



MAESTRÍA EN DERECHO DE LAS TECNOLOGÍAS
DE INFORMACIÓN Y COMUNICACIÓN

INFOTEC CENTRO DE INVESTIGACIÓN E
INNOVACIÓN EN TECNOLOGÍAS DE LA
INFORMACIÓN Y COMUNICACIÓN

DIRECCIÓN ADJUNTA DE INNOVACIÓN Y
CONOCIMIENTO
GERENCIA DE CAPITAL HUMANO
POSGRADOS

**“MANUAL
DIDÁCTICO PARA
USUARIOS DE LA
RED EN EL
RECONOCIMIENTO
DE LA IDENTIDAD
DIGITAL.
¿QUIÉNES SOMOS
EN INTERNET?”**

PROPUESTA DE INTERVENCIÓN
Que para obtener el grado de MAESTRO EN
DERECHO DE LAS TECNOLOGÍAS DE
INFORMACIÓN Y COMUNICACIÓN

Presenta: Lorena Navarro Manzanilla

Asesora: Dra. Ana Josefina Bello Jiménez

Ciudad de México, diciembre 2021



AUTORIZACIÓN DE IMPRESIÓN Y NO ADEUDO EN BIBLIOTECA
MAESTRÍA EN DERECHO DE LAS TECNOLOGÍAS DE INFORMACIÓN Y
COMUNICACIÓN

Ciudad de México, 1 de octubre de 2021
INFOTEC-DAIC-GCH-SE-0299/2021.

La Gerencia de Capital Humano / Gerencia de Investigación hacen constar que el trabajo de titulación intitulado

Manual didáctico para usuarios de la
red en el conocimiento de la identidad
digital ;Quiénes somos en la Internet.

Desarrollado por la alumna **Lorena Navarro Manzanilla** y bajo la asesoría de la **Dra. Ana Josefina Bello Jiménez**; cumple con el formato de Biblioteca. Por lo cual, se expide la presente autorización para impresión del proyecto terminal al que se ha hecho mención.

Asimismo, se hace constar que no debe material de la biblioteca de INFOTEC.

Vo. Bo.



Lic. Juan Ramón Abarca Damián
Coordinador de Biblioteca

Anexar a la presente autorización al inicio de la versión impresa del trabajo referido que ampara la misma.

Tabla de contenido

| | |
|--|-----------|
| Tabla de contenido | 5 |
| Introducción | 1 |
| Capítulo 1. Identidad y conceptos básicos | 3 |
| 1.1. Identidad y atribuciones de la personalidad | 4 |
| 1.2. Conceptos básicos sobre la identidad | 9 |
| 1.2.1. ¿Qué es identidad?..... | 10 |
| 1.2.2. Derecho a la identidad..... | 13 |
| 1.2.3. ¿Qué es la identidad legal?..... | 18 |
| 1.2.4. ¿Qué es un dato personal?..... | 19 |
| 1.2.5. ¿Qué es privacidad?..... | 23 |
| Capítulo 2. Internet, sociedad y su impacto en el Derecho | 28 |
| 2.1. Internet descripción y nociones básicas | 29 |
| 2.2. La sociedad de la información frente al uso de Internet | 34 |
| 2.3. Internet y sociedad, su impacto en derecho | 41 |
| Capítulo 3. La identidad digital | 53 |
| 3.1. ¿Qué es la identidad digital? | 54 |
| 3.2. Reconocimiento de la identidad digital | 56 |
| 3.3. Atribuciones de la identidad digital | 61 |
| 3.4. Sistemas de identificación digital | 65 |
| 3.5. Identidad digital y las redes sociales | 67 |
| 3.6. Identidad digital y protección de datos personales | 72 |
| 3.7. Identidad digital post mortem | 77 |
| Capítulo 4. Instrumentos de regularización de la identidad digital | 85 |
| 4.1. Análisis de casos internacionales prácticos aplicables al reconocimiento de la identidad digital | 86 |
| 4.1.1. Unión Europea (<i>eIDAS -Regulation</i>) | 86 |
| 4.1.2. Bélgica (Belgian Mobile ID)..... | 87 |
| 4.1.3. Reino Unido (<i>GOV.UK Verify</i>)..... | 88 |
| 4.1.4. Iniciativa ID4D de la ONU y el Banco Mundial. | 10 |

| | |
|---|------------|
| 4.2.Análisis de casos nacional prácticos aplicables al reconocimiento de la identidad digital..... | 91 |
| 4.2.1. Mecanismos de “identidad digital” implementados por el Gobierno Mexicano (https://www.gob.mx/identidad)..... | 91 |
| 4.2.2. Iniciativa para expedir la Ley General de Identidad y Ciudadanía Digital. | 93 |
| Conclusiones | 99 |
| Bibliografía..... | 102 |

Índice de figuras

| | |
|---|----|
| Figura 1. Aspectos Generales. Nombres de dominio y protocolo de internet | 31 |
| Figura 2. Personas que usan Internet (% de la población a nivel mundial) | 32 |
| Figura 3. Porcentaje de la población de seis años o más según condición de uso de Internet, 2019 | 42 |
| Figura 4. Distribución de los usuarios de Internet en áreas urbano-rural | 42 |
| Figura 5. ¿Qué riesgos puedes sufrir en Internet?, INAI | 45 |
| Figura 6. Protección de datos personales y ciberseguridad, INAI | 49 |
| Figura 7. 10 ejes principales de las Recomendaciones en el entorno digital, INAI | 59 |
| Figura 8. Usuarios de internet en México, We are social e INEGI | 60 |
| Figura 9. 6° Estudio sobre los Hábitos de los Usuarios de Internet en México 2020, Asociación de Internet.MX | 61 |
| Figura 10. Redes sociales en el mundo, We are social e INEGI | 69 |
| Figura 11. Como proteger tus datos personales en las redes sociales, INAI | 74 |
| Figura 12. Principios de identificación para el desarrollo sostenible | 91 |
| Figura 13. Principios de identificación para el desarrollo sostenible | 93 |

Índice de cuadros

| | |
|--|----|
| Cuadro 1. Padrón Electoral (INE, corte al 15 de enero de 2021) | 16 |
| Cuadro 2. Atributos que constituyen la Identidad | 63 |
| Cuadro 3. <i>World Economic Forum. “The Global Risks Report 2020”, 15th Edition</i> | 96 |

Introducción

Internet ha cambiado de forma radical la forma en que interactuamos. La economía y la sociedad han evolucionado tan rápido hacia un mundo de interconexión digital, en donde a partir de mediados de la década de los 90's surgió el movimiento denominado "revolución digital", el cual tiene como principal factor la posibilidad de que las personas puedan establecer comunicaciones a través de sistemas informáticos remotos, en un mundo global que trasciende más allá de las fronteras nacionales, originando nuevas dinámicas de comportamiento e interacción entre los seres humanos, en donde se forja un intercambio de información masivo, nuevos hábitos, incluido la forma de identificación.

De forma tradicional, nuestros sistemas de identidad se han basado en interacciones físicas y mediante la acreditación de documentos tangibles, para demostrar quienes somos, siendo un factor fundamental en el desarrollo social, económico, financiero y gubernamental.

El aumento exponencial en el uso del Internet y las nuevas tecnologías de la información y comunicación generó la necesidad de demostrar quienes somos en la red, es decir, acreditar nuestra identidad de forma digital. Lo anterior, ante la necesidad de las personas y empresas de encontrar soluciones de acreditación de identidad válidas y seguras para la prestación de servicios, mercados, estándares y reconocimiento digital.

La identidad resulta un término complejo para conceptualizar, el cual es un factor esencialmente humano y que de forma general se compone por el conjunto de características que definen a una persona y lo permite ser identificable, como consecuencia, la identidad digital sería la versión de la identidad física de una persona en la red, por lo que dicho reconocimiento se ha convertido en la forma de representación individual respecto a nuestra interacción y actuar en el mundo digital.

