta tres mil 135 pesos en el orbe.[168]

Cantidades que permiten conocer que efectivamente los datos personales tienen un precio en el mercado, y esto es derivado a la integración del mundo digital en nuestra vida, toda vez que los procesos tecnológicos aceleran los procesos que tratan con datos biométricos o cualquier otro dato personal, por lo que actualmente podrían aumentar los precios que se precisaron.

Existe un valor en el mercado comercial de los datos personales, con aplicaciones en ventas, captación de usuarios, el pago de los usuarios en plataformas digitales, conseguir seguidores en plataformas de interacciones sociales y actualmente monetización de contenido en plataformas como *YouTube* y *Facebook*, lo que permite advertir que además de un valor por publicidad.

También permite un valor por la creación de perfiles digitales que contengan datos personales, es decir, entre más se conozca del usuario tiene más valor la

[168] *Idem.*

base de datos que contenga su información, porque ello permite vulneraciones, manipulaciones, y generar conductas entre los mismo, y por ende el control de los mismos.

En conclusión, una vez relacionado lo expuesto en este apartado con los dos capítulos que anteceden, establecido un valor interno subjetivo de los datos biométricos por cada titular y establecido el valor objetivo de mercado, se puede afirmar que los datos personales son tan importantes en nuestra sociedad actual que su simple almacenamiento presupone ganancias para su titular y el propio encargado, además que son herramientas de poder y control de las masas, dejando a un lado el valor económico, publicitario y comercial, los datos biométricos forman parte elemental de las personas y su valor es proporcionar al grado de sensibilidad que estos implique para el titular, entre más sensible sea el dato personal para su titular, más valor tiene y actualmente con el uso de medios ópticos que los captan es una realidad que por su escaza regulación existe un estado de vulneración en los derechos de las personas.

III.3. REGISTRO NACIONAL DE USUARIOS DE TELEFONÍA MÓVIL

El Registro Nacional de Usuarios de Telefonía Móvil, por sus siglas RENAUT, fue pretendido ser incorporado al sistema jurídico mexicano mediante un paquete de reformas publicado en el Diario Oficial de la Federación de publicación del 16 de abril del 2021, relativo al decreto por el que se reformaban y adicionaban diversas disposiciones de la Ley Federal de Telecomunicaciones y Radiodifusión, a través de cual se pretendía que existiera un Registro Nacional que proporcionara y contuviera datos biométricos de los usuarios de la telefonías móviles.[169]

Específicamente el paquete de reformas a la Ley Federal de Telecomunicaciones y Radiodifusión adicionó al Título Séptimo el Capítulo I Bis, respecto del: “Padrón

[169] *Cfr.* Decreto por el que se reforman y adicionan disposiciones a la Ley Federal de Telecomunicaciones y Radiodifusión, publicado en el Diario Oficial de la Federación de fecha 16 de abril del 2021.

Nacional de Usuarios de Telefonía Móvil,"[170] incorporaciones efectuadas en el sentido de: "promover la colaboración con autoridades en materia de seguridad y justicia en los asuntos relacionados con la comisión de delitos,"[171] objeto principal del Registro en cita, y lo que interesa respecto de esta investigación ubica su fundamento en el artículo 180 Ter de la Ley precitada específicamente en lo relativo a su fracción VI que establece que el Registro contendrá sobre cada línea telefónica móvil, los datos biométricos del usuario y, en su caso, del representante legal de la persona moral titular de la línea telefónica, lo que deberá regirse por los lineamientos que en su caso emita el Instituto Federal de Telecomunicaciones y Radiodifusión.

En el mismo sentido con las reformas a la Ley en mención se establece que: "el registro de una línea telefónica en el Padrón será obligatorio para el usuario, que será obligado a entregar y proporcionar identificación oficial, comprobante de domicilio y datos biométricos, para la activación de la línea telefónica."[172] Disposición que sin duda alguna evidencia un estado de vulneración a los derechos de acceso, rectificación, cancelación y oposición de los usuarios de telefonías móviles y titulares de sus datos biométricos, toda vez que en ningún supuesto remite la posibilidad de decidir sobre el tratamiento de datos de su titular, por el contrario, se habla de una obligación de otorgar sus datos.

En la misma línea de investigación de conformidad con la Ley Federal de Telecomunicaciones y Radiodifusión, se autorizan a los concesionarios de telecomunicaciones a: "recabar e ingresar la información sobre la identidad, datos biométricos y domicilio del usuario, así mismo admite la posibilidad que esto se efectúe mediante el uso de medios digitales y medios remotos,"[173] cuestiones normativas que permiten realizar un análisis cualitativo comparado con aspectos

[170] *Cfr.* Reformas propuestas a la Ley Federal de Telecomunicaciones y Radiodifusión.
[171] C*fr.* Reformas al artículo 180 Bis primer párrafo Ley Federal de Telecomunicaciones y Radiodifusión.
[172] *Cfr.* Reformas al artículo 180 Ter de la Ley Federal de Telecomunicaciones y Radiodifusión.
[173] *Cfr.* Reforma propuesta al artículo 180 Quinties de la Ley Federal de Telecomunicaciones y Radiodifusión.

que ya fueron mencionados, que van en el sentido de advertir sobre las vulneraciones de los medios informáticos que traten datos personales de las personas.

Respecto de la responsabilidad de estas bases de datos, si bien se remite a legislar en el sentido que: “los concesionarios serán responsables de la veracidad e integridad de la información,”[174] en nada se menciona lo relativo a las disposiciones en materia de tratamiento de datos personales en posesión de sujetos obligados, así como también los faculta a la realización de altas y bajas de los usuarios registrados, es decir, en atribuciones relativas a la identidad de los usuarios, presupuestos reformados que permiten la vulneración directa del derechos humano a la identidad, intimidas y protección de los datos personales.

Ahora bien el párrafo sexto del artículo 180 Quinties de la Ley en cita establece que el usuario titular del servicio telefónico puede no reconocer como propio un número de línea telefónica móvil vinculado a su nombre o denominación social, podrá solicitar al Instituto, al concesionario de telefonía o, en su caso, al autorizado, la actualización de la información correspondiente o su baja del Padrón Nacional de Usuarios de Telefonía Móvil, y a pesar de esta facultad del titular el propio articulado en su párrafo final advierte que la baja de un número de línea telefónica móvil en el Padrón Nacional de Usuarios de Telefonía Móvil no implica la eliminación del registro correspondiente, el registro del número asociado a dicha persona se mantendrá por un plazo de 6 meses, disposición que a todas luces presupone una violación a las disposiciones que se analizaron relativas a la Ley General, así como tampoco remite a hacer mención al aviso de privacidad que debería ser obligatorio para este rubro.

Lo único que se establece relativo a la protección de los datos personales de los usuarios de telefonía móvil es que remiten que la información contenida en el

[174] *Cfr.* Reforma propuesta al artículo 180 Quinties párrafos 2º y 3º de la Ley Federal de Telecomunicaciones y Radiodifusión.

Padrón Nacional de Usuarios de Telefonía Móvil a que se refiere el artículo 180 Bis será confidencial y reservada en términos de la Ley General de Transparencia y Acceso a la Información Pública, de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados y de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, leyes que conforme a los artículos anteriores estudiados resulta debatible su aplicabilidad al caso concreto y tutela de los derechos humanos, toda vez que del cuerpo normativo se advierten posibilidades para dejar de atender las disposiciones en materia de protección de datos personales.

Del mismo decreto para reformar la Ley de Telecomunicaciones y Radiodifusión, se añaden al repertorio de sanciones lo dispuesto por el Capítulo II Bis del Título Décimo Quinto, establece una lista de supuestos por los concesionarios que para el efecto de sujetos en materia de datos personales tienen el carácter de particulares, pueden ser sancionados por respecto al uso del Registro Nacional de Usuarios de Telefonía Móvil, y cabe destacar a la fracción VI del artículo 307 Bis, en el que: "se sancionarán si obtienen un lucro indebido, directamente o indirectamente por el tratamiento de los datos personales, sancionado con infracción de dos a tres veces el valor del lucro obtenido,"[175] monto que no podría ser realmente cuantificado por un peritaje en caso de controversia toda vez que el lucro podría aducirse como mínimo o en su caso nulo dada la naturaleza que ya se analizó de los datos biométricos como datos personales, en este tenor, la infracción no presupone la cesación de la concesión otorgada por lo que es una infracción que se podría considerar simbólica para el lucro real que se podría obtener del tratamiento de datos biométricos.

De las porciones normativas citadas y analizadas cualitativamente se advierten que existen vulneraciones por parte de estas disposiciones en materia de datos personales, identidad e intimidad de las personas, derivado de lo anterior ante

[175] *Cfr.* Reformas propuestas a la fracción V del Artículo 307 Ter de la Ley Federal de Telecomunicaciones y Radiodifusión.

notorio poder de control y como limitante al poder del Sujeto Obligado, Instituto Federal de Telecomunicaciones y Radiodifusión, así como de los particulares beneficiados, los concesionarios, por lo anterior y en el tenor de los controles constitucionales que se cuentan la defensa de la constitucionalidad de los actos, ante las reformas el propio Instituto Federal de Telecomunicaciones promovió una controversia constitucional que quedó registrada bajo el número 71/2021 con fecha de presentación de 26 de mayo del 2021.

La controversia constitucional 71/2021 fue presentada por el Instituto Federal de Telecomunicaciones con el objeto de:

> […]Declarar la invalidez de los artículos 180 Bis en relación con el Tercero Transitorio, 180 Quáter, primer párrafo del Segundo Transitorio, Cuarto Transitorio y Sexto Transitorio del Decreto por el que se reforman y adicional diversas disposiciones de la Ley Federal de Telecomunicación y Radio Difusión, publicado en el Diario Oficial de la Federación el 16 de abril del 2021.[176]

Y conforme al incidente de suspensión de la controversia constitucional en cita la Suprema Corte de Justicia de la Nación concedió al Instituto Federal de Telecomunicaciones suspensión dentro la controversia constitucional 71/2021 promovida en contra del Padrón Nacional de Usuarios de Telefonía Móvil.

Al resolver el incidente de suspensión la Suprema Corte de Justicia de la Nación concedió la suspensión respecto a la obligación de instalar, operar, regular y mantener el Padrón Nacional de Usuarios de Telefonía Móviles, argumentado que:

---

[176] SUPREMA CORTE DE JUSTICIA DE LA NACIÓN, *Controversia Constitucional: 71/2021*. Disponible en: <https://www.scjn.gob.mx/sites/default/files/acuerdos_controversias_constit/documento/2021-05-31/MP_ContConst-71-2021.pdf > [Consulta: 09-enero-2022].

“existía un riesgo sobre la autonomía constitucional del Instituto Federal de Telecomunicaciones con su simple entrada en vigor.”[177]

En el mismo tenor de medio de control de constitucionalidad en lo relativo a la inconstitucionalidad de las normas en materia del Padrón Nacional de Usuarios de Usuarios de Telefonía Móvil, se promovieron las acciones de inconstitucionalidad 82/2021 y su acumulada 86/2021, promovidas por el órgano garante en materia de protección de datos personales, el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, así como de los Senadores pertenecientes de la LXIV Legislatura de la Cámara Alta de la Nación, con el mismo objeto de inconstitucionalidad del paquete de reformas, para:

> […]Declarar la invalidez de los artículos 180 Bis en relación con el Tercero Transitorio, 180 Quáter, primer párrafo del Segundo Transitorio, Cuarto Transitorio y Sexto Transitorio del Decreto por el que se reforman y adicional diversas disposiciones de la Ley Federal de Telecomunicación y Radio Difusión, publicado en el Diario Oficial de la Federación el 16 de abril del 2021.[178]

De la controversia constitucional y de las acciones constitucionales citadas se advierte que la regulación en materia del Registro Nacional de Usuarios de Telefonía Móvil contenía vacíos legales y presupuestos inconstitucionales, y que conforme al estudio cualitativo se afirma que efectivamente de las disposiciones en materia y de datos biométricos deben ser derechos tutelados rigurosamente, sin importar el sujeto que los trate tanto obligado o particulares.

---

[177] INSTITUTO FEDERAL DE TELECOMUNICACIONES, *La Suprema Corte de Justicia de la Nación concede al Instituto Federal de Telecomunicaciones suspensión dentro la Controversia Constitucional 71/2021 promovida en contra del Padrón Nacional de Usuarios de Telefonía Móvil, México,* Comunicación y Medios, (Comunicado 55/2021) 15 de junio 2021. Disponible en: < www.ift.org.mx > [Consulta: 10-enero-2022].

[178] SUPREMA CORTE DE JUSTICIA DE LA NACIÓN, Acción de Inconstitucionalidad 82/2021 y su Acumulada 86/2021, Disponible en: <https://www.scjn.gob.mx/sites/default/files/acuerdos_controversias_constit/documento/2021-05-28/MI_AccInconst-82-2021.pdf> [10-enero-2022].

Concomitante a lo anterior se retoma lo expuesto en el primer capítulo, relativo a la consulta de sentencias en versión pública emitidas por el Poder Judicial de la Federación, empleando la plataforma del Consejo de la Judicatura, en la cual al ingresar como búsqueda la frase exacta de biométricos en el buscador temático, arrogó una cantidad considerable de sentencias que hacían referencia a juicios de amparo y recursos en relación a las reformas a la Ley Federal de Telecomunicaciones y Radiodifusión, por lo que es evidente que existe una rechazo y problemática en torno a intentar emplear los datos biométricos en un registro nacional, derivado de la notoria incompatibilidad con los derechos humanos de las personas.

En el mismo esquema de protección de datos personales, el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, advierte que de estas violaciones principalmente destacan los conceptos de violación relativos a los:

> Derechos fundamentales como privacidad, vida privada, intimidad, identidad y protección de los datos personales, por lo menos, de 122 millones de usuarios de telefonía móvil. Sin embargo, hasta octubre pasado el documento de la controversia constitucional interpuesta por el IFT no era público; el Instituto optó por anunciarla a través de comunicados de prensa.[179]

Por lo tanto, se convalida que efectivamente con este Registro analizado en el presente apartado se violan los derechos humanos precisados.

---

[179] INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES, *CONSEJERÍA JURÍDICA DEBE INFORMAR SOBRE CONTROVERSIA CONSTITUCIONAL PRESENTADA POR EL IFT EN CONTRA DEL PANAUT: INAI,* México, Dirección General de Comunicación Social y Difusión, 14 de noviembre del 2021, disponible en:<https://home.inai.org.mx/wp-content/documentos/SalaDePrensa/Comunicados/Nota%20INAI-101-21.pdf> [Consulta: 11-enero-2022].

En adición debe destacarse que no es conveniente que un Estado tenga tantos datos biométricos de sus gobernados, porque ello implica un poder sobre estos y sobre su esfera más íntima, siendo cierto que este poder está limitado por la Ley General referida, esta no limita expresamente el tratamiento de los datos biométricos, además que las disposiciones tildadas como inconstitucionales de la Ley Federal de Telecomunicación y Radiodifusión buscar y pretender evadir las disposiciones protectoras de este derecho humano.

Del otro lado se encuentran los particulares quienes en términos de la Ley Federal de Telecomunicación y Radiodifusión son concesionarios que tienen en su caso la facultad para tratar datos personales de los usuarios de las telefonías móviles, siendo que por los medios de control constitucional citados las disposiciones se ven viciadas de ser violatorias y contrarias a la Constitución Política de los Estados Unidos Mexicanos.

Lo cierto es que, de igual forma como se analizó en el capítulo anterior, los mecanismos constitucionales vistos en este apartado podrían ejercitarse en lo relativo a las Instituciones de Crédito que utilizan los datos biométricos como forma de identidad, sirviendo casi en similitud los argumentos expuestos, permitiendo entonces un verdadero control constitucional que garanticen los derechos de protección de datos, identidad e intimidad.

Finalmente, el Registro Nacional de Usuarios de Telefonía Móvil como se advirtió en este apartado difiere con la aplicabilidad de los derechos de acceso, rectificación, cancelación y oposición, argumento que se torna importante para el caso de se convalide su constitucionalidad a futuro dentro de México, lo cual conforme a las características de los derechos humanos, su evolución permite garantizar el Estado de Derecho y de respeto a los derechos de identidad y protección de datos.

En conclusión de este capítulo, una vez estudiados los elementos de los datos biométricos como datos personales sensibles, resaltando los aspectos del

tratamiento de los datos y delimitado el campo de estudio de los datos biométricos dentro del sistema jurídico mexicano, se llega a la conclusión que los datos biométricos no son protegidos por la legislación mexicana con el rigor de deberían serlo, de igual forma, se concluye que existen violaciones a los derechos sustantivos de identidad, intimidad y protección de datos por la falta legislativa en materia de uso de los datos biométricos y que los presupuestos normativos actuales no son suficientes.

IV. CAPÍTULO IV DE LAS PROBLEMÁTICAS DEL USO DE SISTEMAS BIOMÉTRICOS

En el último capítulo de la investigación se abordarán las principales problemáticas que se advierten del uso de los sistemas biométricos como un forma de identidad y una forma de otorgar el consentimiento en la celebración a los actos jurídicos, tratando las problemáticas principalmente desde el ámbito jurídico, es decir, las implicaciones a los derechos que conlleva su uso, de igual forma señalando las vulneraciones a derechos sustantivos de las personas, buscando como principal objetivo cerrar las líneas de investigación que previamente fueron argumentadas en los capítulos precedentes.

IV.1. LA INSEGURIDAD JURÍDICA DEL USO DE SISTEMAS BIOMÉTRICOS COMO FORMA DE IDENTIDAD Y DE CONSENTIMIENTO PARA ACTOS JURÍDICOS

Como previamente se ha abordado en los dos capítulos que anteceden los datos biométricos de un individuo constituyen un elemento sustancial de la misma persona, recapitulando la categoría de los mismos como datos personales sensibles que forman parte de la esfera de privacidad más íntima de un individuo, por lo que la falta de una regulación exhaustiva provoca una evidente transgresión a los derechos humanos, y en este apartado se analizaran de forma cualitativa, legislativa y analítica los elementos que constituyen estas aducidas violaciones.

Empezando por recordar que en el estudio internacional de la legislación de los datos biométricos, en palabras de Tábata Andrea Romero Cerdán: "El pasado 27 de abril de 2016, el Parlamento Europeo y del Consejo, aprobó el Reglamento (UE) 2016/679 (en adelante, RGPD) con el que se le otorga a algunos datos personales, la calidad de especiales, por concebir que dada su naturaleza, requieren de una protección particular."[180] Que permite advertir como se observó en el marco

[180] *Op.cit*. ROMERO CERDÁN, Tábata Andrea, *La autenticación y verificación de la identidad a través de información biométrica como paradigma del tratamiento de datos personales en México*.

internacional existe un mayor rigor regulatorio en torno a los datos biométricos en comparación con el sistema jurídico nacional.