El presente trabajo, tiene como objetivo, generar una investigación que permita guiar a los usuarios para gestionar y administrar adecuadamente su identidad digital, mediante la educación e información, previniendo una posible vulneración a sus datos personales y su privacidad, elementos que se encuentran vinculados con su identificación y diferenciación como usuarios.



Capítulo 1.
Identidad y conceptos básicos

Capítulo 1. Identidad y conceptos básicos

Los derechos humanos se caracterizan de forma general como derechos individuales, en ese sentido y conforme a nuestro tema en particular, el derecho a la identidad es reconocido como un derecho humano fundamental que brinda existencia jurídica a los seres humanos¹, ya que se encuentra íntimamente ligada a su individualidad, información, datos personales y su vida privada, elementos que se encuentran vinculados al derecho y desarrollo del ser humano dentro de una colectividad.

Para comprender mejor su concepto, la palabra identidad proviene del latín *identitas* y este de *ídem* (lo mismo), al respecto, la Comisión de Derechos Humanos del Distrito Federal, ahora Ciudad de México, define a la identidad como un elemento esencial del ser humano “que representa la individualidad de cada uno y la potencialidad de desarrollarnos como personas y como parte de un grupo social, [...] así como gozar y ejercer las libertades y los derechos que el orden jurídico nos reconoce y otorga”²

El concepto de identidad cuenta con una dualidad en su definición, por una parte, se refiere a características que poseen las personas que nos hacen percibir que son lo mismo, por ejemplo, un grupo de hombres o de mujeres y por el otro, se refiere a características que nos hacen percibir que una persona es única, diferente a las demás, que permite identificar específicamente e inequívocamente a una persona, como lo son los datos personales.³

Para efectos del presente trabajo, podemos comprender que la identidad se refiere a la combinación de características y atributos que hacen a una persona única en un contexto dado, sí bien, hay atributos personales que son inherentes a la persona, lo cierto, es que también hay atributos particulares más relevantes como

¹ López Velarde Campa, Jesús Armando Coordinador, *El derecho a la identidad como base para el ejercicio de los derechos humanos de niñas, niños y adolescentes en situación de calle en la Ciudad de México*, Instituto de Investigaciones Jurídicas UNAM, Primera edición, México, 2017.

² 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, Recuperado de: <http://cdhdf.org.mx/wp-content/uploads/2014/09/poblaciones-callejeras-integrado-imprenta.pdf> (consultado en agosto 2020)

³ Anders, V. et al. *Etimología*, 2001-2020. Recuperado de: <http://etimologias.dechile.net/?identidad> (consultado en agosto 2020)

en un contexto biográfico de datos personales, como por ejemplo, el nombre, edad, dirección, entre otros, así como también la existencia de peculiaridades biométricas como la imagen, rostro, huellas dactilares o escaneo de iris, que nos hacen únicos y permiten nuestra identificación inequívoca e irrepetible.⁴

Todas estas características se encuentran íntimamente ligadas a la personalidad del sujeto, representado por el conjunto de atributos que lo identifican, otorgándole una identidad que bajo la garantía de su reconocimiento como derecho humano, permiten reconocer y otorgar la oportunidad al individuo de ejercer plenamente sus derechos, no sólo de reconocimiento e identificación, sino también, de desarrollo económico, social, cultural, así como, aquellos de carácter civil y político, los cuales se relacionan con el ejercicio pleno de la nacionalidad y ciudadanía del individuo.⁵

1.1. Identidad y atribuciones de la personalidad.

La identidad y la personalidad son dos conceptos que van unidos⁶, sin embargo, de forma particular, podemos concebir a la identidad como un elemento esencial del ser humano “que representa la individualidad de cada uno y la potencialidad de desarrollarnos como personas y como parte de un grupo social, [...] así como gozar y ejercer las libertades y los derechos que el orden jurídico nos reconoce y otorga”. La identidad personal significa “ser en sí mismo, representado en sus propios caracteres y sus propias acciones, constituyendo la misma verdad de la persona”.⁷

En la antigüedad no todos los seres humanos eran considerados como personas, por lo que, para ser reconocidos dependían de diversos factores como la libertad, ciudadanía y estatus social, para ser sujetos de derechos y obligaciones.

⁴ World Bank, *Digital Identity Toolkit*, Working Paper, Washington D.C., 2014, Recuperado de: <http://documents.worldbank.org/curated/en/2014/06/20272197/digital-identity-toolkit-guide-stakeholders-africa> (consultado en julio 2020)

⁵ Secretaría de Gobernación, *El derecho a la identidad como derecho humano*, México, SEGOB, 2010, p.4.

⁶Fernández Elisa, “Identity and personality: or as we know we are different from others”, *Revista Digital de Medicina Psicosomática y Psicoterapia*, Sociedad Española de Medicina Psicosomática y Psicoterapia, 2011, pág. 1.

⁷ Jiménez García, Hilda Adriana A., López Velarde Campa, Jesús Armando Coordinador. *El derecho a la identidad como base para el ejercicio de los derechos humanos de niñas, niños y adolescentes en situación de calle en la Ciudad de México*, Instituto de Investigaciones Jurídicas UNAM, Primera edición, México, 2017, p. 120.

Sin embargo, con la abolición de la esclavitud, surgió el principio fundamental del derecho moderno contemporáneo, el cual reconoció igual dignidad para todo ser humano, otorgándose a los seres humanos el carácter de persona.⁸

Con ello, se pretende mostrar que toda persona posee derechos por el solo hecho de serlo y que éstos deben de ser reconocidos y garantizados por la sociedad, sin ningún tipo de discriminación social, económica, jurídica, política, ideológica, cultural o sexual.⁹

Armonizando estas ideas, podemos establecer como concepto jurídico, que persona es sinónimo de sujeto de derecho y personalidad es una categoría atribuida a un ser humano vivo.

El propio Galindo Garfias¹⁰ nos dice:

La persona es el centro imprescindible alrededor del cual se desenvuelven otros conceptos jurídicos fundamentales, como son la noción y la existencia misma del Derecho objetivo y el Derecho subjetivo, la obligación, el deber jurídico y la concepción de toda relación jurídica. Todos estos conceptos básicos en la dogmática y en la realidad del Derecho, no podrían encontrar una adecuada ubicación en la sistemática jurídica, sino a través del concepto de “persona”. En el lenguaje ordinario, se dice que una persona tiene o no personalidad o que tiene, de acuerdo con su modo de ser, mayor o menor personalidad, sin que esto implique la negación de su categoría de persona.¹¹

En opinión de Fernández Sessarego¹², “la personalidad es tan sólo la manifestación fenoménica de la persona, su exteriorización en el mundo, su peculiar

8 Ferrara, Francisco, *Teoría de las Personas Jurídicas*, Traducción de Eduardo Ovejero y Maury, Madrid, 1929.

9 Pacheco, Máximo G., *Los derechos fundamentales de la persona humana*, Instituto Interamericano de Derechos Humanos, Serie de Estudios de Derechos Humanos, Tomo II, 1999, pág. 67.

¹⁰ Galindo Garfias, Ignacio, *Derecho Civil*, Primer Curso, Parte general, Personas, Familia, Editorial Porrúa, S.A., México, 1991, Décima Edición, pág. 306.

¹¹ Treviño García Ricardo, *La persona y sus atributos*, Universidad Autónoma de Nuevo León Facultad de Derecho y Criminología, 2002, p. 31.

¹² Fernández Sessarego, Carlos, *¿Qué es persona para el derecho?*, *Derecho Privado, Libro en Homenaje a Alberto J. Bueres*, Editorial Hammurabi, Buenos Aires, 2001. p.4.

“manera de ser”. Cada ser humano, en cuanto ser libre, tiene una cierta “personalidad” que lo identifica y, por consiguiente, lo distingue de los demás.¹³

Bajo ese contexto, el maestro Rafael De Pina¹⁴, determina que la personalidad cuenta con diversas atribuciones que permite diferenciar a los individuos, expresando que “Las cualidades o propiedades de un ser constituyen sus atributos. Son aquellos elementos propios y característicos, que encontramos en todas las personas y que tienen ciertas consecuencias jurídicas”.

Por su parte, el Ricardo Treviño García, enuncia que la identidad, cuenta con diversos atributos para su reconocimiento, los cuales actualmente vinculamos con los datos personales de un sujeto, mismos que se enuncian a continuación para su mejor referencia:¹⁵

- a) Nombre;
- b) Domicilio;
- c) Estado;
- d) Patrimonio.

En nuestro sistema jurídico mexicano, derivado de la adición Constitucional publicada en el Diario Oficial de la Federación del 17 de junio de 2014, del artículo 4º, párrafo octavo, representó un parteaguas para reconocerse en México el derecho a la identidad como derecho fundamental para que las personas tuvieran certeza de que el Estado tiene que reconocer y buscar los mecanismos legales para hacerla efectiva.¹⁶

La Constitución Política de los Estados Unidos Mexicanos, en su artículo 4º, párrafo octavo, menciona: “toda persona tiene derecho a la identidad y a ser registrado de manera inmediata a su nacimiento. El Estado garantizará el

¹³ Maritan Grisel Galiano, “REFLEXIONES CONCEPTUALES SOBRE LAS CATEGORÍAS: PERSONA, PERSONALIDAD, CAPACIDAD Y SUJETO DE DERECHO”, *Revista Derecho y Cambio Social*, Depósito legal: 2005-5822, Publicado enero 2013, p. 5.

¹⁴ De Pina, Rafael, *Elementos de Derecho Civil Mexicano, Introducción- Personas- familia*, Vol. Primero, Editorial Porrúa, S. A., México, 1963, Tercera Edición, p. 210.

¹⁵ Treviño García Ricardo, *La persona y sus atributos*, Universidad Autónoma de Nuevo León Facultad de Derecho y Criminología, 2002, p. 45.

¹⁶ Cásares García Leonel, “Noción básica del derecho a la identidad en México”, *Revista Hechos y Derechos*, Instituto de Investigaciones Jurídicas UNAM, Número 27, Publicado el 6 de mayo de 2015.

cumplimiento de estos derechos. La autoridad competente expedirá gratuitamente la primera copia certificada del acta de registro de nacimiento”.¹⁷

Asimismo, mediante la Observación General No. 14, aprobada por el Comité de los Derechos del Niño en 2013¹⁸, determinó que el interés superior de la infancia es un derecho, un principio y una norma de procedimiento, dicha observación fomentó se publicaran dos reformas constitucionales trascendentes para los derechos humanos de niñas, niños y adolescentes: la primera al artículo 4º, que adicionó el principio del interés superior de la niñez, y la segunda al artículo 73, que facultó al Congreso de la Unión para expedir leyes en materia de derechos de niñas, niños y adolescentes.

Derivado de lo anterior, el 4 de diciembre de 2014, fue publicada la Ley General de los Derechos de Niñas, Niños y Adolescentes en México, en la cual, en su artículo 19, señala los elementos del derecho a la identidad, el cual a la letra determina lo siguiente:

Artículo 19. Niñas, niños y adolescentes, en términos de la legislación civil aplicable, desde su nacimiento, tienen derecho a:

- I. Contar con nombre y los apellidos que les correspondan, así como a ser inscritos en el Registro Civil respectivo de forma inmediata y gratuita, y a que se les expida en forma ágil y sin costo la primera copia certificada del acta correspondiente, en los términos de las disposiciones aplicables;
- II. Contar con nacionalidad, de conformidad con lo dispuesto en la Constitución Política de los Estados Unidos Mexicanos y los tratados internacionales;
- III. Conocer su filiación y su origen, en la medida de lo posible y siempre que ello sea acorde con el interés superior de la niñez, y

¹⁷ H. Congreso de la Unión, Cámara de Diputados, Leyes Federales Vigentes, Constitución Política de los Estados Unidos Mexicanos, recuperado de: http://www.diputados.gob.mx/LeyesBiblio/pdf/1_241220.pdf (consultada en noviembre de 2020).

¹⁸ Comité de los Derechos del Niño, Observación General No.14 sobre el derecho del niño a que su interés superior sea una consideración primordial (artículo 3, párrafo 1). CRC/C/GC/14, 29 de mayo de 2013.

IV. Preservar su identidad, incluidos el nombre, la nacionalidad y su pertenencia cultural, así como sus relaciones familiares.¹⁹

Dichos atributos, sí bien son considerados como elementos de la personalidad de un individuo, lo cierto es que constituyen las propiedades y características de la identidad, las cuales resultan propias de las personas físicas, que como se ha mencionado con antelación, son titulares de derechos.

En relatadas condiciones, se puede afirmar que la identidad puede analizarse bajo dos planteamientos, el primero, como una forma de auto identificación del individuo hacia la sociedad y en segundo plano como parte de las atribuciones de la personalidad, como objetivación de la identidad de la persona, la cual se construye a través de procesos sociales.²⁰

En consecuencia, es claro que la identidad reconocida como parte de la personalidad de un individuo constituye un derecho fundamental reconocido para todo ser humano, el cual resulta necesario para el ejercicio de otros derechos fundamentales, por lo que desde el momento del nacimiento, se reconoce el derecho que tiene toda persona de contar con una identidad, lo anterior, toda vez que se comprende como una prueba de la existencia de esa persona como individuo, así como la diferenciación con los demás sujetos y otorgándose su personalidad para el ejercicio de sus derechos.

Al respecto, cabe traer a colación que más de 1.500 millones de personas en el mundo en desarrollo carecen de cualquier forma de identificación oficialmente reconocida, ya sea en papel o en formato electrónico.²¹

La Organización Mundial de la Salud, reportó en mayo de 2014, que, a nivel mundial, dos tercios (38 millones) de los 56 millones de defunciones anuales no se

¹⁹ H. Congreso de la Unión, Leyes Federales Vigentes, Ley General de los Derechos de Niñas, Niños y Adolescentes, recuperado de: <http://www.ordenjuridico.gob.mx/Documentos/Federal/pdf/wo99957.pdf> (consultada en noviembre de 2020).

²⁰ Aymerich Ignacio, *Identidad individual y personalidad jurídica*, Facultad de Derecho Depto. de Filosofía del Derecho Universidad de Castellón, 12080 Castellón España, 2008, p. 395.

²¹ World Bank, *Identification for Development Strategic Framework*, Working Paper, Washington D.C., 2016.

registran y cerca de la mitad de los nacimientos que se producen en todo el mundo quedan sin registrar.²²

Esta brecha de control de registro, genera grandes problemas entorno al reconocimiento de la identidad, representando un obstáculo para la participación de las personas en la vida política, económica y social, ya que no cuentan con una forma segura de afirmar y verificar su identidad, por lo que es posible que una persona no pueda abrir una cuenta bancaria, votar en una elección, acceder a la educación o la atención médica, recibir un pago de pensión o presentar peticiones oficiales en Corte.²³ Además, los sistemas de identificación deficientes significan que los estados tendrán dificultades para recaudar impuestos, hacerlos partícipes en programas sociales y garantizar la seguridad.

1.2. Conceptos básicos sobre la identidad

1.2.1. ¿Qué es identidad?