Así mismo, la autora en cita proporciona dos elementos que deben ser considerados al momento de tratar los datos biométricos de las personas, que se constriñen en: "la legitimación del tratamiento de los datos biométricos y la evaluación de la necesidad y proporcionalidad, principios que colaboran en el entendimiento de la necesidad regulatoria exhaustiva y los presupuestos normativos que deberían actualizarse para requerir el uso de datos biométricos."[181]

Estos principios del tratamiento de los datos biométricos en términos de la autora Tábata Romero atienden a que:

> Primero, el principio de legitimación, en donde los responsables del tratamiento de datos biométricos deberán precisar en la evaluación de impacto, la base de legitimación del tratamiento. Obligación que como se analizó en el capítulo anterior atiende a los principios que rigen el tratamiento de los datos personales, específicamente el principio de licitud. Ello significa que en primer lugar, el responsable deberá acreditar el consentimiento del interesado; en segundo lugar, que el tratamiento se realice en apego al consentimiento otorgado o bien de conformidad con alguna base legítima establecida en la legislación de la materia y, en tercer lugar, en caso de que el tratamiento se funden en el interés legítimo perseguido por el responsable, éste deberá privilegiar en todo momento los derechos de las personas, además de tomar en cuenta las expectativas razonables de aquellos que pudieran resultar afectadas por el tratamiento.[182]

En el tenor anterior, se tiene que frente a las vulneraciones e inseguridad de los titulares de los datos biométricos debe existir una causa fundada por la cual se vayan a usar los datos biométricos, partiendo de esta premisa se debe atender a

[181] *Idem.*
[182] *Cfr., Idem.*

una hipótesis normativa que establezca claramente la procedencia de este tratamiento.

Segundo, del principio de la evaluación de la necesidad y proporcionalidad, Romero Cerdán lo define en términos de una: “obligación de los responsables a realizar una evaluación de la finalidad con la que los datos son tratados a fin de determinar su necesidad y proporcionalidad.”[183]

Así es como, para realizar una adecuada evaluación en materia de protección de datos personales deben atenderse la normatividad aplicable, que como se observó en el capítulo anterior deja un vacío legal interpretativo y poco favorable para el titular.

Para la autora antes citada, Tábata Romero: “la necesidad se acredita cuando la finalidad con la que se realiza el tratamiento de datos personales no puede conseguirse por otros medios.”[184] Es decir, que el objetivo de identificar a las personas o en su caso otorgar su consentimiento no puede obtenerse mediante otros mecanismos o procedimientos, argumento que se ha abordado y que es óbice no cumple con el requisito de necesidad, esto es, que para identificar a una persona no sólo pueden usarse sus datos biométricos, sino que se advierten otras formas, como son las tarjetas de identidad, los documentos expedidos por el Registro Civil, y demás que no forzosamente involucran proceso de autenticación mediante el uso de los datos biométricos, por lo tanto este principio es notoriamente superado por la realidad.

En tanto que la proporcionalidad, se comprobará a través de tres tipos de análisis, conforme a Tábata Romero: “el de necesidad, el de idoneidad y el de proporcionalidad en sentido estricto. La convergencia de estos tres, permitirá a los responsables del tratamiento ponderar los derechos y libertades en juego, para

[183] *Op.cit.* ROMERO CERDÁN, Tábata Andrea, *La autenticación y verificación de la identidad a través de información biométrica como paradigma del tratamiento de datos personales en México*.
[184] *Cfr., Idem.*

determinar la necesidad y proporcionalidad de la medida."[185] Partiendo de esta premisa, tal y como sucedió con el Registro Nacional de Usuarios de Telefonía Móvil, en el que se pretende justificar el uso de datos biométricos en determinadas circunstancias, se entendería como un interés colectivo para legitimarse para el uso de la biometría de las personas para la persecución de delitos, pero en todo caso se argumenta que la acumulación masiva de los datos biométricos incrementa los riesgos para la seguridad, toda vez que las bases de datos a mayor escala dejan a los individuos más vulnerables ante ilícitos, los cuales serán abordados en el apartado siguiente.

Aunado a lo anterior se debe tomar en consideración que el tratamiento de los datos biométricos contenidos en bases grandes, o en bases de datos por extranjeros no están reguladas y que trasladan la responsabilidad de su uso al usuario final, propician las violaciones en la vida privada de las personas.

Afectando su privacidad no sólo en el momento de la vulneración de las bases, sino de forma casi permanente o hasta que se corroboren sus datos fueron eliminados o recuperados, y que en consecuencia de un almacenamiento no autorizado, y en relación con el marco teórico de los datos biométricos, recordando que todos los rasgos físicos y conductuales que pueden ser medibles y que se dotan de inmutabilidad, no pueden ser modificados con facilidad.

Por su parte, el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales elaboró un manual que permite conocer cómo deberían ser tratados los datos biométricos dentro del territorio nacional, estableciendo un mecanismo denominado evaluación de impacto en la protección de los datos personales, definiéndola como:

[185] *Op.cit.* ROMERO CERDÁN, Tábata Andrea, *La autenticación y verificación de la identidad a través de información biométrica como paradigma del tratamiento de datos personales en México*.

> Un análisis documentado mediante el cual los responsables que pretendan poner en operación o modificar políticas públicas, programas, sistemas o plataformas informática, valoran los impactos reales respecto de determinado tratamiento de datos personales, a efecto de identificar posibles riesgos para dichos datos, con el objeto de conocer las medidas implementadas y por implementarse, para protegerlos y mitigar los riesgos identificados.[186]

La evaluación de impacto, nos permite inducir que existe un riesgo e impacto cuando los datos biométricos son tratados, mismos que se buscan ser mitigados en el mismo sentido protector, dado que existen actualmente riesgos en utilizar los datos biométricos como forma de identidad y en su caso como datos personales.

La guía en cita, señala que:

> Esta realización de evaluaciones de impacto en la protección de datos personales es una obligación para los sujetos obligados en términos de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados cuando realicen tratamientos intensivos o relevantes, tomando en cuenta las excepciones del artículo 79 de la Ley General citada, sin embargo, la realización de estas evaluaciones es una buena práctica que el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, recomienda realizar para cualquier clase de responsable, sea éste del sector público o privada e independientemente del tipo de tratamiento de datos personales que realice. [187] De lo anterior se desprende por una parte la obligación de realizar las evaluaciones de impacto, pero por otra se continúa dejando en un estado de incertidumbre a los titulares de los datos biométricos, es decir, no existe un

[186] INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES, *Guía para el Tratamiento de Datos Biométricos*, INAI, México, 2018, p. 58.
[187] *Cfr., Idem.*

mecanismo vinculante que obligue y que regule el tratamiento directo de los datos biométricos.[188]

En sintonía con el párrafo que antecede, la evaluación de impacto referida únicamente obliga a realizarla pero no impide la vulneración a los derechos sustantivos relativos a la protección de datos personales, identidad e intimidad, por el contrario, sólo se permite conocer qué tanto el tratamiento puede afectar a los derechos de titular, y conoce la vulneración de los mismos, no así para generar mecanismos que fehacientemente permitan la protección de los derechos.

No es óbice a lo anterior que dentro del contenido de la misma guía se refiere a lo precisado en el párrafo que antecede que:

Solo se emitirán recomendaciones no vinculantes sobre la evaluación de impacto en la protección de datos personales presentado por el responsable obligado en términos Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, dentro de los 30 días siguientes contados a partir del día siguiente a su presentación, recomendaciones que como se señala no tienen el carácter de obligatorio ante los sujetos obligados, pero que hasta cierto punto pueden marcar un camino que pueden o no seguir los responsables. Los responsables regulados por la Ley Federal de Protección de Datos Personales en Posesión de Particulares, es decir, particulares, pueden decidir voluntariamente realizar una evaluación de impacto en la protección de datos personales no requerirán presentarla ante el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, derivado de esto, existe un rango amplio de posibilidades para que sucede.[189]

---

[188] *Idem.*

[189] *Cfr.* INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES, *Guía para el Tratamiento de Datos Biométricos*, *op. cit.,* p. 59.

Y finalmente de lo relativo al uso de sistemas biométricos dentro de una organización, se recomienda:

> A todos los responsables realizar una evaluación de impacto en la protección de datos, para determinar riesgos relacionados con el tratamiento de los datos biométricos y analizar las posibilidades de efectuar medidas para mitigar dichos riesgos, recomendación en el mismo sentido no genera obligación de los responsables. Asimismo, se señala que para realizar la evaluación de impacto en la protección de datos personales deberá considerarse el propósito del sistema y su contexto, este análisis puede también desarrollarse mientras el sistema opere con el objeto de realizar los cambios y modificaciones cuando éstos resulten necesarios.[190]

Recomendaciones que sin lugar a dudas consolidan un paso para la protección de los datos biométricos, pero dado objetivo final de exclusivamente referirse a una evaluación de impacto y al no ser vinculantes, carecen de cualquier significancia jurídica que permita a los titulares ejercitar acciones para hacer valer sus derechos sustantivos.

Conclusivamente y en concordancia con el capítulo segundo y tercero se resalta que actualmente conforme al marco regulatorio nacional y el internacional aplicable al país no existen mecanismos reales protectores y que limiten el uso de los sistemas biométricos como forma de identidad y de otorgar el consentimiento para la celebración de actos jurídicos, pese a los esfuerzos del órgano garante de emitir recomendaciones y guías para su tratamiento, entonces se torna necesario que dentro del marco jurídico se contemplen obligaciones al respecto y que permitan delimitar el uso de los datos biométricos, por tratarse de un aspecto inherente a todas las personas y que forman parte esencial de la identidad.

---

[190] *Cfr., Idem.,* pp. 59 y 60.

IV.2. EL SISTEMA JURÍDICO MEXICANO FRENTE A LOS SISTEMAS BIOMÉTRICOS

En este rubro inicialmente se estudiarán las repercusiones y se analizará el valor que tienen los datos biométricos usados como forma de identidad y de consentimiento para actos jurídicos, también se abordarán los riegos en materia de ciberseguridad y delitos informáticos que atañen en el plano fáctico y que permiten inducir los problemas en relación con vulneración a derechos fundamentales de los usuarios de los sistemas biométricos.

IV.2.1.LA VALIDACIÓN Y ALCANCE JURÍDICO DE LA IDENTIFICACIÓN A TRAVÉS DE LOS SISTEMAS BIOMÉTRICOS

Hablar de validación de la identificación exige distinguir entre tres conceptos que podrían llegar se confundirse: la identificación, la autenticación y para efectos de la investigación el consentimiento para la celebración de actos jurídicos, dada la relevancia se precisa en términos de los siguientes párrafos.

La identidad desde la perspectiva de los datos biométricos como se definió en el primer capítulo, por Díaz Vanessa es:

> La identificación basada en el sistema biométrico de reconocimiento, consiste en utilizar un dato y compararlo con una lista o base de datos; generalmente se utiliza cuando se desconoce la identidad de un individuo y se requiere averiguarla; por ejemplo, cuando se encuentra una huella en la escena del crimen, se realiza la cadena de custodia para su resguardo, y se permite la identificación del individuo comparando esa huella que se obtuvo con una base de datos de las huellas dactilares de o de cualquier otro dato biométrico obtenido, buscando la compatibilidad.[191]

[191] *Cfr.* DÍAZ RODRÍGUEZ, Vanessa, *Licencia biométrica, caja de pandora, Hechos y Derechos,* México, UNAM, Instituto de Investigaciones Jurídicas, 2013, núm. 16, disponible en: <https://revistas.juridicas.unam.mx/index.php/hechos-y-derechos/article/view/6867/8803 > [Consulta: 29-enero-2022].

Por lo que atañe a los procesos de autenticación y efectuando una metodología de investigación analítica, para Díaz Vanesa:

> La autenticación se basa en el sistema biométrico de verificación, el cual sólo utiliza un dato comparado con el mismo previamente almacenado, es decir, que a comparación con la identidad, en la autenticación se conoce la identidad de una persona y este proceso permite que a través de un dato biométrico previamente almacenada en una base conocida, efectúe el ejercicio comparativo y permite decir fehacientemente si una persona es quien dice ser.[192]

También el proceso de autenticación es definido por la Organización para la Cooperación y el Desarrollo Económicos, por sus siglas OCDE como: "una función que establece la validez y por la cual se puede asegurar la identidad de un usuario, aparato u otra entidad."[193]

Conviene distinguir los tres aspectos señalados, por la importancia que tienen cada uno de ellos en relación con el uso de datos biométricos, además que los procesos de identidad, autenticación y consentimiento no deberían ejecutarse en simultaneidad, en la inteligencia, que cada uno de ellos tiene un objetivo diferente, por lo que siendo una práctica común en plataformas denominadas como banca móvil es denominador que exclusivamente se pida una sola vez ingresar al sistema el dato biométrico, es decir, identificarse, ejecutar los sistemas de autenticación que permiten saber que una persona es quien dice ser, y celebrar actos jurídicos, realizar depósitos, retiros y transferencias, cuestiones que tienen naturaleza y rigor jurídico diferente entre cada una de ellas.

---

[192] *Cfr., Idem.*

[193] ORGANIZACIÓN PARA LA COOPERACIÓN Y DESARROLLO ECONÓMICOS, *Recommendation on electronic authentication and OECD guidance for electronic authentication*, OCDE, 2007, p. 16, disponible en: <http://www.oecd.org/sti/ieconomy/38921342.pdf > [Consulta: 02-febrero-2022].

Resaltando lo anterior que los tres procedimientos por seguridad del usuario, así como por cuestiones inherentes a los derechos de derechos humanos a la protección de los datos personales, identidad, intimidad y los derechos de acceso, rectificación, cancelación y oposición deben forzosamente ejecutarse por procesos automatizados por separado, toda vez que si se ejecutan en un mismo movimiento o exclusivamente al ingreso de una plataforma digital los procesos no están completamente protegidos y cuanto menos son diferenciados.

Por lo tanto conforme al vacío jurídico, en caso de controversia daría lugar a argumentar que el cliente al ingresar su datos biométricos que no quiso identificarse, autenticarse o celebrar actos jurídicos, por lo que conforme a la teoría general de las obligaciones, este consentimiento se adolece de un vicio, aduciendo una confusión entre la identidad, autenticación y el consentimiento, dando lugar a concluir que nunca pudo ser su deseo obligarse en términos del acto que lo indujeron a celebrar, ya que solamente se estaba autenticando o identificando.

Lo antes mencionado, no sólo implica una inseguridad para el usuario de la plataforma o el cliente, sino que involucra un perjuicio para la Institución de Crédito o empresa que celebra actos electrónicamente, siendo una consecuencia de este vacío legal que para el caso de una controversia donde se demande el cumplimiento de alguna obligación contraída por medios electrónicos, se podría configurar una nulidad del acto cuya causa sea un vicio en el consentimiento por haber inducido al error a una de las partes del mismo, lo que se puede traducir en una pérdida de quien prestó el servicio, o quien entregó una mercancía, porque una vez ejecutado el servicio ha implicado un gasto a la empresa y también se dejan de percibir las ganancias del mismo, además de generar desconfianza entre los usuarios por la inseguridad que implica la celebración de actos jurídicos vía electrónica.

Hasta este momento toma importancia el reconocimiento y valor que tienen los datos biométricos en celebración de los actos jurídicos, aunado a su valor como datos personales, y finalmente, conforme a los capítulos anteriores se reconoce la

relevancia de tomar en consideración si el uso de los datos biométricos como mecanismo para otorgar el consentimiento yace en el efecto, naturaleza y alcance jurídico que éste tiene en la celebración de actos jurídicos.

Tomando en cuenta lo alcanzado en el capítulo segundo, se está en la presencia del consentimiento como un elemento de existencia de este acto jurídico, por lo que cualquier vicio de este da lugar a una nulidad del mismo, y recordado que el uso de datos biométricos a través de medios electrónicos se considera en equivalencia con el consentimiento expreso, y como fue descrito en el capítulo tercero la Ley Federal citada para: "el tratamiento de los mismos como datos sensibles el consentimiento debe otorgarse por escrito,"[194] que podría caerse en un camino circular para su protección, concluyendo que el consentimiento para tratar los datos sensibles, como los datos biométricos, a través de los mismos datos biométricos, y debe prevalecer la diferenciación de los procesos descritos en el presente apartado.

IV.2.2. USURPACIÓN DE IDENTIDAD POR MEDIOS ELECTRÓNICOS

La usurpación de la identidad de las personas es un delito previsto por la legislación mexicana, y en relación con la investigación se prevé pueda ser efectuada por medios digitales, y como ha quedado precisado, es posible identificar e incluso autenticar a una persona por medio de los datos biométricos, entonces se parte de la premisa general que la usurpación de identidad implica un riesgo para los derechos sustantivos de las personas que se identifican a través del uso de los datos biométricos y que celebran actos jurídicos.

Como introducción del apartado y a manera de dotar de importancia a la investigación, Rodolfo Romero Flores dice que:

[194] *Cfr.* artículo 8. Ley Federal de Protección de Datos Personales en Posesión de los Particulares.
Todo tratamiento de datos personales estará sujeto al consentimiento de su titular, salvo las excepciones previstas por la presente Ley.
El consentimiento será expreso cuando la voluntad se manifieste verbalmente, por escrito, por medios electrónicos, ópticos o por cualquier otra tecnología, o por signos inequívocos.

> En la actualidad Internet ha propiciado el surgimiento de la identidad electrónica o identidad digital, que fundamentalmente está constituida por datos personales sensibles que pueden incluir claves de acceso a cuentas bancarias o redes, mediante los cuales las personas se comunican u operan en redes informáticas o telemáticas y cuya circulación transfronteriza es potencialmente peligrosa ante su posible apropiamiento no autorizado. De igual forma, la identidad puede asumir distintas vertientes, tales como la identidad genética o biológica, la identidad sexual, la identidad cultural, entre otras.[195]

De la cita realizada se establece la importancia que tiene la usurpación de identidad dentro del sistema jurídico informático, mismo que como se estudió tiene implicaciones directas a la identidad, autenticación y forma de otorgar el consentimiento en los actos jurídicos.

La usurpación de identidad, se encuentra prevista en términos del artículo 211 Bis del Código Penal para el Distrito Federal hoy Ciudad de México, artículo que fue adicionado por Gaceta Oficial de la Ciudad de publicación del 10 de marzo del 2014, y en su tipo penal contempla la conducta de: "[…]la usurpación con fines ilícitos de la identidad de otra persona u otorgue su consentimiento para llevar a cabo la usurpación en su identidad, estableciendo una penalidad de 1 a 5 años de prisión y de 400 a 600 días multa,"[196] recordando que en sistema de justicia penal actual, se pondera la reparación del daño que se ocasione, en este tenor, se vuelve complicado la cuantificación del monto por concepto de reparación de daño porque en el entiendo el bien jurídico tutelado es la identidad, e implícitamente la intimidad y la protección de datos personales.

---

[195] ROMERO FLORES, Rodolfo, *El robo o Usurpación de Identidad por Medios Informáticos o telemáticos: su tratamiento jurídico penal*, México, Instituto de Investigaciones Jurídicas, UNAM, , p. 304, disponible en: <https://archivos.juridicas.unam.mx/www/bjv/libros/6/2958/20.pdf> [Consulta: 04-febrero-2022].

[196] *Cfr.* artículo 211 Bis. Código Penal para el Distrito Federal.
Al que por cualquier medio usurpe, con fines ilícitos, la identidad de otra persona, u otorgue su consentimiento para llevar a cabo la usurpación en su identidad, se le impondrá una pena de uno a cinco años de prisión y de cuatrocientos a seiscientos días multa. Se aumentarán en una mitad las penas previstas en el párrafo anterior, a quien se valga de la homonimia, parecido físico o similitud de la voz para cometer el delito establecido en el presente artículo.

Al respecto de la porción normativa citada no existen a la fecha criterios emitidos por los órganos jurisdiccionales en México, situación que puede ser con motivo de dos razones: primera, la falta de aplicación del tipo penal en el plano fáctico, es decir, que hasta el momento existen pocas conductas que se encuadren en la hipótesis punitiva o; segundo, que el tipo penal se adecua perfectamente en la conducta y se aplica exactamente como la ley lo establece y que no ha sido necesario realizar interpretaciones o adecuaciones judiciales al respecto del tipo penal en mención, además se trae a colación que en materia penal rige el principio de exacta aplicación de la ley.