Como se ha mencionado en párrafos precedentes, la identidad, ha sido reconocida como un derecho fundamental, personalísimo, autónomo y distintivo de las personas; es el reconocimiento del ser de cada persona elevada por el derecho a la categoría del bien jurídico protegido, por considerarla digna de tutela jurídica.

En tal sentido, es el derecho que tiene todo ser humano, sin distinción de raza, color, sexo, idioma, religión, opinión política o de cualquier otra índole, origen nacional o social, posición económica, nacimiento o cualquier otra condición, a ser inscrito inmediatamente después de su nacimiento en un registro mediante el cual se establecerá su nombre, nacionalidad, filiación y pertenencia a un grupo cultural.²⁴

Al momento de abordar el estudio de la identidad, se pueden encontrar estudios bajo dos perspectivas: desde lo individual y desde lo social. Es decir, se puede estudiar la identidad desde explicaciones que emanan causalmente desde el

²² Organización Mundial de la Salud, *Registro civil: por qué es importante contabilizar los nacimientos y las defunciones*, Centro de Prensa, notas descriptivas, OMS, 30 de mayo de 2014.

²³ Gelb, A., J. Clark, *Identification for Development: The Biometrics Revolution*. Center for Global Development Working Paper, no. 315, 2013.

²⁴ Jiménez García, Hilda Adriana A., López Velarde Campa, Jesús Armando Coordinador, *El derecho a la identidad como base para el ejercicio de los derechos humanos de niñas, niños y adolescentes en situación de calle en la Ciudad de México*, Instituto de Investigaciones Jurídicas UNAM, Primera edición, México, 2017, p. 121.

"individuo" como organismo que es y se siente diferente al resto, o desde lo social, que sería como ese individuo se relaciona con el entorno y quiere identificarse o diferenciarse de su grupo social, es decir, como experimenta el individuo ese "yo soy" con relación al grupo o al "nosotros".²⁵

En consecuencia, dicho registro reconoce la pertenencia de una persona a un Estado, una sociedad y una familia, generando vínculos jurídicos, políticos, sociales, económicos y culturales que implican su "incorporación como sujeto de derecho dentro de un Estado y su acceso a un conjunto de derechos humanos reconocidos internacionalmente".²⁶

Bajo ese contexto, el artículo 18 de la Convención Americana sobre Derechos Humanos²⁷, 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."

En consecuencia, podemos afirmar que, al contar con un nombre, apellido y demás datos personales, como domicilio, ocupación, entre otros, se puede otorgar la identidad a un ser humano, a fin de hacerlo identificable de los demás. Es por ello, que la Real Academia Española, define a la identidad como al "conjunto de rasgos propios de un individuo o de una colectividad que los caracterizan frente a los demás."²⁸

Sin embargo, el tratar de definir el concepto de identidad resulta más complejo de lo que la misma ley considera, el diccionario jurídico mexicano de la Universidad Nacional Autónoma de México, la define como el "conjunto de los datos

²⁵ Fernández Elisa, "Identity and personality: or as we know we are different from others", *Revista Digital de Medicina Psicosomática y Psicoterapia*, Sociedad Española de Medicina Psicosomática y Psicoterapia, 2011.

²⁶ Jiménez García, Hilda Adriana A., López Velarde Campa, Jesús Armando Coordinador. *El derecho a la identidad como base para el ejercicio de los derechos humanos de niñas, niños y adolescentes en situación de calle en la Ciudad de México*, Instituto de Investigaciones Jurídicas UNAM, Primera edición, México, 2017, p. 121.

²⁷ *Convención Americana de Derechos Humanos*, recuperado de: <http://ordenjuridico.gob.mx/TratInt/Derechos%20Humanos/D1BIS.pdf>, (consultado el de febrero de 2020).

²⁸ *Diccionario de la lengua española*, 23 ed., [versión 23.3 en línea]. Disponible en: <https://dle.rae.es> (consultado el de febrero de 2020).

en virtud de los cuales se establece que una persona es verdaderamente la que se dice o la que se presume que es”²⁹.

Por su parte, el Fondo de las Naciones Unidas para la Infancia (UNICEF) establece que la identidad consiste en el “...reconocimiento jurídico y social de una persona como sujeto de derechos y responsabilidades y a su vez, de su pertenencia a un Estado, un territorio, una sociedad y una familia, condición necesaria para preservar la dignidad individual y colectiva de las personas.”³⁰

Asimismo, la Comisión Nacional de los Derechos Humanos (CNDH), considera que la identidad se adquiere durante el proceso de desarrollo vital de la persona, a través de su información genética, la interacción familiar, la historia personal y el medio cultural en que se desenvuelve; integrando un conjunto de atributos inherentes a ella que la hacen única e irrepetible.³¹

Aunado a lo anterior, la misma CNDH, considera que la identidad permite a las personas:³²

- a) Saber quiénes son y distinguirse de los demás.
- b) Tener una nacionalidad que los vincula con un Estado determinado y gozar de todos los derechos que éste les reconoce.
- c) Acceder a servicios y prestaciones que contribuyen a la satisfacción de otros derechos como a la salud, a la educación, a programas sociales, entre otros.

En consecuencia, de forma general podemos decir que la identidad, es reconocida como un derecho humano que se compone por las características y datos personales que definen a una persona que nos ayuda a identificarla y diferenciarla de los demás, siendo un elemento primigenio de la personalidad que otorga el acceso a otros derechos esenciales como salud, educación, protección,

²⁹ *Diccionario jurídico mexicano: tomo I, A-B México*, Universidad Nacional Autónoma de México, Instituto de Investigaciones Jurídicas, 1982. p.p.14-15.

³⁰ UNICEF, *Registro de Nacimiento en América Latina y el Caribe, Panorama regional*, Oficina Regional de UNICEF para América Latina y el Caribe, Boletín No. 1, 15 de julio de 2011, recuperado de: [http://www.unicef.org/lac/UNICEF_TACRO_boletin_registro_de_nacimiento_06152011\(3\).pdf](http://www.unicef.org/lac/UNICEF_TACRO_boletin_registro_de_nacimiento_06152011(3).pdf) (consultado en noviembre de 2020)

³¹ Comisión Nacional de los Derechos Humanos, *Niñas, niños y adolescentes tienen derecho a la identidad*, CNDH, Coordinación del Programa sobre Asuntos de la Niñez y la Familia, México, 2018.

³² *Idem*.

nacionalidad, ciudadanía e inclusión en la vida económica, social, cultural y política en un país para cualquier persona.

1.2.2. Derecho a la identidad

Una vez que hemos comprendido el concepto de identidad, es importante denotar que éste constituye un derecho, denominado derecho a la identidad y como se ha mencionado, este es reconocido como un derecho humano a través de diversos instrumentos internacionales.

No obstante, en nuestro país fue hasta hace pocos años, que el concepto de identidad se plasmó como derecho humano reconocido en nuestra Constitución Política, estableciéndose desde entonces con claridad, que toda persona tiene derecho a la identidad y a ser registrado gratuitamente de manera inmediata a su nacimiento y señala la obligación del estado mexicano de garantizar el cumplimiento de estos derechos.³³

El derecho al nombre propio, a la personalidad jurídica, a la nacionalidad y por ende a la identidad, constituye el derecho primigenio que se convierte de manera automática en la llave de acceso a otros derechos esenciales para cualquier persona.³⁴

El derecho a la identidad como todo derecho humano, es:

- Inherente: Adquirido solo por el hecho de ser seres humanos.
- Universal: Reconocido internacionalmente.
- Inalienable: No pueden transmitirse por medio de ningún acto ni negocio jurídico.
- Imprescriptible: no se adquieren ni se pierden por el mero transcurso del tiempo.
- Irrenunciable: No se pueden renunciar a ellos, ni la autoridad puede establecer sanción alguna en contra de ellos.