Es importante ejecutar un estudio cualitativo del precepto normativo, específicamente del párrafo segundo del artículo 211 Bis del Código Penal para el Distrito Federal, aplicable para la Ciudad de México, donde se contemplan agravantes para el delito de usurpación de identidad, aumentando las penas en una mitad, a quien se valga de la homonimia, parecido físico o similitud de la voz para cometer el delito, aspectos que incrementan el tipo penal y de una hipotética interpretación sistemática y funcional, que no es permitida en materia penal, incorporan el uso de los datos biométricos, siendo posible similitudes en la voz o en su caso por la capacidad de la base de datos y fidelidad del ejercicio comparativo y de autenticación que existan datos biométricos registrados como similares.

Al respecto y conforme al marco regulatorio analizado, Rodolfo Romero establece que:

> La suplantación de identidad obliga a acciones legislativas que permitan establecer normativamente un serie de conductas típicas, antijurídicas y sancionables en las legislaciones sustantivas penales; en virtud de que con los instrumentos jurídico-penales vigentes en la mayor parte de los países incluyendo México, no es factible abordar un tratamiento penal de las conductas

vinculadas a la suplantación de identidad y, por ende, no existe seguridad jurídica.[197]

Partiendo de un estudio legislativo y comparativo a nivel nacional en diversas entidades federativas del país en sus códigos sustantivos en materia penal se han establecido diversos presupuestos para el delito de robo y de usurpación de identidad, además de lo analizado respecto de la Ciudad de México, por lo que partiendo de la metodología legislativa en cada entidad federativa, de los Código Penales se tiene que los Estados de Aguascalientes, Baja California, Baja California Sur, Chihuahua, Guanajuato, Hidalgo, Michoacán, Quinta Roo, Sinaloa, Sonora, Tamaulipas, Tlaxcala y Zacatecas, contienen en sus hipótesis normativas el tipo penal de usurpación de la identidad, a continuación se describen los preceptos normativos referentes al delito de robo y de usurpación de identidad:

Del Código Penal para el Estado de Aguascalientes, en su artículo 181 establece el tipo penal del acceso informático indebido, teniendo como hipótesis normativas y verbo rector los siguientes: “acceder a la información contenida en un aparato para el procesamiento de datos, y él; interferir el buen funcionamiento de un sistema operativo, programa de computadora, base de datos o cualquier archivo informático, sin autorización de su propietario o poseedor legítimo.”[198], artículo que fue reformado el 28 de noviembre de 2018, imponiendo en caso de cometer la conducta típica de 3 a 6 meses de prisión, y como agravante establece que si el sujeto activo es el responsable del mantenimiento o seguridad del sistema de información prevé la pena de 6 meses a 1 año de prisión.

En la misma tesitura, el artículo 181 A del Código Penal para el Estado de Aguascalientes, prevé el delito de suplantación de identidad, y establece en su conducta el usurpar o sustituir a otra persona a través de cualquier medio, utilizando sin consentimiento, sus datos personales con fines ilícitos o lucrativos, aun cuando

[197] *Op.cit.* ROMERO FLORES, Rodolfo, *El robo o Usurpación de Identidad por Medios Informáticos o telemáticos: su tratamiento jurídico penal*, p. 305.
[198] *Cfr.* artículo 181 del Código Penal del Estado de Aguascalientes.

estos no se logren.[199] En adición que también contempla como usurpación no sólo cuando este uso se haga sin el consentimiento del titular de la identidad, sino que también cuando el titular consienta que se utilice su identidad por un tercero, correspondiendo en ambos supuestos una pena de 4 a 12 años de prisión.

Del Código Penal para el Estado Libre y Soberano de Baja California Sur en el capítulo V, por reformas del 31 de julio de 2021, se contempló la usurpación de identidad, regulando en sus artículos 363 y 364 las hipótesis normativas referentes a este delito, estableciendo como verbo rector a quien usurpe o suplante la identidad de una persona, [200] y en adición el artículo 364 de la Codificación en cita, establece la equiparación de la usurpación, en los aspectos que interesan contemplando: "el uso de medios telemáticos o informáticos, valiéndose de alguna manipulación informática o de intersección de datos, accese a base de datos automatizadas no autorizadas y lleve a cabo el empleo no autorizado de datos personales o suplante identidades y obtenga un lucro indebido para sí o para otro;"[201] estableciendo en este supuesto agravantes.

En relación al Código Penal del Estado de Chihuahua, por reformas del 23 de octubre de 2021, se adicionó el capítulo VI, referente a la usurpación de identidad, estableciendo en un solo artículo la siguiente hipótesis normativa: "A quien por cualquier medio usurpe, con fines ilícitos, la identidad de otra persona, se le impondrá prisión de seis meses a tres años y de ochenta a trescientos días multa."[202]

---

[199] *Cfr.* artículo 181 A Código Penal para el Estado de Aguascalientes.

[200] Artículo 363 del Código Penal para el Estado Libre y Soberano de Baja California Sur.
Usurpación de identidad. Al que por cualquier medio incluyendo el informático, usurpe o suplante a otro con fines ilícitos, para ejercer un derecho que legítimamente pertenezcan a otro o de apropiamiento de la identidad de otra persona, se le impondrá una pena de tres a seis años de prisión y multa de quinientos a seiscientos días. La misma pena se impondrá a quien otorgue su consentimiento para que con fines ilícitos, otro lleve a cabo la usurpación de su identidad.

[201] *Cfr.* artículo 364 fracción I del Código Penal para el Estado Libre y Soberano de Baja California Sur.

[202] *Cfr.* artículo 206 Ter del Código Penal del Estado de Chihuahua.

En similar sentido en el Código Penal del Estado de Guanajuato el 11 de septiembre de 2015, se adicionó el capítulo único referente a la usurpación de identidad y en sólo en el artículo 214-a, se contempló el tipo penal de la siguiente forma:

> A quien empleando cualquier medio y sin el consentimiento de quien legalmente deba otorgarlo se haga pasar por otra persona, utilice su identidad, ejerza sus derechos o se apropie de sus datos personales, o siendo titular de éstos, otorgue su consentimiento para que se efectúen dichas conductas, en beneficio propio o de un tercero, o para producir un daño al titular de la identidad, a su patrimonio, o a persona ajena, se sancionará con pena de prisión de uno a cinco años y de diez a cincuenta días multa.[203]

Y aportando a esta investigación se consideró como agravante de la penalidad cuando se demuestre que el sujeto activo tenga experiencia en las ramas tecnológicas o de ingeniería, además contemplando que es agravante para la comisión del delito ser empleado en cualquier institución bancaria, financiera o crediticia.

Del Código Penal para el Estado de Hidalgo en su último artículo, esto es, el 370, contempla en similitud el delito de usurpación a la identidad, y en lo que suma a este trabajo se destaca que establece que: ”Comete el delito de usurpación de identidad quien por sí o por interpósita persona, por cualquier medio y con fines ilícitos, se apodere, apropie, transfiera, utilice o disponga de datos personales de otra persona sin autorización de su titular u otorgue su consentimiento para llevar a cabo la usurpación de su identidad, en beneficio propio o de un tercero.”[204] Resaltando que se incorpora el uso de datos personales.

[203] *Cfr.* artículo 214-a del Código Penal para el Estado de Guanajuato.
[204] *Cfr.* artículo 370 del Código Penal para el Estado Hidalgo.

También el Código Penal para el Estado de Michoacán de Ocampo, sólo en el artículo 301 bis, regula lo relacionado al delito de usurpación de identidad, contemplando en similitud con Código Penal del Estado de Hidalgo, el uso de datos personales para realizar actos jurídicos.

Del Código Penal para el Estado Libre y Soberano de Quintana Roo por reformas del 06 de septiembre de 2013, se adicionó el capítulo VI relacionado a la usurpación de identidad, el cual contiene regulaciones similares a las que se han reseñado anteriormente.

Del Código Penal para el Estado de Sonora, se contempla la usurpación de identidad en los artículos 241 Bis, 241 Bis 1 y 241 Bis 2, destacando que en el artículo 241 Bis 1, el espíritu legislador realizó un listado de aquellos documentos con los que se puede usurpar la identidad de la persona, destacando de las fracciones XXVI y XVVII que se reguló el uso de la firma electrónica y de cualquier otra información o documento que identifique electrónicamente a un individuo o en su caso le permita el acceso a sus bienes o patrimonio, sirviendo como base para sostener la investigación, relacionado con el uso de la firma electrónica y el permitir celebrar actos jurídicos.

El Código Penal para el Estado de Tamaulipas, en su artículo 263 Bis, contempla el delito de robo de identidad, y en su tipo penal se establece que: “Comete el delito de robo de identidad, quien por cualquier medio usurpe o suplante la identidad de una persona con fines ilícitos a través de medios electrónicos, informáticos, redes sociales o cualquier otro medio de comunicación, con el propósito de causar un daño patrimonial, moral, psicológico, ya sea para beneficio propio o de otra persona.” [205] Resaltando que establece la comisión del hecho delictivo por el uso de medios electrónicos, informáticos o incluso de las redes sociales.

[205] *Cfr.* artículo 263 Bis del Código Penal del Estado de Tamaulipas.

En similitud de las demás codificaciones estatales, el artículo 282 del Código Penal del Estado Libre y Soberano de Tlaxcala establece el delito de usurpación de identidad.

Del Código Penal para el Estado de Zacatecas, por reformas de publicación de 4 de agosto del 2012, se incorporaron en el Capítulo VI disposiciones relativas a la falsificación y usurpación de identidad, y específicamente el artículo 227 establece 4 fracciones en las que se contienen los supuestos normativos para la tipificación de este delito: primero, al que oculte su nombre o apellido y tome otro imaginario o el de otra persona, al declarar ante una autoridad; segundo, al que para eludir la práctica de una diligencia judicial o administrativa o una notificación de cualquier clase o citación de una autoridad, oculte su domicilio, designe otro distinto o niegue de cualquier modo el verdadero; tercero, al funcionario o empleado que en los actos propios de su cargo, atribuyere a una persona determinada título o nombre, a sabiendas que no le pertenece y con perjuicio de alguien; y cuarto, al que por cualquier medio manifieste ante la autoridad una nacionalidad falsa, conductas típicas que se sancionan con 1 a 3 años de prisión de con multa de 100 a 300 cuotas, mismas que guardan mayor relación con las manifestaciones que efectúen ante las autoridades que mencionan.

Y del correlativo artículo 227 Bis del Código Penal para el Estado de Zacatecas, se establece la tipificación de la conducta de: “quien ejerza ilícitamente un derecho o use cualquier tipo de datos, informaciones o documentos que legítimamente pertenezcan a otro, que lo individualiza ante la sociedad y que le permite a una persona física o jurídica colectiva ser identificada o identificable, para hacerse pasar por él,”[206] delito que se sanciona con pena privativa de libertad de 1 a 4 años y multa de 200 a 300 cuotas.

[206] *cfr*. artículo 227 bis del Código Penal para el Estado de Zacatecas.
Se sancionará con prisión de uno a cuatro años y multa de doscientas a trescientas cuotas, a quien ejerza ilícitamente un derecho o use cualquier tipo de datos, informaciones o documentos que legítimamente pertenezcan a otro, que lo individualiza ante la sociedad y que le permite a una persona física o jurídica colectiva ser identificada o identificable, para hacerse pasar por él.

Y en comparación con la legislación aplicable en la Ciudad de México, se equiparan a la usurpación de identidad y se impondrán las mismas penas citadas a quienes: "[…] otorguen el consentimiento para llevar a cabo la usurpación de identidad o se valgan de la homonimia, parecido físico o similitud de la voz para cometer algún ilícito,"[207] por lo que, existe similitud en la tipificación con la Ciudad de México.

Del Código Penal para el Estado de Sinaloa, se adicionó al Título Sexto relativos a los delitos contra la inviolabilidad del domicilio, de la intimidad y de la identidad de las personas, el Capítulo III referente a la suplantación de identidad, por reformas del 25 de mayo del 2015, específicamente interesa conocer el contenido de los artículos 177 Bis, 177 Bis A y 177 Bis B, en los que casi en similitud con los Códigos Penales citados establece la tipificación para el delito de usurpación, también denominado suplantación de identidad, y se destaca que específicamente se abunda en el tipificación de: "uso de medios informáticos, telemáticos o electrónicos, a través de internet, cualquier sistema informático también refieren el empleo no autorizado de datos personales o el acceso no autorizado a bases de datos automatizadas para suplantar identidades; así como, se contempla el tratamiento de datos identificativos, o medio de comunicación,"[208] tutelando principalmente la identidad de una persona física.

Se equiparán a la usurpación de identidad y se impondrán las mismas penas previstas en el párrafo anterior a quienes otorguen el consentimiento para llevar a cabo la usurpación de identidad o se valgan de la homonimia, parecido físico o similitud de la voz para cometer algún ilícito.
Las sanciones previstas en este artículo se impondrán con independencia de las que correspondan por la comisión de otro u otros delitos.

[207] *Cfr.* artículo 227 Ter del Código Penal para el Estado de Zacatecas.
Las penas señaladas en el artículo anterior se incrementarán hasta en una mitad, cuando la usurpación sea cometida por un servidor público aprovechándose de sus funciones, o por quien sin serlo, se valga de su profesión o empleo para ello.

[208] *Cfr.* Artículo 177 BIS. Código Penal para el Estado de Sinaloa
A quien por cualquier medio suplante la identidad de otra persona, con fines ilícitos o de lucro para sí o para otra, u otorgue su consentimiento para llevarla a cabo, se le impondrá prisión de seis meses a tres años y de cuatrocientos a seiscientos días multa.
Artículo 177 BIS A. Código Penal para el Estado de Sinaloa
Será equiparable al delito de suplantación de identidad y se impondrán las mismas penas previstas en el artículo anterior: I. Al que por algún uso de medio informático, telemático o electrónico, obtenga algún lucro indebido para sí o para otro o, genere un daño patrimonial, mediante el empleo no

En el Estado de Baja California el Código Penal para el Estado de Baja California, establece en su Título Tercero denominado delitos contra la inviolabilidad del secreto y de los sistemas y equipos de cómputo y protección de los datos personales, con reforma de fecha 12 de noviembre del 2021, en específico en el artículo 175 Quinquies, el tipo penal de la conducta consistente: "al que por cualquier medio usurpe o suplante con fines ilícitos o de lucro, la identidad de otra persona, u otorgue su consentimiento para llevar a cabo la usurpación o suplantación en su identidad,"[209] y en el mismo sentido de las agravantes previstas en los Códigos locales precitados considera la homonimia, parecido físico o similitud de la voz para cometer el delito, e abunda en la agravante que el sujeto activo del delito tenga licenciatura, ingeniería o cualquier otro grado académico reconocido en el rubro de la informática, telemática o sus afines.

Continuando con la cita del párrafo anterior, se equiparan al delito de usurpación o suplantación de identidad los mismos presupuestos que se analizaron para el Código Penal para el Estado de Sinaloa, considerándose se sigue la línea legislativa en considerar como medios para la realización del ilícito los medios digitales,

---

autorizado de datos personales o el acceso no autorizado a bases de datos automatizadas para suplantar identidades; II. A quien transfiera, posea o utilice, sin autorización de quien deba otorgarla, datos identificativos de otra persona con la intención de cometer, intentar o favorecer cualquier actividad ilícita; y III. Al que asuma, se apropie o utilice indebidamente a través de internet, cualquier sistema informático, o medio de comunicación, la identidad de una persona física o jurídica que no le pertenezca para ostentarse como tal sin consentimiento de éste, ya sea en beneficio propio o de un tercero.

Artículo 177 BIS B. Código Penal para el Estado de Sinaloa Las penas previstas para el delito de suplantación de identidad o su equiparación se aumentarán hasta en una mitad más, cuando quien lo cometa se valga de la homonimia, parecido físico o similitud de la voz; sea servidor público y se aproveche de sus funciones; o, quien sin serlo se valga de su profesión o empleo para ello.

[209] *Cfr.* artículo 175 Quinquies del Código Penal para el Estado de Baja California.

Tipo y punibilidad. - Al que por cualquier medio usurpe o suplante con fines ilícitos o de lucro, la identidad de otra persona, u otorgue su consentimiento para llevar a cabo la usurpación o suplantación en su identidad, se le impondrá pena de seis meses a seis años de prisión y de cuatrocientos a seiscientos días multa.

Se aumentarán en una mitad las penas previstas en el párrafo anterior, a quien además se valga de la homonimia, parecido físico o similitud de la voz para cometer el delito así como en el supuesto de que el sujeto activo del delito tenga licenciatura, ingeniería o cualquier otro grado académico reconocido en el rubro de la informática, telemática o sus afines.

Serán equiparables al delito de usurpación o suplantación de identidad y se impondrán las penas establecidas por este artículo, cuando se actualicen las siguientes conductas: [...]

internet y tecnologías de la información, siendo esta la legislación más actual que se incorpora en una legislación estatal y que evidentemente frente a la legislación de la Ciudad de México, ya contempla aspectos tecnológicos para la realización del delito de usurpación de identidad. Finalmente de esta legislación sustantiva local debe destacarse que realiza una separación de la tutela con delitos contra la intimidad y la imagen.

De las anteriores citas a los Códigos Penales de las Entidades Federativas se logra advertir un avance en la tarea legislativa, y con similitudes en el tipo penal que establecen en algunos casos los medios para la comisión del delito de usurpación de identidad, principalmente mediante el uso de tecnología de la información y sistemas digitales, presuponiendo entonces un avance para la problemática que se plantea en este trabajo de investigación, pero esto no resulta así en el ámbito federal.

Bajo esta misma línea de investigación y en una necesidad de una robusta hipótesis normativa que permita, prevenga y en su caso tratara de erradicar el delito de usurpación de identidad, el 14 de octubre del 2021 se presentó iniciativa que adicionaba diversas disposiciones al Código Penal Federal, en materia de robo de identidad, a cargo del diputado Vicente Alberto Onofre Vázquez, en la que se sostiene la adición del Capítulo III Quáter y el artículo 390 Ter del Código Penal Federal, en el cual se propuso que quedaría en los siguientes términos:

> Comete el delito de robo de identidad el que por cualquier medio obtenga datos personales o financieros con el objetivo de suplantar la identidad de un tercero, con la finalidad de obtener algún beneficio para sí o para otra persona en perjuicio del patrimonio de la persona suplantada, o para la comisión de cualquier otro delito. A quien cometa este delito, se le impondrá pena de seis a diez años de prisión y hasta doscientos días multa, sin perjuicio de las penas que correspondan por otros delitos que resulten. Lo dispuesto en este artículo se

aplicará sin perjuicio de las medidas y sanciones administrativas que establezcan las leyes correspondientes.[210]

Reforma al precepto normativo que fue propuesto en materia federal, y en la exposición de motivos de la iniciativa referida se estableció que:

> El delito de robo no sólo se limita a cometer hechos ilícitos en materia económica, generando daños patrimoniales en perjuicio de las víctimas, sino también sus alcances llegan a ser mucho más amplios, toda vez que la información y datos personales que fueron robados son aprovechados por el delincuente para suplantar la identidad de la tercera persona y cometer otros actos ilícitos de mayor o menor impacto, advirtiéndose que existe una diferencia en el robo de identidad y usurpación, por lo que en el aparado que siguiente al presente se abordara esta distinción, así mismo se establece en la iniciativa que a pesar de que el robo de identidad presenta gran incidencia en todo el país, aún no se encuentra tipificado a escala federal.[211]

Ahora bien, en materia Federal si existe una regulación que podría equiparse, como fue estudiado en el capítulo tercero de la investigación la Ley Federal de Protección de Datos Personales en Posesión de los Particulares regula el presupuesto de los delitos en materia del tratamiento de datos personales, pero se tiene que recordar que por el ámbito de aplicación de la Ley Federal en comento, las hipótesis normativas no son aplicables para quienes incurran en el robo o en su caso usurpación de identidad, toda vez que son sujetos de la ley las personas físicas o morales de carácter privado que lleven a cabo el tratamiento de datos personales y las personas que lleven a cabo la recolección y almacenamiento de datos personales, que: “sea para uso exclusivamente personal, y sin fines de divulgación

---

[210] *cfr.* Iniciativa que adiciona diversas disposiciones al Código Penal Federal, en materia de robo de identidad, a cargo del diputado Vicente Alberto Onofre Vázquez, del grupo parlamentario de Morena, del 14 de octubre del 2021, disponible en: <http://sil.gobernacion.gob.mx/Archivos/Documentos/2021/10/asun_4234504_20211014_1634235907.pdf > [Consulta: 08-febrero-2022].
[211] *Cfr., Idem*.

o utilización comercial,“[212] junto con sus excepciones ya estudiadas, por lo tanto deviene de una importancia para su regulación por el derecho penal y su tutela judicial para proteger los datos personales incluidos los datos biométricos en el ámbito federal.

Al respecto de la importancia de una mayor legislación penal Rodolfo Romero establece que:

> El también denominado “robo de identidad”, “usurpación de identidad”, “suplantación de identidad”, “falsificación de la identidad y su uso indebido”, de acuerdo con investigaciones internacionales realizadas por el Consejo Económico y Social (ECOSOC) de la Organización de la Naciones Unidas, la Unión Europea y la Organización para la Cooperación y el Desarrollo Económicos (OCDE), es el delito de más rápido crecimiento en el mundo sin que existan acciones legislativas concretas y políticas públicas acertadas para sancionar esta conducta atípica en el plano penal.[213]

De lo anterior se desprende que, el delito de usurpación de identidad es uno delitos que más se ejecuta en el mundo y que mayor avance tecnológico-legislativo se requiere para su prevención y sanción, además de ser un delito que al igual que muchos tutela derechos humanos insertos en el tipo penal, siendo el caso de la intimidad, identidad, protección de datos, por lo que este delito advierte vulneraciones a los sistemas informáticos que contengan y almacenen los datos biométricos de las personas, y contrario a la creencia de mayor seguridad y fiabilidad en su uso para identificarse, autenticarse o celebrar actos jurídicos, el robo de identidad se sobrepone a cualquier beneficio que su uso pudiera tener.

Bajo esta misma línea argumentativa, los delitos relacionados al uso de medio electrónicos, incluyendo la usurpación de identidad, constantemente el tipo penal

---

[212] *Cfr.* artículo 2º de la Ley Federal de Protección de Datos Personales en Posesión de Particulares.
[213] *Op.cit.* ROMERO FLORES, Rodolfo, *El robo o Usurpación de Identidad por Medios Informáticos o telemáticos: su tratamiento jurídico penal*, p. 305.

se verá superado por la evolución imparable de los delitos con aplicación de tecnologías de la comunicación e información, más aún si estas tienen un enfoque a la sistematización y automatización de los procesos de identificación y autenticación, porque existen cada vez un mayor número de atentados contra los datos personales sensibles, datos biométricos que se contienen en diversas bases de datos ya sean de entes públicos o privados, y esto sin lugar a dudas se relaciona directamente con una violación a la identidad, intimidad y protección de datos personales a través de los medios y tecnologías de la información.

Finalmente se llega a la conclusión que la usurpación de identidad como un delito contemplado en diversas entidades federativas, es una respuesta a la realidad social que acontece en el país, en virtud de resolver los problemas de identidad, protección de datos personales, intimidad, vulneración de los derechos de acceso, rectificación, cancelación y oposición, y demás que se relacionan directamente con el uso de tecnologías de la información, sistemas informáticos, bases de datos que contienen datos biométricos, que cada día es más común su uso por la mayoría de la población y que además se han convertido en requisitos para poder acceder a servicios y bienes ofertados a través de plataformas digitales.

IV.2.3. ROBO DE LOS DATOS Y SISTEMAS BIOMÉTRICOS DE LA PERSONA

En relación con el apartado anterior, el robo de los datos biométricos como datos personales sensibles debe ser considerado como un tema de importancia para la legislación en materia penal, debe ponderarse la tutela de acceso a los datos personales contenidos en medios electrónicos, mismos que su protección es reconocida por la Constitución Política de los Estados Unidos Mexicanos, más aún cuando el tratamiento de los mismos se efectúa de manera no autorizada, y en el mismo tenor, no sólo debe ser considerado como delito el obtener y almacenar los datos sensibles sin autorización, sino que debe tutelarse la titularidad de los mismos y las protecciones y disposiciones que se estudiaron en el capítulo tercero de la investigación, así como la tutela de los derechos de acceso, rectificación,

cancelación y oposición, con mecanismos punitivos y restaurativos que permitan su protección.

Al respecto Romero Flores refiere que:

> El binomio tecnología-usurpación de identidad demuestra que la utilización está cada vez más extendida de dispositivos tecnológicos de telecomunicación genera la ausencia o presencia directa de las personas que puede ser aprovechada para la comisión de delitos, también refiere que actualmente se cuenta con un manejo suficiente de los instrumentos tecnológicos que presentan mayores oportunidades de fraude, es decir, mayores posibilidad técnicas y distancia entre los sujetos, se da lugar en muchos de los casos a una falta de control de la identidad, resultando de una metodología inductiva que la novedad tecnológica-delincuencial y la incertidumbre que se genera en torno a su tratamiento jurídico-penal, cabe plantear la relevancia de estas conductas, y, en su caso, determinar legislativamente los hechos punibles vinculados al robo o usurpación de identidad.[214]

También en el mismo sentido que lo estudiado Rodolfo Romero advierte que: "la acción legislativa tiene un efecto correctivo-punitivo tendría que ser acompañado de políticas públicas de carácter preventivo, buscando la responsabilidad y advertir a la ciudadanía del problema de este tipo de delitos en contra de los datos personales, identidad e intimidad."[215]

Comúnmente los términos de usurpación y robo de identidad son utilizados como sinónimos, lo mismo acontece en las legislaciones locales que fueron citadas, entonces resulta necesario realizar una distinción en cuanto a los términos que se emplean.

---

[214] *Cfr.* ROMERO FLORES, Rodolfo, *El robo o Usurpación de Identidad por Medios Informáticos o telemáticos: su tratamiento jurídico penal*, México, *op. cit.*, p. 306.
[215] *Idem.*

En primer lugar, el robo se puede definir como el delito que se comente: “apoderándose con ánimo de lucro una cosa mueble ajena, empleándose violencia o intimidación sobre las personas, o fuerza en las cosas,”[216] el Código Penal Federal establece que el robo es el delito que: “comete aquél que se apodera de una cosa ajena mueble, sin derecho y sin consentimiento de la persona que puede disponer de ella con arreglo a la ley.”[217]

Por lo tanto, de ambas definiciones se puede inferir que el robo acontece sobre bienes muebles, es decir, que conforme a la investigación realizada la identidad de las personas al ser un derecho humano no puede ser considerado un bien mueble o tangible, por lo cual la identidad es un derecho de las personas y no un bien mueble, por lo que la denominación aun que se emplee en legislaciones locales y generales y federales en materia de datos personales, conforme al significado de la palabra robo no entraría en el tipo penal.

En segundo lugar, la usurpación la define la Real Academia Española como: “delito que comete quien utiliza de forma estable el estado civil, nombre y apellidos de otra persona, suplantando su personalidad”.[218]

Y en el mismo sentido que se relacionó en el apartado que antecede, la usurpación o su sinónimo como suplantación de la identidad implica que una persona suple o se ostenta ante terceros con la identidad de otra persona con fines ilícitos o que la misma otorgue su consentimiento para llevar a cabo la usurpación en su identidad, es decir, que la conducta es otra en la del robo es la apropiación y en la usurpación es la utilización u ostentación de la identidad de una persona a quien no le corresponde.

---

[216] REAL ACADEMIA ESPAÑOLA, disponible en: <https://dle.rae.es/robo > [Consulta: 15-febrero-2022].

[217] *Cfr.* artículo 367 del Código Penal Federal.
Comete el delito de robo: el que se apodera de una cosa ajena mueble, sin derecho y sin consentimiento de la persona que puede disponer de ella con arreglo a la ley.

[218] REAL ACADEMIA ESPAÑOLA, disponible en: <https://dle.rae.es/usurpaci%C3%B3n> [Consulta: 15-febrero-2022].

Sin perjuicio de lo establecido anteriormente, se señala que si bien en las definiciones y análisis legal del delito de usurpación se establecían la usurpación y el robo como sinónimos, en cuanto al tipo penal convendría distinguirlo, porque pueden ser delitos que se tipifiquen de manera aislada, por una parte tener previsto el robo de bases de datos o sistemas informáticos que contengan datos personales de los individuos o elementos que los permitan identificar.

Y por otra parte la utilización de los datos de identidad o elementos que los distingan del resto y que se efectúe con fines lucrativos o para la realización de otros delitos o celebración de actos jurídicos bajo esa identidad, por lo que resulta necesario que en las legislaciones vigentes y aplicables locales se distingan ambos delitos y que en la legislación federal se tipifiquen como delitos aislados, para que las conductas puedan ser sancionadas, y en el mismo sentido la legislación en materia de datos personales tanto en el ámbito federal como en el general establezcan infracciones para el robo de datos personales contenidos en cualquier medio y a su vez la usurpación o suplantación de identidad utilizando datos biométricos.

En este sentido de la tarea legislativa que se requiere Rodolfo Romero Flores establece que:

> Es un hecho que incorporar en la legislación sustantiva penal, una serie de conductas vinculadas a la suplantación de identidad requerirá distinguir en el tipo penal al menos tres elementos básicos, mismos que tendrían interés o incidencia en la calificación jurídica-penal de los mismos hechos. Estos posibles elementos del tipo penal serían: la apropiación de los datos personales por medio convencionales o informáticos (inclusive telemáticos); y un segundo elemento, la transferencia o cesión de los datos personales; y un tercer elemento, su posterior

utilización o facultad arrogada de manera indebida para su utilización sobre dichos datos personales.[219]

De estos tres elementos que propone para un tipo penal más robusto se harán a continuación las relaciones correspondientes a esta investigación:

Primero, de la realización de la conducta que se ha identificado como robo de los medios o sistemas informáticos o en su caso telemáticos que contengan datos personales, entre ellos los datos biométricos, que permitan identificar a una persona, se habla entonces de un apropiamiento de bienes tangibles o no, que contengan datos personales sensibles que permiten la identificación de una persona, tipo penal que específicamente podría encuadrar en el apartado del delito de robo pero con una visión de tutela a la identidad y protección de datos personales.

Segundo, del elemento que estableció Rodolfo Romero se destaca lo investigado en relación con la materia de datos personales, específicamente las disposiciones citadas del tratamiento de los datos personales, contenidos en la legislación federal, general y en su caso, las locales en la materia, lo anterior en función que se habla de transferencia, almacenamiento y uso de los datos, y al igual que se estudió en el apartado de valor de los datos personales, la comercialización y poder económico que tienen las grandes bases de datos que contienen elementos de identidad de las personas.

Tercero, como se contempla en el delito de usurpación o suplantación de identidad, de este tipo podría advertirse un uso ilícito así como una ostentación de una identidad que no le pertenece a una persona, y podría ser una consecuencia de las dos conductas que anteceden, siendo está la conducta que más afecta en el derecho de identidad de las personas, porque involucra la ejecución de actos,

[219] *Cfr.* ROMERO FLORES, Rodolfo, *El robo o Usurpación de Identidad por Medios Informáticos o telemáticos: su tratamiento jurídico penal*, o*p.cit.*, p. 852.

delitos o conductas que importan para el derecho frente a terceros, y principalmente porque pueden ser acciones que crean obligaciones, afectan en su patrimonio, honra, reputación, identidad y que directamente afectan al titular de la identidad.

Por último de las conductas analizadas, en virtud de la justicia penal como última instancia o razón y como un mecanismo sancionador y reparador del daño, se tendrá que precisar la forma de reparación de los daños que se ocasionaran con las conductas descritas, y es óbice que es complicado realizar una cuantificación del valor de los datos personales, pero no así para el valor de la identidad, intimidad, y para la sanción de estas conductas que sin duda alguna deberá atenderse al proyecto de vida de cada individuo y a su vez el grado del daño ocasionado. Relativo a lo anterior el tipo penal exigiría la penalidad más elevada para el último elemento, la usurpación, en función que esta conducta requiere de un robo de datos personales almacenados, un tratamiento de datos indebido o no autorizado y finalmente la utilización o ejecución de actos a nombre de otra persona.

IV.3. PROTECCIÓN Y SEGURIDAD INFORMÁTICA DE LOS DATOS

Hablar protección informática de datos obliga a abordar la disciplina de la ciberseguridad y seguridad informática, en lo relativo a las bases de la ciencia que consisten en el estado de seguridad y confianza que los sistemas de información brindan a los usuarios, la seguridad debe ser entendida desde una visión multidisciplinaria que permite conocer los riesgos y prevenirlos en materia de sistemas informáticos, para la seguridad en general la gestión de los riesgos es importante porque previenen y evitan los riesgos para realizar ciertas acciones y evitar delitos como la usurpación de identidad mediante el uso de sistemas informáticos.

Entrando al tema de la seguridad informática, esta puede definirse como la encargada de la seguridad del medio informático, según varios autores la informática es:

> La ciencia encargada de los procesos, técnicas y métodos que buscan procesar, almacenar y transmitir la información, mientras tanto la seguridad de la información no se preocupa sólo por el medio informático, se preocupan por todo aquello que pueda contener información, en resumen, esto quiere decir que se preocupa por casi todo, lo que conlleva a afirmar que existen varias diferencias, pero lo más relevante es el universo que manejan cada uno de los conceptos en el medio informático.[220]

Para María López Barrientos, la seguridad se: "refiere a todo tipo de precauciones y protecciones que se llevan a cabo para evitar alguna acción que comprometa a la información."[221] Incluyendo en la definición un universo consistente en todas las herramientas, métodos y mecanismos cuyo objetivo sea proteger la información de cualquier peligro o riesgo que pudiera presentarse o vulnere su integridad e información contenida, así mismo la seguridad informática se relaciona con la seguridad de la red, ya que la información requiere un canal de transporte y de dispositivos que trasmiten y captan la información por medio de redes, siendo el principal objetivo de los sistemas informáticos que los datos lleguen con seguridad al destino deseado.

De igual forma para María Jaquelina López Barrientos y Cintia Quezada Reyes se define como:

> La seguridad informática, o de forma más global, la seguridad en los sistemas de información, representa el conjunto de medios y técnicas implementados para asegurar la integridad y que no se difundan involuntariamente los datos que recorren el sistema de información, entendiendo como tal al conjunto de datos y de recursos (físicos, lógicos y humanos) que permiten el almacenamiento y la

[220] ROMERO CASTRO, Irene Martha, *et al.*, *Introducción a la seguridad informática y el análisis de vulnerabilidades*, Manabí, Ecuador, Editorial Área de Innovación y Desarrollo, Primera edición, 2018, p. 14.
[221] LÓPEZ BARRIENTOS, María Jaquelina y Cintia Quezada Reyes, *Fundamentos de seguridad informática*, México, UNAM, Facultad de Ingeniería, 2006, p. 23.

circulación de la información que contiene. También representa la red de actores que intervienen sobre él, que intercambian datos, acceden a ellos y los usan.[222]

De las anteriores definiciones citadas se tiene que destacar el ámbito de aplicación de los riesgos y peligros que sufren los sistemas informáticos específicamente en la vulneración a los derechos sustantivos como la identidad, protección de datos personales, intimidad y la seguridad jurídica en su vertiente protectora de los usuarios de las plataformas para la celebración de actos jurídicos vía remota, principalmente porque el usuario en la medida de lo posible debe preservar los datos personales que incluya es éstas, así como la protección de su identidad, toda vez que como se ha abordado en la investigación es posible mediante el robo de datos y usurpación de identidad hacer el proceso de autenticación, identificación e incluso la celebración de actos jurídicos sin que el sistema jurídico mexicano proteja al usuario.

A manera de ilustrar los principales riesgos a los sistemas informáticos a grandes rasgos se pueden resumir de la siguiente forma:

> Primero, ataque destructivo (denegación de servicio, borrado de sitio, ransomware); segundo, el ataque por la toma de control de los medios; tercero, ataques cuyo objetivo es el robo de bases de datos con fines de lucro o de espionaje y; cuarto, ataque que se denomina APT *o Advanced Persistent Threat*, que es un ataque que requiere una ejecución generalmente a grandes empresas, así como las organizaciones no gubernamentales.[223]

Parte técnica que permite conocer el panorama general que pueden sufrir las bases de datos personales sensibles que sean contenidas por sistemas

---

[222] *Seguridad informática hacking ético: conocer el ataque para una mejor defensa*, Barcelona, España, Ediciones ENI (Epsilon), 4a edición, 2018. Disponible en: <https://search-ebscohost-com.pbidi.unam.mx:2443/login.aspx?direct=true&db=cat02025a&AN=lib.MX001002087437&lang=es&site=eds-live > [Consulta: 19-febrero-2022].
[223] *Cfr., Ibidem.*

informáticos y registros automatizados de identificación o autenticación, lo anterior, sirve de sustento para señalar de forma general los riegos y ataques a que son susceptibles los datos personales, así como para ventilar la mitificación del uso de tecnología siempre presupone una mayor seguridad y certeza en los procesos.

Actualmente y como se hizo referencia a lo largo de la investigación los delitos informáticos van emparejados con el desarrollo de las tecnologías de información, si bien la sociedad de ha visto con visto beneficiada con su uso y avance, también la delincuencia se ha beneficiado de estos, y entre los más preocupantes han sido el acceso a información que ofrecen las redes de comunicación, donde principalmente se les permite cometer delitos desde y hacia cualquier lugar del mundo, llegando a una cantidad de víctimas tan grande como sea la red de comunicación, los delitos informáticos abarcan una variedad extensa de modalidad para su ejecución, modalidades que se citan de los autores Jesús Loredo y Aurelio Ramírez:

- Ataques contra sistemas y datos informáticos.
- Usurpación de la identidad.
- Distribución de imágenes de agresiones sexuales contra menores.
- Estafas a través de internet.
- Intrusión en servicios financieros en línea.
- Difusión de Virus.
- Botnets (redes de equipos infectados contralados por usuarios remotos)
- Phishing (adquisición fraudulenta de información personal confidencial). [224]

Los anteriores en cuanto a materia general de delitos informáticos, existiendo también los delitos relativos al uso de redes sociales y acceso a todo tipo de información, consistentes en:

[224] LOREDO GONZÁLEZ, Jesús Alberto y Aurelio Ramírez Granados, *Delitos Informáticos: su clasificación y una visión general de las medidas de acción para combatirlo*, Nuevo León, Facultad de Ciencias Físico Matemáticas, Universidad Autónoma de Nuevo León, México, 2013, p. 45.

- Acceso a material inadecuado (ilícito, violento, pornográfico, etc)
- Adicción- Procrastinación (distracciones para los usuarios)
- Problemas de socialización.
- Robos de identidad.
- Acoso (pérdida de intimidad).
- Sexting (manejo de contenido erótico)
- Ciberbullying (acoso entre menores por diversos medios: móvil, Internet, videojuegos)
- Cibergrooming (método utilizado por pederastas para contactar con niños adolescentes en redes sociales o salas de chat.