³³ Registro Nacional de Población, Acciones y Programas, *Derecho a la identidad, la puerta de acceso a tus derechos*, Agosto, 2019. Recuperado de: <https://www.gob.mx/segob/renapo/acciones-y-programas/derecho-a-la-identidad-la-puerta-de-acceso-a-tus-derechos> (consultado en septiembre de 2020)

³⁴ *Idem*.

El hablar sobre el derecho a la identidad, su importancia y relevancia radica en su establecimiento en diversos instrumentos internacionales como un derecho fundamental para ser reconocido ante la sociedad, como, por ejemplo:

- Declaración Universal de los Derechos Humanos de 1948.³⁵
- Convención sobre los Derechos del Niño de 1989, que en su artículo 7º establece el derecho al nombre, a la nacionalidad y a la filiación.³⁶
- Convención Internacional sobre la eliminación de todas las formas de discriminación racial de 1965.³⁷
- Pacto Internacional de Derechos Civiles y Políticos de 1966.³⁸
- Convención sobre la eliminación de todas las formas de discriminación contra la Mujer de 1979.³⁹
- Declaración Americana de los Derechos y Deberes del Hombre de 1948.⁴⁰
- Convención Americana sobre Derechos Humanos de 1969⁴¹, entre otros.

En nuestro país el derecho a la identidad, conforme al Programa Nacional de Derechos Humanos 2020-2024, busca establecer dos pilares fundamentales para su ejercicio, la identidad jurídica y la identidad biométrica, ligadas a través del identificador único que es la Clave Única de Registro de Población, mejor conocido

³⁵ Declaración Universal de los Derechos Humanos, aprobada y proclamada por la Asamblea General de las Naciones Unidas en su Resolución 217 A (III) del 10 de diciembre de 1948, artículo 15.

³⁶ Convención sobre los Derechos del Niño, adoptada y abierta a la firma y ratificación por la Asamblea General de las Naciones Unidas en su Resolución 44/25 del 20 de noviembre de 1989; entrada en vigor el 2 de septiembre de 1990, artículo 7º.

³⁷ Convención Internacional sobre la Eliminación de Todas las Formas de Discriminación Racial, adoptada y abierta a la firma y ratificación por la Asamblea General de las Naciones Unidas en su Resolución 2106 A (XX) del 21 de diciembre de 1965; entrada en vigor el 4 de enero de 1969, artículo 5º.

³⁸ Pacto Internacional de Derechos Civiles y Políticos, adoptado y abierto a la firma, ratificación y adhesión por la Asamblea General de las Naciones Unidas en su Resolución 2200 A (XXI) del 16 de diciembre de 1966; entrada en vigor el 23 de marzo de 1976, artículo 24

³⁹ Convención sobre la Eliminación de Todas las Formas de Discriminación contra la Mujer, adoptada y abierta a la firma y ratificación, o adhesión, por la Asamblea General de las Naciones Unidas en su Resolución 34/180 del 18 de diciembre de 1979; entrada en vigor el 3 de septiembre de 1981, artículo 9º.

⁴⁰ Declaración Americana de los Derechos y Deberes del Hombre, aprobada en la Novena Conferencia Internacional Americana, Bogotá, 1948, artículo 19.

⁴¹ Convención Americana sobre Derechos Humanos, aprobada y suscrita en la Conferencia Especializada Interamericana sobre Derechos Humanos, San José de Costa Rica, 22 de noviembre de 1969; entrada en vigor el 18 de julio de 1978, artículos 18. Derecho al nombre, y 20. Derecho a la nacionalidad.

como CURP, y así garantizar su unicidad, proponiendo la integración del Registro Nacional de Población conformado por información de identidad jurídica y biométrica, a fin de garantizar el derecho a la identidad de todas las personas y expedir un documento único digital de identificación nacional “biometrizado”, en coordinación con los tres órdenes de gobierno, protegiendo los datos personales.⁴²

En México, al menos 1 millón de personas de todas las edades no cuentan con registro de nacimiento. De ellas, más de 600 mil son niñas, niños o adolescentes.⁴³

- El 22.7% de este total es población indígena.
- 6 de cada 10 son niñas, niños y adolescentes.

A pesar de los esfuerzos gubernamentales, que se traducen en alentadores avances de cobertura de registro de nacimiento general de alrededor del 97% a nivel nacional, aún quedan importantes brechas por cerrar: en municipios de perfil rural, en la población indígena y en la que vive en condiciones de alta marginación social⁴⁴, asimismo, a la fecha, México no cuenta con una base de datos que vincule la identidad jurídica y biométrica de toda la población, lo que impide brindar un servicio de identidad y de identificación como lo demanda nuestra sociedad y lo mandata la Constitución, lo cual facilita el robo de identidad, el fraude y la inseguridad.⁴⁵

Aunado a lo anterior, independientemente del registro civil, existen diversos esfuerzos institucionales, por medio de los cuales se ha tratado de fomentar un control e inscripción de los ciudadanos a fin de reconocer su identidad, tal es el caso del Instituto Nacional Electoral (INE), quién a través de la creación del padrón electoral, como autoridad máxima en la materia, lleva a cabo el registro de las y los

⁴² Programa Nacional de Derechos Humanos 2020-2024, publicado en el Diario Oficial de la Federación el 10 de diciembre de 2020. Recuperado de: http://dof.gob.mx/nota_detalle.php?codigo=5607366&fecha=10/12/2020 (consultado en febrero 2021)

⁴³ UNICEF, *Derecho a la identidad. La cobertura del registro de nacimiento en México*, Enero, 2019. Recuperado de: https://www.unicef.org/mexico/media/1016/file/UNICEF_Derecho%20a%20la%20identidad.pdf (consultado en noviembre de 2020)

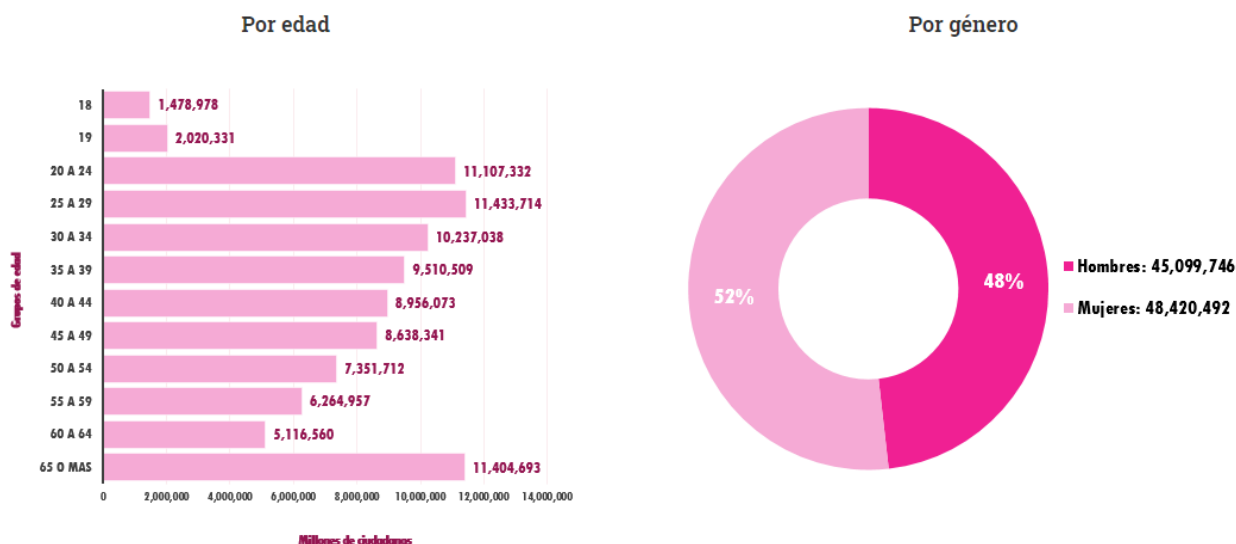
⁴⁴ *Idem.*

⁴⁵ Registro Nacional de Población, Acciones y Programas, “Derecho a la identidad, la puerta de acceso a tus derechos”, Agosto, 2019.

ciudadanos mexicanos que solicitaron su inscripción al mismo, con la finalidad de obtener su Credencial para Votar con fotografía y así ejercer su derecho al voto.