Mediante el uso de tecnologías e internet, el tipo de amenazas y delitos incrementa día a día, por lo que particulares y gobierno se han visto en la necesidad de generar sistemas de protección, antivirus, que a su vez sirve de protección para los datos que contengan en los sistemas informáticos y que son susceptibles de ser vulnerados, sistemas de protección que se pueden clasificar conforme a Jesús Loredo y Aurelio Ramírez de la siguiente forma:

- Adware (muestra contenido publicitario en las actividades del usuario).
- Spyware (recopila datos personales y los envía a un tercero sin consentimiento del usuario).
- Aplicaciones de origen dudoso (programas que pueden poner en riesgo el equipo).
- Software de control backdoor (permiten el acceso remoto al equipo)
- Ficheros con extensión oculta (Malware que se oculta dentro del otro tipo de archivo para evitar ser detectado).
- Programas de marcación telefónica con coste (generan cargos en la factura de manera fraudulenta).
- Suplantación de identidad (phihising).

- Programas que dañan la esfera privada (software que merma la seguridad del sistema).
- Programas broma.
- Juegos (distracción en el entorno laboral).
- Software engañoso (hacen creer el usuario que esta vulnerable y lo persuaden para comprar soluciones).
- Utilidades de compresión poco habituales (archivos generados de manera sospechosa). [225]

Actividades enunciadas que sin lugar a dudas vulneran los derechos fundamentales y que afectan su esfera jurídica más íntima, de igual forma, se relacionan directamente con la utilización de datos biométricos como una forma de identidad y de consentimiento para actos jurídicos, en virtud que, como se analizó en capítulos anteriores a través de los sistemas biométricos contenidos en medios digitales y automatizados es posible realizar el ejercicio de identificación y autenticación de las personas, por lo que, al estar contenidos en medios informáticos, estos son propensos a las actividades delictivas enunciadas y por ende a la comisión de delitos que no solo vulneran la integridad de la base de datos que lo contengan sino que violan derechos humanos.

El riesgo que conlleva la realización de estas actividades en contra de las personas siempre ha sido un punto eje de esta investigación, principalmente por la facilidad actual que se tiene para acceder a la información de las personas desde cualquier parte del mundo y en cualquier momento, por lo que un ambiente donde los riesgos se incrementan a la par de las tecnologías no pueden existir soluciones de seguridad definitivas, resultando que pese a los sistemas de protección las empresas, personas, gobiernos, sin importar su tamaño, inversiones o ubicación siempre permanecerán susceptibles a recibir ataques informáticos.

[225] *Idem*. p. 47.

La seguridad informática o ciberseguridad es un resultado de las circunstancias que se han presentado desde el uso masivo de sistemas informáticos y por supuesto el acceso al internet, como una necesidad frente a los actuales ataques, las amenazas y vulneraciones a las bases de datos y todos los sistemas informáticos, por lo que dada la especialización de un sector en la materia y su aplicación dolosa para cometer ilícitos, así como también, las consecuencias de aplicar unas medidas de protección insuficientes.

Concluyendo que la tecnología y avances en las ciencias de la comunicación e informática, así como procesos de identificación, autenticación o incluso de celebración de actos jurídicos de manera remota, se emplean equivocadamente, provocando el estado de inseguridad e incertidumbre jurídica ante peligros que todo usuario de estos sistemas de información debería conocer antes de utilizar sus datos contenidos en bases de datos para identificarse y celebrar actos jurídicos.

Finalmente, en lo particular se tiene que los datos biométricos contenidos en bases de datos en soportes digitales no están exentos de las vulnerabilidades, amenazas y riesgos que se han precisado en el texto de la investigación, no son sistemas infalibles, que si bien los sistemas de protección en materia de seguridad informáticas han avanzado y evolucionado, no son suficientes para brindar una total y completa certeza en los sistemas informáticos, que contrario a la apreciación que se pretende dar al usuario, los datos no son asegurados en su totalidad del robo, usurpación o delitos cibernéticos mencionados.

Lo anterior aunado a la falta de regulación en el sistema jurídico de México, se deja en un estado de incertidumbre y de constante vulneración o en su caso violación a los derechos humanos de los mismos, especialmente en lo relativo al derecho a la identidad, intimidad y protección de datos personales.

IV.4. PANORAMA PROGRESIVO DE LOS SISTEMAS BIOMÉTRICOS COMO FORMA DE IDENTIFICARSE Y DE OTORGAR CONSENTIMIENTO EN ACTOS JURÍDICOS

Como se ha abordado a lo largo del trabajo de investigación, es inevitable que la tecnología sirva para apoyar y resolver los problemas de la población y que principalmente facilite y haga más rápidos los procesos mediante la automatización o uso de los mecanismos informáticos y telemáticos, y el uso de los sistemas biométricos como una forma de identidad y de otorgar consentimiento para la celebración de actos jurídicos.

La sociedad exige que las actividades y tareas se hagan de una forma más rápida y que brinden seguridad en lo que realicen, esto cobra importancia porque como se estudió en este capítulo los sistemas de seguridad informática, así como sus vulnerabilidades conocidas que forman parte del argumento toral de su uso y necesidad de regulación en sentido de protección del usuario y titular de los datos personales sensibles.

En consecuencia para abundar más en lo relativo a la seguridad, uso y premisas que deben regir en el uso de datos biométricos, debe verse a la luz de enfoque en favor del usuario y del titular de los datos, esto es en concordancia con la metodología legislativa empleada y que de la misma se desprende la falta de normatividad expresa que beneficie y proteja al usuario final, en virtud que no se debe oponer la normatividad imperativa al avance tecnológico y sus beneficios para la sociedad, principalmente porque la solución de los problemas jurídicos y la agilización de procesos debe estar emparejada con la tecnología y de las que día con día serán motivo de un avance progresivo.

Bajo la misma premisa y ante la constante demostración que se ha expuesto respecto del uso de dispositivos tecnológicos, es dable afirmar que el espíritu del legislador debe atender a la exigencia de protección en favor de los derechos

humanos del titular de los datos y usuarios de los datos biométricos como forma de consentimiento.

Precisado lo anterior, se deja en claro que si bien se expusieron los motivos negativos y aspectos por los cuales no deberían emplearse los datos biométricos para procesos de autenticación, identidad y en su caso consentimiento, por los peligros, vulnerabilidades y demás razones expuestas, ello no es motivo de negar su utilización y cerrar la apertura armónica entre la tecnología y su implementación en el campo del derecho, por el contrario, en un panorama progresivo de derechos humanos y el uso desmedido y acelerado de tecnologías de la información exige que se regule en favor de las personas y que se brinden las herramientas al operador jurídico para su aplicabilidad en el plano fáctico.

IV.4.1. LAS BASES DE DATOS SENSIBLES Y SU INTEGRACIÓN DE SISTEMAS BIOMÉTRICOS

Como fue abordado en el primer y segundo capítulo los datos biométricos de las personas pueden ser clasificados como datos personales sensibles, esto en su vertiente de forma de identidad y como parte del derecho a la información y protección de datos personales, siendo entonces unos de los grandes problemas a resolver el tratamiento de estos datos biométricos, principalmente por las grandes bases de datos que los contienen y como se estudió a pesar que haya regulación al respecto de datos sensibles y del tratamiento, muchas de esas hipótesis regulatorias se evaden o son inobservadas por los responsables del tratamiento, de ahí que sea necesaria se especifique y sobre todo se remita la responsabilidad en todo momento del responsable de los datos y que no se deje a la deriva al usuario por un aducido tema de seguridad informática o procesos técnicos informáticos.

Sirve de sustento a lo anterior, lo alcanzado por Magdalena Sepúlveda quien expone que:

> La integración de sistemas de información, y la posibilidad de vincular esos registros a través de un identificador común (biométrico), es particularmente problemática en países sin marcos legales o institucionales de protección de datos personales. En aquellos países donde a pesar de la existencia de una ley y una agencia, su implementación es débil. Desgraciadamente, esta es la situación de la mayoría de los países donde los programas de asistencia social se han expandido en años recientes.[226]

No siendo aplicable en México una falta de regulación en materia de datos personales, pero sí una falta de cubrir los vacíos legales en la norma existente en torno al uso de los datos biométricos.

Pese a que se han utilizado los datos biométricos en los últimos años a mayor medida, actualmente el proceso legislativo del tópico es escaso, también es poco común el debate jurídico sobre los riesgos que el uso de esta tecnología implica para el derecho de identidad, la privacidad y la protección de datos de los usuarios y titulares, los mencionados vacíos legales son un tema que no debe pasar desapercibido para la protección, promoción, respeto y garantía de los derechos humanos en función de los datos personales, porque en la actualidad y ante el uso de diversas plataformas digitales aumenta el número de las bases de datos procesan volúmenes masivos de datos personales, incluida datos personales sensibles como son los datos biométricos, y que como se incluyó en la investigación estas bases son susceptibles de ataques y riesgos latentes, que sin lugar a dudas no sólo afectan a las bases y sistemas sino que también directamente los más afectados son los titulares de los datos personales.

---

[226] SEPÚLVEDA, Magdalena, *Tecnología biométrica en programas sociales, ¿una preocupación legítima?*, México, México Social, 30 de mayo del 2019, disponible en: <https://www.mexicosocial.org/magdalena-sepulveda-tecnologia-biometrica-programas-sociales/> [Consulta: 01-marzo-2022].

De lo anterior deviene la necesidad de no sólo considerar como un punto toral deficiente la seguridad técnica informática que pudieran tener las bases de datos, sino que debe ser ponderado en todo momento el aspecto de la responsabilidad y asunción de los daños y perjuicios que pudieran ser ocasionados por las deficiencias de seguridad de las bases de datos que contengan la información biométrica de sus titulares, y que van en contra del derecho humano de protección de datos personales y los derechos acceso, rectificación, cancelación y oposición, tutelados por el párrafo segundo del artículo 16 de la Constitución Política de los Estados Unidos Mexicanos.

IV.4.2.CIBERSEGURIDAD PARA ACTOS JURÍDICOS CELEBRADOS POR MEDIOS ELECTRÓNICOS

El segundo aspecto por mejorar en la protección de los datos humanos de los usuarios que utilicen los datos biométricos como una forma de otorgar el consentimiento es un marco regulatorio más robusto en materia de delitos informáticos, esto es, se requiere que la hipótesis normativa pueda ser encuadrada en la realidad que acontece ante los delitos de usurpación y robo de identidad, así como el robo de bases de datos que contengan información sensible de las personas, mismo que puede llegarse a positivar en forma de una agravante tratándose de datos biométricos.

De igual forma, de manera que se promueva, garantice, respete y protejan los derechos sustantivos en materia de identidad y protección de datos personales, se convertirá en un reto que el operador de la norma, es decir que los órganos jurisdiccionales cuenten con una mayor instrucción para las pruebas relacionadas que pudieran verterse como desfile probatorio en un juicio y que la norma imperativa adjetiva establezca las bases para admitir las pruebas obtenidas por medios electrónicos, así como para en caso en materia penal establecer una cadena de custodia para los mensajes de datos a modo que puedan servir como medio probatorio para encuadrar una conducta atípica realizada por medios digitales y que

afecten la intimidad, datos personales, identidad y en la celebración de actos jurídicos las seguridad de las personas.

Para los objetivos protectores anteriores no basta con un servicio de seguridad o sistemas técnicos que se implementen, porque los avances tecnológicos que se pudieran aplicar para el bienestar de las personas, también son aplicables en perjuicio de estas, dejando de lado la profesionalización de los criminales, los delitos informáticos a comparación de cualquier otro delito pueden cometerse desde cualquier lugar, momento y modo, teniendo las herramientas mínimas para su consumación.

Recapitulando y a manera de resaltar que los servicios de seguridad informática o ciberseguridad tienen como principal objetivo el mejorar la seguridad dentro de un sistema de información, estos servicios principalmente buscan proteger contra ataques de seguridad y de cierta forma dotar de mecanismos e instrumentos de seguridad a los sistemas informáticos, mismos que para efectos de esta investigación se citan y se clasifican de la siguiente forma:

"1) Confidencialidad: Se le considera confidencial a aquello que mantiene en secreto cualquier tipo de información, la confidencialidad protege información secreta de cualquier persona que no esté autorizada para manipularla."[227]

Primer rubro que es suma importancia, dada la relevancia que se analizó principalmente en lo relativo a los datos biométricos como datos personales sensibles, toda vez que la información personal que sea trata sin autorización, o que sea robada o extraída ilícitamente trae como consecuencia una falta de fiabilidad en la seguridad y certeza de una base de datos, por lo que resulta conveniente tener una regulación robusta en el control de la seguridad informática de las bases de

[227] *Seguridad informática,* México, UNAM, página 57, disponible en: <http://www.ptolomeo.unam.mx:8080/xmlui/bitstream/handle/132.248.52.100/250/A5.pdf?sequence=5&isAllowed=y> [Consulta: 22-febrero-2022].

datos que contengan datos biométricos, mediante la regulación de una autoridad encargada y facultada para determinar el grado de seguridad y en su caso autorizar la utilización de bases de datos, que permitirían asegurar la fiabilidad que no pueda ser tratada la información no autorizada u obtenida ilícitamente.

"2) Autenticación: Se trata de la forma en que uno verifica la identidad de un proceso o una persona."[228]

Servicio de seguridad que involucra la mayoría de los puntos torales de investigación: la identidad y la celebración de actos jurídicos, servicio de seguridad que permitiría al usuario confirmar que se trata de una comunicación o intercambio de datos directamente con una persona con quien desea celebrar el actos, es decir, mediante un proceso que permite hacer distinguible a una persona del resto de personas.

Con la limitante que se precisó anteriormente relativa a la capacidad de la base de datos, proceso que depende totalmente del sistema informático que procese la información, primero que el dato biométrico procesado identificar al usuario, es decir, realizar una comparación automatizada de los demás datos almacenados; segundo, que permita verificar la identidad a través de las características únicas de cada dato como se abordó en el primer capítulo capturadas y procesadas por aparatos electrónicos, proceso en el que intervienen diversos factores y de los cuales no hay regulación para su fiabilidad, así como tampoco una forma de comprobar su inviolabilidad.

"3) Integridad: La integridad se encarga de proporcionar controles que aseguren que el contenido de dicha información no ha sido modificado y que se mantenga intacta al ser transmitida a otro lugar."[229]

[228] *Idem.* p. 58.
[229] *Idem.* p. 59.

Clasificación de la seguridad informática que presupone la fiabilidad e inmutabilidad de un sistema de datos, es decir, que este tipo de seguridad establece cundo una base ha sido manipulada o alterada, a través de sellos o marcas que permiten que un mensaje de datos se reputen como inviolados, que en la regulación mexicana como se analizó en el apartado de firmas electrónicas existe y se aplica, pero en relación con los datos biométricos que en ocasiones se utilizan indebidamente como firmas electrónicas.

Además, el proceso de verificación de la integridad de los sistemas de información es complicado y presupone la vulnerabilidad de los mismos, en función que cualquier persona que tenga acceso al mensaje de datos, aún y con sistemas de encriptación sería posible cambiar los datos si logra acceder al sistema, como se prevén en cuanto a la comisión de delitos informáticos.

"4) No repudio: Este servicio se encarga de que no se niegue que un mensaje ha sido transmitido."[230]

Apartado de la seguridad informática es aplicable a la teoría del derecho civil para el consentimiento, expedición y aceptación de la propuesta que podría contenerse en un mensaje de datos firmado o autenticado mediante datos biométricos, comprobación de seguridad que permitiría en caso de una contienda judicial que se compruebe la voluntad para emitir la oferta o aceptación, esto es, que fehacientemente se pruebe que el emisor haya mandado un mensaje y que no se hayan alterado, para que se acredite que se han enviado los datos, aspectos que involucran aspectos técnicos de la informática pero que no son abordados ni estudiados por el derecho, y que dentro de la normatividad mexicana no se ven avances para su regulación y en su caso incorporación como medio probatorio en un juicio.

[230] *Ibidem.*

"5) Control de acceso: Se encarga de limitar el acceso a la organización o al sistema de información de personas que no estén autorizadas."[231]

Servicio de seguridad que permite conocer quien o quienes ingresan a cierta información contenida en las bases de datos, proceso que no es novedoso, toda vez que este se equiparaba a utilizar un número de identificación personal, tarjetas con bandas magnéticas, contraseñas, y que dependía del grado o nivel de acceso que un sistema le otorgaba a esta persona para acceder a los datos almacenados o inclusive modificarlos.

Entonces si una persona tiene un acceso a modificar datos biométricos y que estos se utilicen para identificar a una persona se da lugar a cambiar unilateralmente los datos de identidad, tal y como sucede cuando se corrigen datos en un acta de nacimiento o una credencial de identidad, por lo que al no existir regulación respecto del nivel de seguridad de acceso, así como facultades para manipular los datos, el usuario y titular estaría en una trasgresión directa a sus derechos sustantivos de identidad e intimidad.

"6) Disponibilidad: Como su nombre lo indica este tipo de servicio permite que las personas autorizadas tengan acceso a la información deseada independientemente del día y la hora."[232]

Finalmente la disponibilidad como un servicio de seguridad informática que permite a ciertas personas acceder a la información contenida demuestra la incertidumbre jurídica en la que se pude colocar a un individuo cuando las bases contienen sus datos sensibles y que lo hacen distinguibles del resto, porque si existe una base de datos donde puede accederse, ya sea con o sin autorización, pero que al final de camino permiten que alguien acceda y conozca los datos más íntimos de una persona, y que ante un mal uso y con un grado de especialización técnico podría

[231] *Idem.*, p. 60.
[232] *Ibidem.*

utilizarse para cometer ilícitos, como la usurpación y robo de identidad, y sin que dentro de todas las regulaciones locales se tipifiquen estos delitos, deviene que no haya una fehaciente protección a los derechos de identidad.

Por último, los servicios de seguridad informática si influyen en la violación a derechos sustantivos si se toma en consideración que la legislación en México aún no ha previsto estas hipótesis para la implementación de los datos biométricos tanto en procesos de identidad, autenticación y como para ser utilizados en suplencia de una firma electrónica, en virtud que los aspectos técnicos no se han considerado y tampoco regulados en la legislación y que hoy juegan un papel fundamental en la vida diaria de los usuarios, por lo que se necesita una labor legislativa que consolide un sistema de protección a la identidad de las personas mediante el uso de datos biométricos.

IV.4.3. LA VALIDACIÓN DE LOS SISTEMAS BIOMÉTRICOS

Dentro de la línea de investigación de este trabajo se analizaron como se han utilizado los datos que en su conjunto sistemas biométricos que permiten identificar a las personas y que también lo hacen con respecto al otorgamiento de su consentimiento para la celebración de los actos jurídicos, por lo que ahora importa resaltar que aspectos considerativos deben tomarse en cuenta para una posible futura regulación.

Basados en la fenomenología es un hecho notorio que el uso de las tecnologías de la información incrementan la productividad, rapidez y agilización de diversos procesos, y la implementación del uso de los datos biométricos no es la excepción, pues como se ha abordado la sociedad, aunque con el sesgo de la posibilidad acceder a los medios tecnológicos, implícitamente ha aceptado su uso mediante un uso cotidiano y reiterado han aceptado que se utilicen los datos biométricos como una forma de autenticarse e identificarse ya sea ante autoridades o entre particulares, y todo ello se deriva de un acceso a la vida más fácil y rápida, limitado

las actividades que necesariamente requerían la presencia de la persona interesada en el lugar para celebrar el acto jurídico o en su caso identificarse.