Actualmente⁴⁶, el padrón electoral está integrado por 93 millones 520 mil 238 de registros de los cuales 48.4 millones de mujeres y 45.0 millones de hombres.

93,520,238 Ciudadanos Registrados con Corte al 15 de enero de 2021.



Cuadro 1. Padrón Electoral (con corte al 15 de enero de 2021).⁴⁷

La base de datos del padrón electoral del INE contiene datos personales de los ciudadanos, como: nombre completo, domicilio, fecha de nacimiento, género, fotografía, firma, CURP, clave de elector y las 10 huellas dactilares de las y los ciudadanos.⁴⁸

Adicionalmente, desde el año 2001 el INE solicita a las y los ciudadanos sus datos biométricos; es decir, las huellas dactilares y los rasgos faciales, con el objetivo de evitar duplicidad en los registros y depurar la base de datos que contiene la información de la ciudadanía. La totalidad de los registros en la base de datos tienen biometría facial, lo cual ha generado que el Instituto, haya implementado

⁴⁶ Estadística elaborada con corte al 15 de enero de 2021.

⁴⁷ INE, *ESTADÍSTICAS LISTA NOMINAL Y PADRÓN ELECTORAL*, disponible en: <https://www.ine.mx/credencial/estadisticas-lista-nominal-padrón-electoral/> (consultado en enero de 2021)

⁴⁸ INE, *Tarjeta Informativa: Sobre el Padrón Electoral y los Datos Biométricos*, Central Electoral, publicado el 24 de enero de 2020. Recuperado de: <https://centralelectoral.ine.mx/2020/01/24/tarjeta-informativa-padrón-electoral-los-datos-biometricos/> (consultado en de enero de 2021)

medidas adicionales a las que establece la legislación para salvaguardar los datos personales de las cerca de 90 millones de personas que integran el padrón electoral.⁴⁹

Lo anterior, resulta de vital importancia, toda vez que, para el ejercicio del derecho de identidad de los ciudadanos mexicanos, en la actualidad prácticamente todos los trámites oficiales, ante instituciones públicas, financieras o privadas, se realizan con apoyo de la credencial para votar y mediante una confronta remota con la base de datos del padrón electoral⁵⁰, como medio de identificación oficial.

Tan es así, que desde el mes de enero de 2019 en algunos bancos del país se utiliza un detector de huella para verificar la identidad de los usuarios, de manera que se impida el robo de identidad. Esto sucede gracias a la colaboración entre el Instituto Nacional Electoral (INE) y la Comisión Nacional Bancaria y de Valores (CNBV), a partir del cual, sin vulnerar la base de datos ni la información personal de la ciudadanía, las instituciones bancarias pueden verificar la información con el Padrón Nacional de Electores.⁵¹

Dicho mecanismo permite ejercer y proteger debidamente la identidad de los ciudadanos, coadyuvando a la verificación de los datos personales, en particular, aquellos de carácter biométrico, que permite un ejercicio de identificación confiable y seguro, tanto para los ciudadanos como para las instituciones de orden público y privado.

Actualmente, hacen uso del servicio de verificación un total de 43 instituciones: 2 partidos políticos, 5 AFORE, 15 Bancos, el Colegio de Notarios de Jalisco, la Secretaría de Economía, el Gobierno de la Ciudad de México, Policía Federal, Nacional Financiera, Servicio de Administración Tributaria, BANCOMEXT, CONACYT, el INFONAVIT, el IMSS, AT&T México, TELCEL y 9 instituciones de crédito o financieras.⁵²

⁴⁹ *Idem*

⁵⁰ *Idem*

⁵¹ INE, *INE colabora con instituciones bancarias para prevenir robo de identidad y fraudes a partir de la identificación de huellas dactilares*, Central Electoral, publicado el 17 de febrero de 2019. Disponible en: <https://centralectoral.ine.mx/2019/02/17/ine-colabora-instituciones-bancarias-prevenir-robo-identidad-los-fraudes-partir-la-identificacion-huellas-dactilares/> (consultado en enero de 2021)

⁵² *Idem*

1.2.3. ¿Qué es la identidad legal?

La identidad legal se define como las características básicas de la identidad de un individuo. por ejemplo, nombre, sexo, lugar y fecha de nacimiento conferida a través del registro y la emisión de un certificado por un civil autorizado por una autoridad de registro después del nacimiento, en la mayoría de los casos corresponde a una autoridad gubernamental. En ausencia de registro de nacimiento, la identidad legal puede ser conferida por una autoridad de identificación legalmente reconocida; este sistema debe estar vinculado al sistema de registro civil para garantizar un enfoque de la identidad jurídica desde el nacimiento hasta la muerte.⁵³

La identidad legal se materializa cuando un Estado reconoce mediante la expedición de un documento oficial, la identidad de un ser humano, ya sea a través del registro civil, al momento de registrar a un recién nacido, al expedir el documento oficial que reconoce a una persona como ciudadano al haber cumplido la mayoría de edad, lo cual, por ejemplo, en nuestro país permite el ejercicio del derecho a votar o con la emisión de un pasaporte, a efecto de estar en posibilidad de acreditar nuestra identidad en el extranjero.

La identidad legal, permite el reconocimiento válido y verificable, que fomenta la inclusión y permite un mejor acceso a una variedad de servicios. Cuando los ciudadanos se pueden identificar, se generan datos confiables continuamente para ayudar a los gobiernos a implementar políticas y a medir el progreso del desarrollo.⁵⁴

Aunado a lo anterior, conforme a la materia civil, es importante denotar que la identidad legal se extingue mediante la emisión de un certificado de defunción por parte de la autoridad de registro civil al registrarse el deceso, lo cual, de igual manera, coadyuva en control y registro de la identidad de los ciudadanos.⁵⁵

⁵³ Grupo de Expertos en Identidad Legal de las Naciones Unidas (LIEG) y Definición Operacional de Legalidad del Banco Mundial. *Identidad*, Recuperado de: <https://www.unhcr.org/en-us/1951-refugeeconvention.html> (consultado en septiembre de 2020)

⁵⁴ Tamargo María del Carmen, *Identidad legal, ciudadanía y vulnerabilidad social. Notas para el estudio del subregistro de nacimientos y la indocumentación con perspectiva de género y etnicidad, XXVII Congreso de la Asociación Latinoamericana de Sociología. VIII Jornadas de Sociología de la Universidad de Buenos Aires*. Asociación Latinoamericana de Sociología, Buenos Aires, 2009.

⁵⁵ Véase: Código Civil Federal. Artículo 22.- La capacidad jurídica de las personas físicas se adquiere por el nacimiento y se pierde por la muerte; pero desde el momento en que un individuo es concebido, entra bajo la protección de la ley y se le tiene por nacido para los efectos declarados en el presente Código.

1.2.4. ¿Qué es un dato personal?

Conforme hasta lo aquí analizado, resulta claro que, para el reconocimiento de una identidad, ésta se encuentra necesaria e íntimamente ligada con los datos personales del titular, es decir, ese conjunto de datos personales, nos permitirán conformar y construir esa identidad para su debido reconocimiento.