La población que tiene acceso a estos medios tecnológicos de identificación y de celebración de actos jurídicos celebrados en medios ópticos y de cualquier otra tecnología, además de hacer el procedimiento más rápido, lo realizan desde cualquier lugar y momento, y que actualmente podríamos decir que sirven como barreras o pasos de seguridad adicionales para identificarse, se habla de un sistema de autenticación de dos o tres pasos que contengan el datos biométricos de una persona como elementos de seguridad que no sólo son aplicables en sucursales de las instituciones de crédito, si no que están a la mano de cierto sector de la población.

En la misma línea argumentativa el uso de los datos biométricos, ya sea como una sola capa de protección o como un segundo o tercer paso en un proceso de autenticación brinda un sentimiento de confianza y seguridad en el usuario, porque se sabe es más confiable tener que realizar ciertos pasos y procedimientos para acceder a una plataforma o aplicación en comparación a que sólo se tuviera el acceso mediante una contraseña.

Por lo que se afirma que existe un sistema de confianza que se ha creado en torno a los procesos de autenticación de dos o más pasos y que incluyen la biometría de las personas, y esto se suma a que como se analizó en el primer capítulo relativo al marco teórico y conceptual, que los datos biométricos por las características inherentes a los mismos, son únicos en cada individuo, y de ahí que las personas acepten y prefieran procesos de autenticación que empleen datos biométricos a exclusivamente utilizar contraseñas.

Precisado lo anterior, se reitera que la tecnología que emplea los datos biométricos para el momento de identificarse es beneficiosa para los usuarios en materia de seguridad y confianza, en el tenor que les permite a los usuarios acceder

a nuevos métodos para identificarse de manera inmediata, y que en todo caso antes no se empleaba, como sucedía en el robo y clonación de tarjetas de débito o crédito, caso en los cuales únicamente se le solicitaba al portador de una tarjeta que proporcionara número de identificación personal para acceder a la cuenta, y realizar diversos actos, y actualmente con la implementación de los datos biométricos, estos brindan una mayor confianza al ser pasos de autenticación adicionales y que hoy ya son necesarios para la protección de los usuarios.

Ahora bien, en el panorama creado que no se hubieran implementado estos mecanismos de tecnología de identificación biométrica, se podrían estar utilizando únicamente las contraseñas e implementar contraseñas dinámicas, o incluso la implementación de dos o tres pasos con estos, pero el punto toral del uso de los datos biométricos ha sido la creencia de seguridad y protección, porque al ser datos únicos de cada persona se estima que los mismos dan una fiabilidad indiscutible, aunque en la realidad y de acuerdo con la investigación los datos son susceptibles de ser violentados.

Es por ello, que ante la creencia y desconocimiento de la seguridad cibernética su uso ha incrementado y con ello la necesidad de que exista una regulación al respecto que más que beneficiar y propiciar su uso, permitan al usuario acceder a un medio de defensa para la tutela de sus derechos humanos.

Antes de concluir este apartado, es necesario que se tome en consideración que el avance ha beneficiado los procesos de autenticación e identidad, y caso contrario se sostiene que los datos biométricos como forma de otorgar el consentimiento para la celebración de actos jurídicos se implementan como sustitutivos de la firma autógrafa, incluso llegando a dar el alcance de una firma electrónica avanza, y de este rubro los datos biométricos más que ayudar a la agilización de procesos hacen que el usuario quede sin medios de defensa frente a posibles delitos en materia de ciberseguridad o en su caso propios errores del usuario.

Finalmente, los avances que se han implementado como pasos de seguridad adicionales basados en la biometría de las personas además de ser un mecanismo de confianza consolidan un sistema de autenticación de varios pasos que añade seguridad en la identificación de las personas, así como para el ingreso de los diversos tipos de cuentas de usuario, ya sea de trabajo, personales o de entretenimiento.

Como se analizó si bien ningún sistema informático es inviolable, estos mecanismos brindan seguridad y confianza adicional a los usuarios por las propias características de los datos biométricos, avances que sin lugar a dudas benefician a la población que tiene alcance a estos dispositivos, y que en el rubro del consentimiento para actos jurídicos no es así, pues se buscan evadir las disposiciones relativas a firmas electrónicas, resultando de lo anterior en la necesidad de un marco regulatorio más exigente y protector a los usuarios.

IV.4.3.1. SERVICIOS DE CERTIFICACIÓN DE FIRMAS ELECTRÓNICAS Y DE SISTEMAS BIOMÉTRICOS PARA LA CELEBRACIÓN DE ACTOS JURÍDICOS

Como fue motivo de disenso anteriormente y en relación a las firmas electrónicas, en este apartado se abordará finalmente la disyuntiva de los datos biométricos como forma de otorgar el consentimiento, en el sentido que como se precisó a lo largo de la investigación los datos biométricos no sólo han sido utilizados para procesos de autenticación sino que artificiosamente se han empleado como forma de propalación de actos jurídicos, porque si bien ya existe dentro del sistema regulatorio mexicano la adecuación para la firma electrónica y la firma electrónica avanzada, con la implementación en diversas plataformas de comercio electrónico se han pretendido utilizar a los datos biométricos obtenidos y procesados por mecanismos automatizados como forma de otorgamiento del consentimiento, y equiparado al tácito.

Se sostiene conforme a los resultados expuestos a lo largo de la investigación, específicamente en lo relativo al acto jurídico y del consentimiento, que no es

correcto que se empleen como equiparado o incluso homónimo a una firma electrónica, avanzada o no, a los datos biométricos, así como tampoco es correcto que se pretenda incorporar como un tipo de consentimiento tácito a la utilización de los datos biométricos, porque utilizarlos de estas formas implican un riesgo constante por su mal uso o deficiencia dentro de los sistemas de seguridad informáticos, además que la legislación contiene vacíos que podrían presuponer su indebida utilización, aunado a que no existen criterios judiciales que interpreten la norma y que la legislación que podría utilizarse por analogía es insuficiente y que además remite la responsabilidad al usuario.

Bajo el mismo argumento, es importante resaltar en la importancia del cuidado de la firma electrónica avanzada toda vez que la misma presupone el mismo rigor que una firma autógrafa, como se estudió el uso de la firma autógrafa por sí misma establece riesgos y falsificaciones, y se necesita de expertos en materia de grafoscopía que nos permitieran determinar si una firma es de la persona que dice ser, y esto se obtiene a través de peritajes que se basan en firmas indubitables, y para el caso de las firmas electrónicas no es el mismo presupuesto, pues desde el experto a valorar la prueba debe ser experto en informática y la pericial ahora se basará en la inalterabilidad de la firma, en forma de cadena de datos, por lo tanto, se puede afirmar que ambas firmas tienen sus peritajes que permitirían dilucidar respecto del valor de una firma, y esta situación no podría acontecer para el caso de los datos biométricos.

En continuidad con el párrafo que antecede, los datos biométricos si bien podrían cambiar como se analizó en el primer capítulo por cuestiones externas y del tiempo, también sucede con la firma autógrafa, pues con el paso de tiempo puede perder caracteres físicos, y esta situación no se convalida con el uso de firmas electrónicas, puesto que el mensaje de datos y su inviolabilidad no se alteran con el tiempo, si no que dependen de su vigencia, resultando entonces que del estudio comparativo que los datos biométricos comparten características con la firma autógrafa pero no con la firma electrónica, y en el plano fáctico el uso de datos biométricos como forma de

otorgar el consentimiento se ha erróneamente comparado con una firma electrónica, resultando entonces que en una controversia no puedan acreditarse o sustentarse los elementos sobre los cuales debería versar una pericial de estas índoles.

En virtud de lo anterior, y como se advierte del contenido de la presente investigación, la firma electrónica ha servido de mucho para la evolución y la compatibilidad del derecho con la tecnología, así como para el acelerado proceso de automatización de procedimientos y de celebración de actos de jurídicos electrónicos, al igual que la comodidad y practicidad que estos conllevan para los usuarios, pero el punto de debate se encuentra en la seguridad y certeza que se podría tener con el uso de datos biométricos de la misma forma en que se hace con una firma electrónica avanzada.

Ante la vulnerabilidad y la responsabilidad del titular de sus propios datos sensibles de conservarlos pareciera una dicotomía entre su uso y su prohibición, pero en realidad el problema se deriva desde el aspecto legislativo.

Destaca como un panorama de espíritu regulatorio las regulaciones de la firma electrónica, y que esto no debe confundirse el proceso de autenticación o identidad que se lleva con los datos biométricos con el rigor jurídico de una firma electrónica, porque son de naturaleza distinta y con sus características técnicas informáticas diferentes, mientras que en una el principal objetivo debería ser autenticar la identidad de un individuo y hacerla distinguible del resto mediante un rasgo físico o conductual medible único.

Por el otro lado sólo se busca la certeza en los actos mediante elementos que por sus características se pueden analizar como inviolables, luego entonces el punto medio de estos dos aspectos darían el origen a la regulación de los datos biométricos en sus dos vertientes, como una forma de identidad y de otorgar el consentimiento en actos jurídicos, a través del uso de tecnologías que propiciaran la certeza y seguridad.

IV.5. LA IMPORTANCIA DE LA INFORMACIÓN BIOMÉTRICA Y SU CUIDADO

A lo largo de la investigación se han destacado los principales puntos por los cuales la información biométrica es importante, y porque es relevante su regulación para ser utilizada como una forma de identidad y de consentimiento para actos jurídicos.

No queda atrás la problemática de las grandes bases de datos que ya contienen datos biométricos, mismos que ya se utilizan en los procesos de autenticación, identidad y firma, actualmente es el común denominador que no se les dé la importancia y cuidado que merecen, teniendo su origen de un posible desconocimiento del alcance y valor jurídico que tienen, así como no tener en claro la cantidad de circunstancias que pueden derivar de su mal uso, o incluso de los hechos constitutivos de delitos que se vislumbraron.

Al respecto del cuidado e importancia de la biometría de las personas, existen varios manuales que marcan un panorama técnico pero no jurídico, a lo anterior nos sirve citar a Marianne Diaz quien refiere que:

> 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.[233]

[233] DIAZ HERNÁNDEZ, Marianne, *El cuerpo como dato,* Venezuela, Editorial Derechos Digitales, 2018, p. 22, disponible en: <https://www.derechosdigitales.org/wp-content/uploads/cuerpo_DATO.pdf> [Consulta: 03-marzo-2022].

De igual forma conforme a la cita anterior, destaca para el reconocimiento de la importancia de los datos biométricos las palabras una persona moral argentina, la Asociación por los Derechos Civiles, quienes afirman que:

> Los datos biométricos brindan información sobre lo más íntimo de un ser humano: su cuerpo. A su vez, el carácter permanente de ellos impide que en caso de ser divulgados de manera ilegítima, el daño pueda ser reparado. A diferencia de una contraseña, no podemos volver a configurar nuestro iris o nuestra huella digital. Por eso, no hay nada más personal que un dato biométrico.[234]

Continuando con la cita de autores que aportan al tema de la importancia de los datos biométricos tenemos que para Laura Adriana Sánchez Cortés: “debemos considerar que se enseñe a temprana edad en que consisten los datos personales. Una vez que esto se aprenda desde pequeños, al crecer podrán identificar las formas de cuidarlos, y el cómo hacer valer sus derechos cuando detecten que están haciendo mal uso sus datos personales.”[235]

Citas efectuadas de las cuales se desprende que existen diversidad de autores que comparten la idea de la importancia del cuidado de la biométrica de su titular, y esto se remonta desde el origen de la naturaleza del dato biométrico, pues es un dato que forma parte de las características únicas de cada persona, es decir, son cuestiones inherentes a cada ser humano, toda vez que un tratamiento no autorizado tiene un origen más profundo que repercute en la intimidad y cuerpo de las personas, y como se analizó los delitos que pudieran cometerse como la

---

[234] ASOCIACIÓN POR LOS DERECHOS CIVILES, *Desafíos de la biometría para la protección de datos personales: Reflexiones sobre el caso SIBIOS,* Argentina, 2017, p. 12, disponible en: <https://adc.org.ar/> [Consulta: 05-marzo-2022].

[235] SÁNCHEZ CORTÉS, Laura Adriana, *Manual para el uso de datos biométricos en los servicios financieros,* México, INFOTEC CENTRO DE INVESTIGACIÓN E INNOVACIÓN EN TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN, 2019, p. 74, disponible en: <https://infotec.repositorioinstitucional.mx/jspui/bitstream/1027/329/1/INFOTEC_MDTIC_LASC_10102019.pdf> [Consulta: 16-marzo-2022].

usurpación y robo de identidad son graves actualmente en un mundo con perfiles e identidades digitales.

A lo anterior se suma el argumento que ante el desconocimiento de la población sobre la importancia de los datos biométricos, que existe un notorio descuido en su implementación así como su autorización para ser utilizado como una forma de identidad, autenticación y de otorgamiento del consentimiento.

Las plataformas y aplicaciones digitales obtienen el consentimiento para su uso a través de avisos de privacidad ilegibles o que en su caso son extensos y que a nadie le gusta leer y sobre todo que a nadie le gusta perder la comodidad y facilidad que tienen derivado de su uso, entonces la autoridad del Estado debiera justificar la creación de normas imperativas que permitan proteger a los usuarios y titulares de los datos frente a estas arbitrariedades.

Es por lo anterior, que la propuesta legislativa se encamina a la creación de hipótesis normativas que si bien permitan el uso de los datos biométricos para procesos de autenticación y de identidad, que también deban proteger y tutelar los derechos sustantivos, como el caso de implementar responsabilidad y reparaciones de daño elevados para todos aquellos que implementen en su tratamiento datos biométricos y no se autorice para este fin.

De igual forma que debe servir como media de prevención que las penas en caso de delitos de robo de identidad y se usurpación de identidad de incrementen considerablemente para el caso que involucren datos biométricos de las personas.

Una adición al Código Penal Federal serviría como medida persuasiva para prevenir el delito de usurpación y robo de identidad con el uso de datos biométricos, incrementado las penas y en su caso también considerablemente el monto de la reparación del daños, siendo el motivo de éste la violación no sólo a la identidad de las personas, la esfera más íntima de cada individuo y de su cuerpo, derivando

también de una conducta típica más amplia que en su caso permita al operador jurisdiccional que pueda aplicar la penalidad establecida en la inteligencia que el presupuesto normativo involucre la utilización de medios ópticos, digitales, como algunas legislaciones locales citadas en cuanto a la valoración del grado de experticia y ventaja del sujeto activo.

Aunado a todo lo anterior, respecto de la legislación en materia de protección de datos, identidad e intimidad, la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados y la Ley Federal de Protección de Datos Personales en Posesión de Particulares, deben tener un apartado específico sobre el tratamiento de los datos biométricos, que podría decirse sería similar a lo ya existencia de los datos sensibles.

Lo necesario es la cobertura y protección de los derechos sustantivos requieren de medidas amplias y que permitan al gobernado acceder a todos los procedimientos y mecanismos de defensas más favorables para su tutela, y ejemplo de esto sería poder establecer una naturaleza símil a la suplencia de la queja, en materia de juicio de amparo, y como excepción al principio de estricto derecho, en los procedimientos que se lleven ante el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales encontrando sustento que la notoria desventaja y estado de desigualdad que se encuentra un titular con un particular frente a quien maneja sus datos personales, porque al final de cada historia los usuarios y titulares se ven obligados a utilizar los servicios que exigen utilizar sus datos biométricos.

El espíritu legislativo para la regulación de los datos biométricos como una forma de otorgar el consentimiento para actos jurídicos puede yacerse en la legislación vigente y aplicable de la firma electrónica avanzada, dado que su implementación en el sistema jurídico mexicano se ha visto a lo largo de los años, puede servirle al constituyente permanente como base para una posible regulación en materia de datos biométricos, en el entendido que no se pueden seguir usando como

equiparación al consentimiento expreso o como equivalente a una firma electrónica, pues su naturaleza tanto técnica como jurídica son distintas, y no se puede pasar por alto la función del Estado en regular las operaciones entre particulares y brindar la certeza y seguridad que requieren para encontrarse en un Estado de Derecho.

V. CONCLUSIONES

Finalmente de la investigación realizada se arriba a las conclusiones que serán enunciadas a continuación, y en virtud de la realización de una propuesta para la solución de las problemáticas planteadas en torno al uso de los datos biométricos como forma de identificación y de otorgamiento de consentimiento para la celebración de actos jurídicos se realizará encaminada a un paquete de reformas a las diversas legislaciones analizadas en el cuerpo de la investigación, por lo que se verterán las afirmaciones y necesidades con las que se concluye este trabajo, así como de forma enunciativa el sustento de las mismas y la posible solución a las problemáticas jurídicas que fueron expuestas.

En un primer término se concluye que los datos biométricos son datos personales sensibles que se distinguen del resto por ser características únicas medibles de cada individuo, y que en comparación de cualquier otro dato personal estos no pueden ser fácilmente modificados, ello porque son datos inherentes a la naturaleza física de cada individuo, es decir, que los datos biométricos forman parte de la esfera más íntima de cada persona en el entendido que forman parte del cuerpo humano y sus conductas únicas, y un cambio en ellos presupondría un cambio en el físico de las persona, de ahí que su importancia y particular naturaleza permeen en su uso como una forma de hacer distinta a una persona del resto.

Bajo las premisas generales alcanzadas se advierte que los datos biométricos, se dividen en aspectos biológicos y conductuales, de los cuales y para efecto del trabajo de investigación en el primer capítulo se describieron en su mayoría los aspectos biológicos, porque son los que más se utilizan y que mayor confiabilidad tienen, como: el iris, huella dactilar, geometría de la mano, reconocimiento facial, reconocimiento de voz, que son aspectos que cuando son medibles permiten diferenciar a una persona de las demás; y los aspectos conductuales, la forma de caminar, velocidad y estilo de escritura, registro de actividades cotidianas, que son caracteres que se despliegan cada día y que forman parte de nuestra rutina diaria,

que si bien pueden ser medibles, en la actualidad su implementación y utilización en comparación con los biológicos son en menor medida utilizados, concluyéndose de este rubro que los datos biométricos biológicos son los que en mayor medida son utilizados para procesos de identificación, autenticación y celebración de actos jurídicos.

Coincidiendo con el párrafo anterior, que actualmente mediante el uso de tecnologías informáticas se han podido hacer medibles a mayor medida y con mayor fiabilidad los datos biométricos de los individuos, así como realizar el proceso de comparación de los datos biométricos almacenados en una base de datos o servidor, por lo tanto, su uso e implementación para hacer distinguible a una persona de las demás se ha visto en aumento en los últimos años, en suma que los dispositivos móviles que son utilizados ya implementan este tipos de lectores y tecnología que permiten que los datos biométricos de su titular puedan ser captados y procesados automáticamente para saber si una persona es quien dice ser.

Una de las principales ventajas de los datos biométricos como datos físicos únicos es su presumible inalterabilidad y grado de fiabilidad en los procesos comparativos de identificación y autenticación, ventaja que se ve disminuida conforme a la capacidad de procesamiento del *software* y de la cantidad de datos que tenga almacenados la base de datos o servidor, porque estos aspectos técnicos limitan el proceso de autenticación y ponen en duda la fiabilidad de los mismos, de igual forma la ventaja se ve limitada por factores externos y subjetivos, como son el sudor, la limpieza del lector que captura el dato biométrico, la humedad en el ambiente, amputaciones, lesiones, raspones o protuberancias de la parte del cuerpo humano a procesar, factores que no son parte del común denominador pero que permiten dejar abierta la puerta para dudar de la fiabilidad o universalidad del uso de los datos biométricos.