Al respecto, el Convenio 108 del Consejo de Europa, de 28 de enero de 1981, para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, señala en su artículo 2 inciso a), lo siguiente: a) «*Datos de carácter personal*» significa cualquier información relativa a una persona física identificada o identificable («*persona concernida*»).

A fin de contar, con una definición común del concepto de datos personales mediante el DICTAMEN 4/2007 sobre el concepto de datos personales, aprobado el 20 de junio de 2007⁵⁶, por el Grupo de Trabajo del artículo 29 de la Unión Europea⁵⁷, se estableció un acuerdo sobre el concepto de datos personales, los casos en que debe aplicarse la legislación nacional sobre protección de datos y la manera en que ésta debe aplicarse.

El análisis se basa en cuatro componentes principales que pueden distinguirse en la definición de datos personales, esto es: toda información, sobre, identificada o identificable y persona física, los cuales están estrechamente ligados y se complementan entre sí, pero juntos determinan si una determinada información debe ser considerada como datos personales.

1. “*toda información*”. Sugiere una interpretación del concepto, independientemente de la naturaleza o del contenido de la información y del soporte técnico en el que se presente. Esto significa que tanto la información objetiva como la subjetiva sobre una persona, cualquiera que sea su amplitud, y con independencia del soporte técnico que la contenga, puede considerarse

⁵⁶ Dictamen 4/2007 sobre el concepto de datos personales, Grupo de Trabajo del artículo 29 de la Unión Europea, 01248/07/ES WP 136, Adoptado el 20 de junio de 2007.

⁵⁷ El Grupo de Trabajo del artículo 29 (GT Art. 29) es el grupo de trabajo europeo independiente que se ha ocupado de cuestiones relacionadas con la protección de la privacidad y los datos personales hasta el 25 de mayo de 2018 (entrada en aplicación del Reglamento General de Protección de Datos). Véase: https://edpb.europa.eu/our-work-tools/article-29-working-party_es (consultado en diciembre de 2020)

como datos personales. El dictamen también analiza la cuestión de los datos biométricos y su distinción jurídica con respecto a las muestras humanas de las que pueden extraerse.

2. “*sobre*”. No ha suscitado hasta ahora mucho interés, pero es crucial en la determinación del alcance sustantivo del concepto, especialmente en relación con objetos y nuevas tecnologías. El dictamen proporciona tres elementos alternativos - contenido, finalidad o resultado - para determinar si la información versa sobre una persona física. Este componente abarca asimismo la información que puede tener claras repercusiones sobre la manera en que se trata o se valora a una persona.
3. “*identificada o identificable*”. Se centra en las condiciones que deben darse para poder considerar a una persona como identificable, y especialmente en los medios que puedan ser razonablemente utilizado por el responsable del tratamiento o por cualquier otra persona para identificar a dicha persona. El contexto y las circunstancias particulares de cada caso concreto tienen un papel importante en este análisis. El dictamen también trata la seudonimización y el uso de datos cifrados en la investigación estadística y farmacéutica.
4. “*persona física*”. Se centra en el requisito de que los datos personales se refieran a humanos. El dictamen también analiza las conexiones con los datos sobre las personas fallecidas, el *nasciturus* y las personas jurídicas.⁵⁸

Dentro de nuestro sistema legal mexicano, los artículos 3, fracción IX de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados⁵⁹ y 3, fracción V de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares⁶⁰, respectivamente, establecen que se entenderá por dato personal, cualquier información concerniente a una persona física identificada

⁵⁸ Cfr. Dictamen 4/2007 sobre el concepto de datos personales, Grupo de Trabajo del Artículo 29, 01248/07/ES WP 136, Adoptado el 20 de junio 2007.

⁵⁹ Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, publicada en el Diario Oficial de la Federación el 26 de enero de 2017. Disponible en: https://www.dof.gob.mx/nota_detalle.php?codigo=5469949&fecha=26/01/2017 (consultado en septiembre de 2020)

⁶⁰ Ley Federal de Protección de Datos Personales en Posesión de los Particulares, publicada en el Diario Oficial de la Federación el 5 de julio de 2010. Disponible en: <http://www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf> (consultado en septiembre de 2020)

o identificable. Se considera que una persona es identificable cuando su identidad pueda determinarse directa o indirectamente a través de cualquier información.

Asimismo, cabe señalar que dichos datos otorgan al titular, identidad y lo describen, ayudando a conocer entre otros aspectos nombre, su origen, edad, lugar de nacimiento o residencia, datos de localización como domicilio, número telefónico o correo electrónico, trayectoria académica, laboral o profesional, entre otros.

Por su parte, el DICTAMEN 4/2007 sobre el concepto de datos personales, aprobado el 20 de junio de 2007⁶¹, por el Grupo de Trabajo del artículo 29 de la Unión Europea, se refiere a los datos personales sensibles, como aquellos “datos que por su naturaleza puedan atentar contra las libertades fundamentales o la intimidad”.

De conformidad con los artículos 3, fracción X de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados y 3, fracción VI Ley Federal de Protección de Datos Personales en Posesión de los Particulares, de forma general indican que los datos personales sensibles, son aquellos datos personales que afectan a la esfera más íntima de su titular, como es el caso de aquellos que puedan revelar aspectos como de su origen racial o étnico, estado de salud, sus características físicas, ideología, religión, opinión política, preferencia sexual, entre otros.

Al respecto, los datos personales con el carácter de sensibles requieren de un mayor grado o nivel de protección para garantizar la privacidad de los ciudadanos, ya que como lo señalada el artículo mencionado con antelación, su utilización indebida puede dar origen a discriminación o incluso conllevaría a poner el riesgo al titular de dichos datos.

De formar particular, el Reglamento General de Protección de Datos Personales (RGPD) de la Unión Europea, mejor conocido por sus siglas en inglés como GDPR, establece categorías especiales de datos personales, para aquellos que necesitan mayor protección, por su naturaleza y son particularmente sensibles en relación con los derechos y las libertades fundamentales, ya que el contexto de

⁶¹ Dictamen 4/2007 sobre el concepto de datos personales, Grupo de Trabajo del artículo 29 de la Unión Europea, 01248/07/ES WP 136, Adoptado el 20 de junio de 2007.

su tratamiento podría entrañar importantes riesgos para los derechos y las libertades fundamentales.⁶²

1.2.5. ¿Qué es privacidad?

El derecho de la vida privada, surge a partir de la ideología de Samuel Warren y Louis Brandeis en los Estados Unidos en 1890, dentro de su estudio denominado "*The Right to Privacy*", en el definen la idea de que cada individuo debe tener una protección completa de su persona y de su propiedad como un principio del derecho común, fijando la necesidad de demarcar un principio que pudiera ser invocado para proteger la vida privada del individuo frente a su invasión por modernos mecanismos de interceptación o grabación que amenazaran con la difusión indiscriminada de información privada⁶³.

La preocupación de los autores estadounidenses a finales del siglo XIX, al igual que en la actualidad, era generar la necesidad de protección a la esfera privada de las personas, ante el surgimiento de las nuevas tecnologías, aunque en ese momento se trata únicamente de imágenes que eran difundidas a través de medios impresos, lo cierto, es que existía una invasión a la intimidad, sin regulación, ni límite alguno.

La privacidad, generalmente es vinculada como "el derecho a ser dejado sólo", sin embargo, dicha dimensión es limitativa, tomando en consideración que Warren y Brandeis, hacen referencia a un libre desarrollo de la personalidad en aspectos tangibles e intangibles, dando al concepto privacidad, una nueva dimensión de derechos asociados a la evolución social, en el ámbito anglosajón, la privacidad es vista bajo su propia estructura, equipara vida privada, intimidad, libre desarrollo de personalidad y sexual.