La evolución tecnológica y el mayor acceso a la tecnología por sectores ha permitido el uso de dispositivos móviles y fijos que realizan la tarea de capturar,

almacenar, procesar y autenticar a la persona mediante el uso de su biometría, misma suerte que no corren en los sectores marginados o que simplemente no tienen acceso o su posibilidad de implementar medios ópticos o digitales que permitan identificar a una persona de manera automatizada, circunstancia que desde luego robustece que argumento de la falta de universalidad y posibilidad de acceso de la tecnología en los diversos campos de aplicación.

Aunado a lo anterior, se abordó lo relativo a la fiabilidad y seguridad de las bases de datos que contienen los datos biométricos de las personas, en la tesitura que al igual que cualquier otra base de datos o servidores estas están propensas a sufrir ataques y vulneraciones, los cuales conforme la tecnología mejoran pero también los ataques, riesgos y amenazas incrementan, por lo tanto de origen quedaron vislumbrados los aspectos que imposibilitan que las personas en su totalidad y con fiabilidad completa pudieran ser identificadas mediante el uso de los dispositivos tecnológicos utilizando los datos biométricos del individuo.

Sin perjuicio de lo anterior, los procesos automatizados de identidad y de autenticación mediante el uso de datos biométricos no deben ser confundidos ni ser aplicables en un mismo momento, porque como se abordó en la investigación, la identidad es un derecho humano reconocido que va más allá de hacer una persona distinguible del resto, toda vez que responde a rasgos de pertenencia, reconocimiento y sentidos subjetivos que atienden a cada persona; mientras que la autenticación es un proceso mediante el cual a través de rasgos característicos únicos una persona se corrobora ser quien dice ser, es decir, que es un aspecto que exclusivamente sirve cuando una persona se puede hacer distinguible del resto de la población, ambos procesos actualmente se utilizan cómo un sinónimo e incluso se efectúan en un mismo proceso utilizando los datos biométricos, y atendiendo a la protección, garantía, promoción y respeto a los derechos humanos no debería ser de esta forma.

Es importante concluir que si bien la Ley General de Población ya establece el uso de datos biométricos en la Cédula de Identidad, la misma no tiene eficacia en el mundo fáctico porque es una legislación que no se aplica, a saber, son contados los casos de personas que cuentan con su cédula de identificación a pesar de ser una obligación, además como cualquier otro documento de identidad: acta de nacimiento, credencial para votar, pasaporte, cartilla del servicio militar, al contener estos datos de identidad, el derecho de su titular o persona a identificar de rectificar sus datos que atiendan a su realidad social actual como puede ser: el nombre, sexo, filiación, por lo que para el caso de datos biométricos no aplica para la modificación o corrección, y esto es así porque los datos biométricos pueden ser alterados o modificados pero el procedimiento ya involucra el sometimiento del cuerpo a proceso quirúrgicos, y por lo tanto este derecho se ve vulnerado en virtud que no es tan sencillo como cualquier otro dato de identidad.

Ahora bien, como se analizó en la investigación respecto de la Ley General de Población, Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, y el intento de incorporar el Registro Nacional de Usuarios de Telefonía Móvil, en las disposiciones inherentes al uso de datos biométricos como forma de identidad arriban a la conclusión que el Estado ha buscado el control de los datos biométricos de los individuos, y no es novedoso que el Estado sea quien lleve a cabo la labor de hacer identificable a las personas, pero el punto medular es la incorporación de datos biométricos que se procesan mediante medios tecnológicos, ópticos o telemáticos de forma automatizada, y que se almacenan en grandes bases de datos.

Las formas en que automáticamente se procesan los datos biométricos es el punto de partida para la solución del problema, bajo la línea de investigación que faltan normas que regulen y limiten el procesamiento de los datos biométricos ya sean por particulares o por el Estado, bajo el entendido que como se expuso al tratarse de datos biométricos como datos personales sensibles, les son aplicables disposiciones en materia de protección de datos personales, y pese a su tutela se

reconoce que existen vulnerabilidades, riesgos y ataques a todas aquellas bases de datos que contengan la biometría de las personas, y como fue motivo de estudio la trascendencia en su uso provoca que deban ser protegidos, atendiendo a que con los datos biométricos obtenidos es posible realizar el proceso de autenticación, identificación e incluso celebrar actos jurídicos a nombre de otra persona, de ahí que sea importante su regulación y establecer la responsabilidad de seguridad y conservación de la persona que trate los datos.

Bajo el anterior argumento, es que en la Ley General de Población y la Ley General de Protección de Datos Personales en Posesión de Particulares, así como de la Ley Federal de Protección de Datos Personales en Posesión de Particulares deben realizarse adiciones a disposiciones relativas al uso de datos biométricos como forma de identidad y como datos personales sensibles en las que se establezca la responsabilidad y garantía del responsable de los datos de responder para el caso de tratamientos no autorizados, robo de datos y demás delitos estudiados.

Lo anterior, porque como se precisó a lo largo de la investigación la responsabilidad del cuidado se puede decir que está a cargo del titular de los datos, además que los mecanismos disponibles para hacer valer los derechos sustantivos del gobernado no dotan al mismo de la suplencia de la queja o en su caso algún otro mecanismo de protección en virtud que el titular de los datos en su mayoría desconoce tanto de los derechos que goza, como de los procedimientos para su ejercicio e ignora el valor y utilidad de sus datos biométricos, así como tampoco sabe para que autoriza su tratamiento ni mucho menos se sabe si existió una transferencia o tratamiento no autorizado, ello pone de manifiesto la desventaja y vulnerabilidad del titular de los datos biométricos y porque debe operar en su favor la suplencia de la queja o instituciones jurídicas beneficiosas.

La importancia de la identidad ha quedado dilucidada en el cuerpo de investigación y de ella se concluye que es relevante y de interés público que existan

disposiciones imperativas que limiten el uso de los datos biométricos como forma de identificar a los individuos, porque mediante el uso de la tecnología la identidad ha incrementado sus acepciones, como la identidad digital, puntos que exigen que el jurista evolucione en temas que se han explorado pero que falta regular en el sistema jurídico mexicano, y que en el marco internacional hay pocos modelos a seguir, se propone que de forma reglamentaria en la normatividad que se contengan aspectos técnicos y de responsabilidad.

En sintonía con el párrafo que antecede, los procesos de autenticación son igual de importantes que el proceso de identidad, con la anotación que se ha realizado respecto que estos procesos deben realizarse por separado, pues su objetivo es distinto; por un lado se busca identificar a una persona del resto y respectivamente en la autenticación se busca cerciorar que una persona dice ser quien es, por lo tanto, es erróneo que en un mismo momento se pretenda identificar y autenticar a una persona, pues genera confusión y falta de certeza en el momento en virtud que las personas desconocen de ambos procesos y por ende de sus implicaciones, y que incluso se caiga en el error de una persona no desea autenticarse pero sí identificarse o viceversa.

La importancia de la separación de ambos procesos precisados radica principalmente que en la actualidad ambos se llevan en un mismo momento, toda vez que es un hecho notorio que ya ingresando a una aplicación o plataforma digital se le permite al usuario realizar actos como si fuere la persona que dice ser o la persona con la identidad que ostenta, aparte de permitirle celebrar actos jurídicos, por lo tanto resulta violatorio a la seguridad y certeza jurídica tuteladas constitucionalmente, pues a pesar de ser actos entre particulares los mismos afectan los derechos sustantivos de identidad, intimidad, protección de datos personales, nombre, es por ello que es necesaria su regulación desde nivel federal, general, y en la legislación local, que establezca los principios por los que deben regirse el uso de datos biométricos como forma de identidad y de otorgar el consentimiento en la celebración de actos jurídicos.

El principal sustento de la incorporación al sistema mexicano de las disposiciones referidas es la sensibilidad del uso de procesos de identidad y de autenticación con datos sensibles, biométricos, todo en cuanto al uso de sistemas de procesamiento automatizado y mediante sistemas informáticos, proponiendo que se creen apartados en las legislaciones citadas de tal suerte que se establezca como un derecho de recibir una indemnización por un tratamiento no autorizado o incluso como monto de reparación del daño por la comisión de delitos usando datos sensibles, bajo la inteligencia que este último deberá ser quien prevea de los recursos materiales, humanos y tecnológicos suficientes para asegurar el tratamiento correcto de los datos biométricos de los que sea responsable.

Se concluye en la necesidad de realizar un paquete de reformas en materia de protección de datos personales, en la que se establezca la naturaleza única de los datos biométricos, como datos personales sensibles difíciles de alterar, modificar o corregir, reformas que se proponen ser desde la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados y Ley Federal de Protección de Datos Personales en Posesión de Particulares, y que sirva como ley modelo para las legislaciones locales de las Entidades Federativas, así como establecer la responsabilidad directa del encargado o responsable en caso de vulneraciones, robo y riesgos de las bases de datos que contengan datos biométricos de las personas.

De igual forma, se deben incrementar las penalidades, establecer montos mínimos por concepto de reparación del daño e indemnizaciones que deben ser derechos del titular de los datos biométricos, ya sea por el tratamiento no autorizado o por ilícitos que vulneraron la seguridad de los sistemas informáticos del encargado o responsable, todo fundamentado en los derechos humanos que le reconocen al titular y cuya protección debe garantizarse por el Estado mediante los mecanismos jurídicos idóneos.

Aunado a lo anterior se deben implementar mecanismos de suplencia de queja en los procedimientos que tiene la normatividad en materia de protección de datos personales sostenidos en los argumentos que fueron precisados.

Se concluye que el tratamiento de datos personales sensibles, como el caso de los datos biométricos, resulta una medida innecesaria ya que la finalidad que se persigue puede agotarse con mecanismos menos intrusivos a los derechos humanos y el propósito de la identificación o autenticación puede lograrse razonablemente por otros medios automatizados pero que no utilicen datos inherentes sensibles; asimismo el uso es desproporcional y ventajoso para el encargado y responsable, ya que no se pondera su uso con los derechos fundamentales de titular, y que la norma imperativa actual remite toda la responsabilidad al titular, además admite la existencia de los riesgos y ataques a los sistemas informáticos a las bases de datos, y que estos pueden causar daños irreparables al titular.

Por otra parte, los datos biométricos se han utilizado a lo largo de los últimos años como una forma de otorgar el consentimiento para la celebración de actos jurídicos, incluso la legislación civil federal, Código de Comercio, así como la Ley de Instituciones de Crédito y la Ley para Regular las Instituciones de Tecnología financiera y sus disposiciones, Normas Oficiales Mexicanas, establecen y permiten la utilización de los datos biométricos como una forma de otorgar el consentimiento para la celebración de actos jurídicos.

El comercio electrónico, la contratación de servicios y adquisición de servicios mediante el uso de plataformas y aplicaciones digitales han sido actividades que al paso de los años han ido en aumento, y que inevitablemente han generado que el derecho busque regular esta realidad, por lo tanto han derivado de diversas adiciones y reformas para su implementación en México, o incluso la generación de nuevas leyes como es el caso de la Ley de la Firma Electrónica Avanzada y su reglamento, las Reglas Generales a las que deberán sujetarse los Prestadores de

Servicios de Certificación, que atienen a la posibilidad de otorgar el consentimiento de la celebración de un acto jurídico mediante una firma digital.

Como fue precisado, los datos biométricos mediante la implementación de tecnologías y sistemas avanzados de encriptación se han utilizado en similitud a una firma electrónica avanzada, con los mismos efectos, hechos que son carentes de sustento dentro del sistema jurídico mexicano, porque si bien se ha permitido el uso de medios ópticos y telemáticos o de otras tecnologías para la celebración de actos jurídicos, no se permite expresamente el uso de los datos biométricos para otorgar el consentimiento para celebrarlos, además que la legislación civil sustantiva los refiere como signos inequívocos que se equiparan al consentimiento expreso, y como se precisó dada la confusión entre un proceso de autenticación, identidad y ahora de celebración del acto jurídico, no es un signo inequívoco que en un plataforma mediante un dato biométrico, se permita el acceso a un usuario, se autentique su identidad y celebre actos jurídicos todo en un mismo momento y en una misma plataforma o aplicación.

En otras palabras, mediante el uso de aplicaciones y sistemas informáticos se ha permitido el uso de los datos biométricos para otorgar el consentimiento del usuario y generar efectos de derecho, ya sean derechos u obligaciones, circunstancia que no tiene regulación en el sistema jurídico mexicano, esto es, existe el vacío jurídico, en el entendido de llegar a considerar como regulación aplicable a los actos jurídicos celebrados de manera electrónica el Código de Comercio sí prevé dichas circunstancias y que además remite al uso de la Firma Electrónica Avanzada, por el contrario específicamente del uso de datos biométricos como una forma de otorgar el consentimiento no está previsto ni contiendo en hipótesis normativa alguna.

Establecido lo anterior, convino estudiar lo relativo a la Firma Electrónica Avanzada y su regulación en específico, a recordar, la Ley de la Firma Electrónica Avanzada y las Reglas Generales a las que deberán sujetarse los Prestadores de Servicios de Certificación, que sirven como un panorama para un futuro y que desde

este momento se propone, para que se regule el uso de los datos biométricos para la celebración de actos jurídicos y que se llegue a equiparar con una Firma Electrónica, porque no se está en contra de su uso o implementación en diversos procesos pero lo que se debe subsanar el problema del vacío jurídico e incertidumbre que genera su uso sin regulación..

De ese modo, la propuesta legislativa en materia de datos biométricos debe ser encaminada a la generación de disposiciones de carácter técnico-jurídico al igual que la de la Firma Electrónica Avanzada, para la implementación de la tecnología que capta, almacena y procesa los datos biométricos consideraciones que desde luego la legislación debe prever en aras de brindar material para ser posible el estudio y valor jurídico de la biometría de las personas como forma de consentir actos jurídicos y servir de prueba en caso de controversias derivadas de la celebración de actos electrónicos.

Se convalida que a lo anterior, debe asegurarse la fiabilidad de los sistemas automatizados de procesamiento mediante mecanismos más seguros en materia informática que prevengan los delitos informáticos que vulneren los derechos sustantivos de los usuarios de este tipo de plataformas, y esto sólo se logrará a través de certificaciones a los sistemas informáticos que contengan datos biométricos, y la propuesta en concreto es que se evalúen y tengan autorización por el órgano garante en la materia, Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, y por organismos técnicos regulados, como la creación de un órgano o instituto dedicado a la ciberseguridad y especializado en materia de derecho informático, mismos que serían los encargados de evaluar la seguridad de los sistemas informáticos y dar autorización para tratar con datos biométricos.

Los datos biométricos como una forma de manifestar el consentimiento expreso son una realidad que no es necesaria, pues se sostiene en esta conclusión que existen medios menos intrusivos para este fin, o incluso ya existe la Firma

Electrónica Avanzada para el mismo propósito, y es por ello que no podría justificarse su uso, pero en el caso que el derecho deba perseguir a la realidad será necesaria su regulación y que mejor que se tome en consideración una regulación que ya existe que también contiene aspectos técnicos.

En la misma línea de conclusión, es necesario que se regulen los servicios de banca móvil o banca digital que hoy son cada vez más comunes utilizar e incluso son ya obligatorios en caso de tener una cuenta bancaria, porque si no existiera la posibilidad de acceder a la banca móvil los servicios se vuelven tediosos y lentos, además de la pérdida de tiempo que implica acudir de manera presencial al banco a realizar los trámites o actos necesarios, es por ello que la Ley para Regular la Instituciones de Tecnología Financiera y sus disposiciones, así como la Ley de Instituciones de Crédito, deben ser reformadas de modo que no sólo mencionen a los datos biométricos como una forma de otorgamiento del consentimiento, sino que ordenen dirigir la responsabilidad por la vulnerabilidad al mismo banco, pues son ellos quienes al final del día se benefician con los servicios que brindan electrónicamente, ya que han hecho más eficientes sus procesos y requieren cada vez menos de recursos humanos y materiales para sus operaciones.

De igual forma, es necesario que se distingan en estas aplicaciones de banca móvil los momentos y procesos, es decir, primero la autenticación de una persona, luego su autenticación, y posteriormente se pida para la celebración de un acto jurídico su Firma Electrónica Avanzada, en la inteligencia que la utilidad de los datos biométricos correctamente empleados sería como un segundo o tercer paso dentro de la identidad y autenticación, donde el ideal es que exclusivamente los datos biométricos sirvan como soporte o ayuda para brindar seguridad en el ingreso y autenticación del usuario dentro de la plataforma, toda vez que como se precisó estos brindan un mayor sentimiento de confianza y fiabilidad en el usuario, pero estos no deberían ser utilizados excesivamente o exclusivamente en un sólo momento ni para un varios procesos.

Por todo lo anterior, es indispensable que se ejecute un ejercicio de ponderación de derechos sobre los beneficios que tiene la utilización de los datos biométricos como forma de identidad y de otorgar el consentimiento para actos jurídicos, actividad que desde luego siempre debe obedecer a los principios y derechos tanto constitucionales como convencionales, pues no por tener un beneficio económico-temporal deben implementarse métodos intrusivos sin justificación para intentar beneficiar al usuario, cuando en su utilización siempre se deriva la responsabilidad al usuario y titular de los datos biométricos, por el contrario, deben maximizarse y legislarse a favor de sus derechos de identidad, intimidad y protección de datos personales.

Se concluye también que los datos biométricos contenidos en bases de datos de forma digital en sí constituyen un riesgo y peligro para los titulares, pues como se estudió en el último capítulo existen riesgos latentes sobre las bases de datos, también existen delitos en materia de seguridad informática que contienen hipótesis de conductas antijurídicas que advierte la vulnerabilidad que corren los datos almacenados en bases de datos digitales.

Los hechos delictivos referidos en el párrafo que antecede fueron motivo de estudio en el cuerpo de la investigación y que se arribó a sostener que los delitos informáticos y que importan directamente con los datos biométricos son el de usurpación y robo de identidad y que estos tipos penales sólo se prevén en contadas legislaciones sustantivas locales, pero en materia federal no hay disposición expresa al respecto de los datos biométricos, así como tampoco se incorporan en las demás legislaciones locales, por lo tanto la conclusión y propuesta es que se necesita cubrir el vacío legal y subsanar los vacíos legales existentes en materia punitiva respecto a los datos biométricos, ya sea que se incorporen nuevos tipos penales o se robustezcan los actuales añadiendo agravantes por el uso de la biometría de las personas para cometer las conductas delictivas.

En los últimos puntos, se llegó a la conclusión que además de todo lo abordado del aspecto jurídico, se necesita armonizar la legislación con la ciencia informática y de ciberseguridad para brindar la protección a los sistemas informáticos, telemáticos o de otra tecnología que traten datos biométricos, de tal suerte que el derecho exigirá un nuevo perfil de juristas que responda a las exigencias digitales más actuales y permitan la coexistencia de la tecnología en el ámbito legislativo.

Para ir cerrando las conclusiones restantes, se establece que no se pretende de ninguna forma atacar el avance tecnológico y los nuevos mecanismos de procesamiento de información automatizados, pero sí se busca exponer y tratar de solucionar el problema consistente en que el sistema jurídico mexicano se ve superado por una realidad tecnológica, porque la solución principal es la implementación de mecanismos protectores a través de la tarea legislativa y que se colmen los vacíos en materia del uso de datos biométricos como forma de identidad y de consentir actos jurídicos.

Ningún derecho es ilimitado pero los derechos sustantivos a la identidad, intimidad y protección de datos personales en el plano fáctico en México por la utilización de los datos biométricos sin regulación se ven vulnerados, en virtud que como se argumentó a lo largo la investigación, se ha vislumbrado la falta de regulación benéfica para el usuario-titular e inexistente norma imperativa en diversas disposiciones en materia de biometría de las persona.

Por lo tanto en el panorama actual de los derechos humanos es necesario que se cumplan las obligaciones de garantizar, promover, respetar y proteger los datos biométricos como su naturaleza lo exige y esto se vio durante la realización de la investigación cuando se resolvió respecto de la incorporación de datos biométricos en el Registro Nacional de Usuarios de Telefonía Móvil, advirtiendo de origen el cumplimiento de esa obligación.

Finalmente, se concluye que a futuro será inevitable que se traten de agilizar los procesos mediante el uso de la tecnología, y la tarea que se tiene como jurista es tratar de dar las herramientas, acciones y mecanismos que permitan al usuario-titular de los datos biométricos hacer un frente contra las arbitrariedades o vacíos de los que se aprovechan los responsables, es por ello que el perfil del operador del derecho debe encaminarse a entender los nuevos paradigmas tecnológicos y adecuarlos en la realidad para poderlos regular.

Por último, se llega a la conclusión general que el uso de los datos biométricos como forma de identidad y como una forma de otorgar el consentimiento para la celebración de actos jurídicos mediante medios digitales necesita de regulación adecuada, y que esta norma imperativa debe atender a la vulnerabilidad que tiene el usuario-titular, para equilibrar el acceso a la justicia entre este último y el encargado o responsable, cualquier tercero particular moral o físico o el mismo Estado, para cambiar el sentido de las normas actuales y crear nuevas normas en favor del titular, el uso de la biometría es el medio más intrusivo de identificar, autenticar y celebrar actos jurídicos y por lo tanto siempre debe justificarse su implementación, porque el simple de hecho de tratarlos pone en riesgo y vulnera los derechos humanos de los titulares de los datos biométricos.

VI. FUENTES

VI.1. BIBLIOGRAFÍA

AZAOLA CALDERÓN, Luis, *Delitos informáticos y derecho penal*, México, Editorial UBIJUS, 2010.

BARRAGÁN, Julia, *Informática y Decisión Jurídica*, México, Editorial Fontamara 2000.

BÉJAR NAVARRO, Raúl y Héctor M. Cappello y García, *Aproximaciones a la identidad nacional y sus correlatos fácticos,* México, Instituto de Investigaciones Sociales UNAM, 2009.

CARMONA, Alejandro, *Evolución de los medios de comunicación*, México, Editorial Limusa, 1999.

CARRANZA TORRES, Luis, *Habeas data. La protección jurídica de los datos personales*, Argentina, Editorial Alveroni, 2001.

CARRASCOSA LÓPEZ, Valentín, *La contratación informática: el Nuevo Horizonte Contractual: los Contratos Electrónicos e Informáticos*, España, Editorial Comares, 2000.

CHICANO TEJADA, Ester, *Utilización de las bases de datos relacionales en el sistema de gestión y almacenamiento de datos*, Málaga, IC Editorial, 2013.

COMISIÓN DE DERECHOS HUMANOS DEL DISTRITO FEDERAL, *Informe especial, situación de los derechos humanos de las poblaciones callejeras en el Distrito Federal 2012-2013*, México, CDHDF, 2014, disponible en: <https://piensadh.cdhdf.org.mx/images/publicaciones/Informe_especial/2014_Informe_esp_poblaciones_callejeras.pdf>

CONDE ORTIZ, Concepción, *La Protección de Datos Personales: Un Derecho Autónomo Con Base En Los Conceptos de Intimidad y Privacidad*, Madrid, Editorial Dykinson, 2005.

CONDE VILDA, Cristina, *Biometría, reconocimiento facial mediante fusión 2D y 3D*, España, Editorial Dykinson, 2007.

CORRAL JURADO, Javier y Beatriz Solís Leree, *Protección de Datos Personales, Compendio de lecturas y legislación*, México, Tiro Corto Editores, 2010.

DÁVALOS TORRES, María Susana, *Manual de introducción al derecho mercantil*, México, Instituto de Investigaciones Jurídicas UNAM, 2010.

DAVARA RODRÍGUEZ, Miguel, *Manual de Derecho Informático*, 11ª edición, España, Editorial Aranzadi, 2011.

DIAZ LIMÓN, Jaime Alberto, *Abogado digital; estudios sobre derecho cibernético, informático, digital*, México, Universidad Ius Semper, 2019.

DIAZ HERNÁNDEZ, Marianne, *El cuerpo como dato,* Venezuela, Editorial Derechos Digitales, 2018, disponible en: <https://www.derechosdigitales.org/wp-content/uploads/cuerpo_DATO.pdf>

DIRECCIÓN DEL REGISTRO NACIONAL DE POBLACIÓN E IDENTIFICACIÓN PERSONAL, *Registro e Identificación de Población,* México, Secretaría de Gobernación, disponible en:<https://www.transparenciapresupuestaria.gob.mx/work/models/PTP/Reingenieria_Gasto/imagenes/Ventanas/Ramo_4/04E012.pdf>

ESTRADA CAMACHO, Israel, *Huella genética vs. Huella dactilar*, México, Procuraduría General de la República, 2014, disponible en: <https://biblat.unam.mx/hevila/Archivosdecriminologiaseguridadprivadaycriminalistica/2015/vol4/6.pdf>

FERNÁNDEZ DE MARCOS, Isabel Davara, *Breve análisis de la reforma al artículo 6° constitucional en lo relativo a protección de datos personales*, en Carbonell, Miguel y Bustillos, Jorge (coord.), Hacia una democracia de contenidos: la reforma constitucional de transparencia, México, Instituto de Investigaciones Jurídicas UNAM, 2007.

FLORES SALGADO, Lucerito, *Derecho informático*, México, Editorial Patria, 2009.

GIMÉNEZ, Gilberto, C*ultura, Identidad y Procesos de Individualización*, México, Instituto de Investigaciones Sociales, Universidad Nacional Autónoma de México, 2010.

GARCÍA BARRERA, Myrna Elia, *Derecho de las nuevas tecnologías*, México, Instituto de Investigaciones Jurídicas, UNAM, 2008.

GARRIAGA DOMINGUEZ, Ana, *Tratamiento de datos personales y derechos fundamentales*, Madrid, segunda edición, editorial Dykinson, 2009.

GOMÉZ FRÖDE, Carina y Marco Ernesto Briseño García Carrillo, cood., *Nuevos paradigmas del derecho procesal*, México, Instituto de Investigaciones Jurídicas UNAM, 2016.

GÓMEZ-ROBLEDO VERDUZCO, Alonso, *et al.*, *Protección de Datos Personales en México: El Caso del Poder Ejecutivo Federal*, México, Instituto de Investigaciones Jurídicas, UNAM, 2006.

GOZAINI, Osvaldo Alfredo, *Habeas data. Protección de datos personales*, Argentina, Rubinzal-Culzoni Editores, 2001.

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES, *Conceptos Generales de la Protección de Datos Personales*, México, INAI, volumen 1.

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES, *Guía para el Tratamiento de Datos Biométricos*, México, INAI, 2018.

LÓPEZ-AYLLÓN, Sergio y David Arellano Gault, *Estudio en materia de transparencia de otros sujetos obligados por la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental*, México, colaboración IFAI, CIDE, UNAM, 2019.

LÓPEZ-VIDRIERO, Tejedor y Efrén Pascual Santos, *Protección de datos personales. manual práctico para empresas*, España, Editorial Fundación Confemetal, 2005.

LÓPEZ BARRIENTOS, María Jaquelina y Cintia Quezada Reyes, *Fundamentos de seguridad informática*, México, Facultad de Ingeniería UNAM, 2006.

LÓPEZ SANCHEZ, Rogelio y José Luis Leal Espinoza, *El derecho a la información y datos personales en México, una visión comparada con el sistema interamericano y europeo de derechos humanos,* México, Editorial Dykinson, 2018.

LOREDO GONZÁLEZ, Jesús Alberto y Aurelio Ramírez Granados, *Delitos Informáticos: su clasificación y una visión general de las medidas de acción para combatirlo*, Nuevo León, Facultad de Ciencias Físico Matemáticas, Universidad Autónoma de Nuevo León, México, 2013.

MARTÍNEZ GONZÁLEZ, María Mercedes, *Informática jurídica para estudiantes de derecho*, México, Editorial Tecnos, 2014.

MERINO TAPIADOR, Mateos y Juan Sigüenza Pizarro, *Tecnologías biométricas aplicadas a la seguridad*, México, Editorial Ra-Ma. 2005.

ORGANIZACIÓN PARA LA COOPERACIÓN Y DESARROLLO ECONÓMICOS, *Recommendation on electronic authentication and OECD guidance for electronic*

authentication, OCDE, 2007, disponible en: <http://www.oecd.org/sti/ieconomy/38921342.pdf >

OROPEZA, Doris Karina, *La competencia económica en el comercio electrónico y su protección en el sistema jurídico mexicano*, México, Instituto de investigaciones Jurídicas, UNAM, 2018.

OVILLA BUENO, Rocío, *La protección de los datos personales en México*, México, Editorial Porrúa, 2005.

QUINTANA ADRIANO, Elvia Arcelia, *Marco jurídico de las finanzas,* México, Instituto de Investigaciones Jurídicas, UNAM, 2018.

RASCÓN CASTILLO, Rosa del Carmen, *Uso de datos biométricos como método para otorgar el consentimiento en la contratación electrónica, algunos aspectos a considerar*, México, INFOTEC Centro de Investigación e Innovación en tecnologías de la información y comunicación, 2019.

RED IBEROAMERICANA DE PROTECCIÓN DE DATOS PERSONALES, *Estándares de Protección de Datos Personales*, RIPD, disponible en: <https://www.redipd.org/sites/default/files/inline-files/Estandares_Esp_Con_logo_RIPD.pdf>.

ROJINA VILLEGAS, Rafael, *Compendio de derecho civil, introducción, personas y familia*, México, Editorial Porrúa, vigésimo novena edición, 2000.

ROMERO CASTRO, Irene Martha, *et al.*, *Introducción a la seguridad informática y el análisis de vulnerabilidades*, Manabí, Ecuador, Editorial Área de Innovación y Desarrollo, Primera edición, 2018.

ROMERO FLORES, Rodolfo, *El robo o Usurpación de Identidad por Medios Informáticos o telemáticos: su tratamiento jurídico penal*, México, Instituto de Investigaciones Jurídicas, UNAM.

SÁNCHEZ CORTÉS, Laura Adriana, *Manual para el uso de datos biométricos en los servicios financieros,* México, INFOTEC CENTRO DE INVESTIGACIÓN E INNOVACIÓN EN TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN, 2019, disponible en: https://infotec.repositorioinstitucional.mx/jspui/bitstream/1027/329/1/INFOTEC_MDTIC_LASC_10102019.pdf

Seguridad informática, México, UNAM, disponible en: <http://www.ptolomeo.unam.mx:8080/xmlui/bitstream/handle/132.248.52.100/250/A5.pdf?sequence=5&isAllowed=y>

Seguridad informática hacking ético: conocer el ataque para una mejor defensa, Barcelona, España, Ediciones ENI (Epsilon), 4a edición, 2018, disponible en: <https://search-ebscohost-com.pbidi.unam.mx:2443/login.aspx?direct=true&db=cat02025a&AN=lib.MX001002087437&lang=es&site=eds-live >

TÉLLEZ VALDÉS, Julio, *Derecho informático*, 4ta Edición, México, Editorial Mc Graw Hill, 2008.

TOLOSA BORJA, César y Álvaro Giz de Bueno, *Sistemas biométricos,* México, disponible en: <https://www.dsi.uclm.es/personal/MiguelFGraciani/mikicurri/Docencia/Bioinformatica/web_BIO/Documentacion/Trabajos/Biometria/Trabajo%20Biometria.pdf >

VI.2. JURISPRUDENCIA

Gaceta del Semanario Judicial de la Federación, Libro 67, junio de 2019, Tomo II, página 1029, Décima Época, 1a. XLIX/2019 (10a.), Registro digital número 2020107. Disponible en: <https://sjf2.scjn.gob.mx/detalle/tesis/2020107>

Gaceta del Semanario Judicial de la Federación, libro 8, diciembre de 2021, Tomo II, página 1141, Undécima Época, 1a./J. 29/2021 (10a.), Número de registro digital: 2023890. Disponible en: <https://sjf2.scjn.gob.mx/detalle/tesis/2023890>

Gaceta del Semanario Judicial de la Federación, libro 43, junio de 2017, Tomo I, página 580, Décima época, 1a. LXXIII/2017 (10a.), número de registro digital: 2014646. Disponible en: <https://sjf2.scjn.gob.mx/detalle/tesis/2014646>

Semanario Judicial de la Federación y su Gaceta. libro VI, marzo de 2012, Tomo 1, página 273, Décima Época, 1a. XLV/2012 (10a.). número de registro digital: 2000340. Disponible en: <https://sjf2.scjn.gob.mx/detalle/tesis/2000340>

VI.3. HEMEROGRAFÍA

ASOCIACIÓN POR LOS DERECHOS CIVILES, *Desafíos de la biometría para la protección de datos personales: Reflexiones sobre el caso SIBIOS,* Argentina, 2017, disponible en: <https://adc.org.ar/>

BANCO MUNDIAL, *Sistemas de identificación digitales fiables e inclusivos pueden abrir oportunidades para las personas vulnerables del mundo,* Banco Mundial, agosto 2019, número 1, disponible en:<https://www.bancomundial.org/es/news/immersive-story/2019/08/14/inclusive-and-trusted-digital-id-can-unlock-opportunities-for-the-worlds-most-vulnerable>

DÍAZ RODRIGUEZ, Vanessa, *Licencia biométrica, caja de pandora, Hechos y Derechos,* México, UNAM, Instituto de Investigaciones Jurídicas, 2013, núm. 16, disponible en: <https://revistas.juridicas.unam.mx/index.php/hechos-y-derechos/article/view/6867/8803 >

GONZÁLEZ PADILLA, Roy, *Protección de Datos Personales en Posesión de Particulares*, México, Instituto de Investigaciones Jurídicas UNAM, disponible en: <https://revistas-colaboracion.juridicas.unam.mx/index.php/decoin/article/viewFile/33230/30194>

HUERTA ANGUIANO, Julio Alberto, *Naturaleza intrínseca, "contexto" o "finalidad" en la determinación del carácter sensible de los datos personales*, en Revista del

Instituto de Investigaciones Jurídicas, México, Ciudad de México, junio-diciembre 2020, página 5, disponible en: <https://revistas.juridicas.unam.mx/index.php/derecho-informacion/article/view/14658/15717>

Iniciativa que adiciona diversas disposiciones al Código Penal Federal, en materia de robo de identidad, a cargo del diputado Vicente Alberto Onofre Vázquez, del grupo parlamentario de Morena, del 14 de octubre del 2021, disponible en: <http://sil.gobernacion.gob.mx/Archivos/Documentos/2021/10/asun_4234504_20211014_1634235907.pdf >

INSTITUTO FEDERAL DE TELECOMUNICACIONES, *La Suprema Corte de Justicia de la Nación concede al Instituto Federal de Telecomunicaciones suspensión dentro la Controversia Constitucional 71/2021 promovida en contra del Padrón Nacional de Usuarios de Telefonía Móvil, México,* Comunicación y Medios, (Comunicado 55/2021) 15 de junio 2021, disponible en: <www.ift.org.mx>

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES, *CONSEJERÍA JURÍDICA DEBE INFORMAR SOBRE CONTROVERSIA CONSTITUCIONAL PRESENTADA POR EL IFT EN CONTRA DEL PANAUT: INAI,* México, Dirección General de Comunicación Social y Difusión, 14 de noviembre del 2021, disponible en:<https://home.inai.org.mx/wp-content/documentos/SalaDePrensa/Comunicados/Nota%20INAI-101-21.pdf>

JUARÉZ PÉREZ, Melecio Honorio, *Análisis legal de documentos electrónicos,* México, Instituto de Investigaciones Jurídicas UNAM, número 55, enero-febrero 2020, disponible en: <https://revistas.juridicas.unam.mx/index.php/hechos-y-derechos/article/view/14360/15524>

MÁRTINEZ DÍAZ BARRIGA, Leticia Adriana y Sergio Octavio González Nevarez, *La construcción de los procesos de identidad de las y los docentes de educación*

física, México, X Congreso Nacional de Investigación Educativa, número 16, disponible en: <www.comie.org.mx>

MORALES SANDOVAL, Miguel Ángel, *Nuestra identidad digital después de la muerte,* México, Instituto de Investigaciones Jurídicas, UNAM, julio- agosto 2020, número 58. <https://revistas.juridicas.unam.mx/index.php/hechos-y-derechos/article/view/14978/15940>

PÉREZ, Isabel, Avances en la identificación de las personas mediante las huellas dactilares, México, Universidad Nacional Autónoma de México, 11 de mayo del 2020. <http://ciencia.unam.mx/leer/994/avances-en-la-identificacion-de-personas-mediante-las-huellas-dactilares>

PÉREZ SERNA, Jesús Mayo, *Los derechos ARCO (Acceso, Rectificación, Cancelación y Oposición)*, México, 12 mayo del 2010, disponible en: <https://ayudaleyprotecciondatos.es/derechos-arco/>

PICHARDO FLORES, Lorena, *El valor de los datos se relaciona con su vulnerabilidad*, México, Dirección General de Comunicación Social, Universidad Nacional Autónoma de México, 28 de julio del 2021, disponible en: < https://www.dgcs.unam.mx/boletin/bdboletin/2021_613.html#:~:text=En%20la%20era%20digital%20los,Personales%2C%20de%20la%20Unidad%20de >

ROMERO CERDÁN, Tábata Andrea, *La autenticación y verificación de la identidad a través de información biométrica como paradigma del tratamiento de datos personales en México*, Revista del Posgrado de Derecho de la UNAM, México, Ciudad de México, 27 de agosto del 2019, disponible en: http://revistaderecho.posgrado.unam.mx/index.php/rpd/article/view/85/237#toc>

SANTILLÁN, María Luisa, *Los derechos de los invisibles,* México, Universidad Nacional Autónoma de México, 2019, número 1. <http://ciencia.unam.mx/leer/839/los-derechos-de-los-invisibles-identidad-legal-de-las-poblaciones-callejeras>

SECRETARÍA DE GOBERNACIÓN, *Conoce los mecanismos de identidad digital,* México, Blog Oficial de la Secretaría de Gobernación, 2017, número 1, disponible en: https://www.gob.mx/identidad/es/articulos/identidad-digital>

SEPÚLVEDA, Magdalena, *Tecnología biométrica en programas sociales, ¿una preocupación legítima*, México, MEXICO SOCIAL, 30 de mayo del 2019, disponible en: <https://www.mexicosocial.org/magdalena-sepulveda-tecnologia-biometrica-programas-sociales/>

TORRES CARRASCO, Katia Gesell, *Sistemas de identificación de personas,* México, Ecos Sociales, 2020, número 23, disponible en: <file:///C:/Users/Roberto%20M%20L/Downloads/4155-Texto%20del%20art%C3%ADculo-22274-1-10-20201127.pdf>

VÉLEZ MARTÍNEZ, Cuauhtémoc, *Dispositivos Biométricos,* México, Instituto de Ingeniera, Universidad Nacional Autónoma de México, núm. 11, disponible en: <www.ii.unam.mx>