Al respecto, Alan Westin⁶⁴, amplió la concepción de la privacidad, incluyendo la facultad que todo individuo tiene para terminar, cómo, cuándo y hasta qué punto

⁶² Artículo 4, apartados 13, 14 y 15, y artículo 9, y considerandos 51-56 del Reglamento General de Protección de Datos Personales.

⁶³ Magallanes Martínez Víctor Hugo Hiram, *Derecho a la protección de datos personales. su diseño constitucional, the right of personal data protection and its constitutional design*, Instituto de Investigaciones Jurídicas-UNAM, 2016.

⁶⁴ Westin, Alan, "*Privacy and Freedom*", Nueva York, Ateneum, 1967, p. 7.

su información personal puede ser comunicada a los demás, estructurándose así al derecho de la privacidad bajo dos componentes:

- i. Respetar la *libertad individual* de la persona, incluyendo el llamado “derecho a aislarse”, y, por otro lado,
- ii. *Autodeterminación informativa*⁶⁵, reconocido como el derecho de controlar la información relativa a uno mismo.

Por su parte la Declaración Universal de los Derechos Humanos contempla a la privacidad, en su artículo 12, tal y como se transcribe a continuación:

“Artículo 12

Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación.

Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques.”

Conforme al artículo analizado con antelación, en sentido amplio, se reconoce el derecho a mantener la privacidad del individuo fuera del alcance de otras personas, asegurándose la confidencialidad de sus cosas privadas.

Dentro de nuestro sistema jurídico mexicano, el derecho a la privacidad no se encuentra expresamente reconocido como tal, sin embargo, la Suprema Corte de Justicia de la Nación (en adelante SCJN), al resolver el Amparo en Revisión 134/2008, respecto al derecho de la privacidad, señaló lo siguiente:

“...un reconocimiento del derecho a la persona que tiene su idea originaria en el respeto a la vida privada, siendo una de las libertades tradicionales protegidas por la Constitución Política de los Estados Unidos Mexicanos la inviolabilidad del domicilio, que tiene como finalidad principal el respeto a un ámbito de vida privada personal y familiar que, por regla general, debe quedar excluido del conocimiento

⁶⁵ El derecho a la autodeterminación informativa se traduce en el poder de disposición y control que faculta a su titular a decidir cuáles de sus datos proporciona a un tercero. Véase: Exposición de motivos de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, Consideración Primera.

ajeno y de las intromisiones de las demás, con la limitante que la propia Ley Fundamental establece para las autoridades.”⁶⁶

Es importante denotar que con dicho criterio la Corte, determina que el derecho de la privacidad contempla a todas aquellas intromisiones o molestias que por cualquier medio puedan realizarse en el ámbito de la vida privada de las personas, sin acotarse únicamente al espacio físico como el domicilio, en donde normalmente se desenvuelve la intimidad, sino al entorno en dónde se desenvuelve el individuo.⁶⁷

Asimismo, el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, a través del Diccionario de Protección de Datos Personales⁶⁸ define a la privacidad como:

“La privacidad se puede entender como el ámbito de la vida privada que se tiene derecho a proteger de cualquier intromisión.

Por su parte, el derecho a la privacidad es el derecho de las personas para separar aspectos de su vida privada del escrutinio público, es decir, el derecho de las personas para desarrollar en un espacio reservado ciertos aspectos de la vida personal.

Este derecho tiene dos componentes esenciales: el derecho de aislarse y el derecho de controlar la información de carácter personal.”⁶⁹

En conclusión, podemos conceptualizar a la privacidad como aquello que una persona lleva a cabo en un ámbito reservado, tomando en cuenta que la privacidad, no se refiere a todos los campos de la actividad privada, libres de interferencia, sino estrictamente a los asuntos más íntimos y personales.

⁶⁶ Tesis 2a. LXIII/2008. Amparo en Revisión 134/2008. Primera Sala de la Suprema Corte de Justicia de la Nación. Sentencia del treinta de abril de dos mil ocho. México, p.p. 22 y 23.

⁶⁷ *Idem*. Este juicio de amparo dio origen a la tesis 2a. LXIII/2008, "DERECHO A LA PRIVACIDAD O INTIMIDAD. ESTÁ PROTEGIDO POR EL ARTÍCULO 16, PRIMER PÁRRAFO, DE LA CONSTITUCIÓN POLÍTICA DE LOS ESTADOS UNIDOS MEXICANOS". Semanario Judicial de la Federación y su Gaceta, Novena Época, México, t. XXVII, mayo de 2008, página 229. Reg. IUS. 169700.

⁶⁸ *Diccionario de Protección de Datos Personales. Conceptos Fundamentales*, Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI), Primera edición, noviembre de 2019.

⁶⁹ *Ibidem*. p.p. 672.

En consecuencia, dicha potestad otorga a los ciudadanos el derecho a mantener su privacidad fuera del alcance de otras personas, asegurándose la confidencialidad de sus cosas privadas, lo anterior, toda vez como se analizó con antelación, la privacidad se asocia como "el derecho a ser dejado sólo", así como el libre desarrollo de la personalidad.⁷⁰

⁷⁰ Escalante Gonzalbo, Fernando. *El Derecho a la Privacidad*, Cuadernos de Transparencia número 2. México: IFAI. 2008.



Capítulo 2.
**Internet, sociedad y su impacto en
el Derecho**

Capítulo 2. Internet, sociedad y su impacto en el Derecho

Sin duda, la transformación tecnológica y digital han provocado cambios en la sociedad desde las formas de trabajo, las maneras de interacción y comunicación. Al mismo tiempo el Internet ha facilitado cada vez más el acceso a la información en un entorno global reduciendo los límites, el espacio y tiempo a gran velocidad, con el propósito de facilitar las necesidades de la sociedad de nuestro tiempo.⁷¹

En ese contexto, ante los evidentes cambios significativos que han propiciado las tecnologías de la información y comunicación, surgió la llamada “Sociedad de la Información”, la cual fue reconocida a través de la Cumbre Mundial sobre la Sociedad de la Información (CMSI), que se celebró en dos fases, a saber, en Ginebra 2003 y Túnez 2005, aprobándose los documentos de resultados de la CMSI, en los que se estableció un sólido compromiso de *“construir una sociedad de la información centrada en la persona, abierta a todos y orientada al desarrollo, en la que todas las personas puedan crear, consultar, utilizar y compartir información y el conocimiento, para que las personas, las comunidades y los pueblos puedan emplear plenamente sus posibilidades en la promoción de su desarrollo sostenible y en la mejora de su calidad de vida, sobre la base de los propósitos y principios de la Carta de las Naciones Unidas y respetando plenamente y defendiendo la Declaración Universal de Derechos Humanos.”*⁷²

Bajo esa premisa, es claro que el Internet como fenómeno protagonista de esta nueva evolución y transformación digital, trae consigo grandes ventajas y posibilidades en materia de comunicación e intercambio de información, sin embargo, lo cierto, es que ha generado una gran brecha entre diversos problemas y riesgos jurídicos en su uso, implicación y desconocimiento del uso de las nuevas tecnologías.

⁷¹ Garduño Vera Roberto, “La sociedad de la información en México frente al uso de internet”, *Revista Digital Universitaria*, UNAM, 10 de septiembre 2004, Volumen 5 Número 8, p. p. 3-4.

⁷² Cumbre Mundial sobre la Sociedad de la Información (CMSI). Ginebra 2003 y Túnez 2005. Recuperado de: <http://www.itu.int/net/wsis/basic/index-es.html> (consultado en febrero de 2021)

2.1. Internet descripción y nociones básicas

De manera muy breve, podemos determinar que Internet⁷³ es una red de ordenadores que se comunican entre sí utilizando el protocolo de control de transporte/protocolo de Internet (TCP/IP). Se trata de una red internacional de ordenadores interconectados que permite a millones de personas comunicarse unas con otras en el "ciberespacio" y acceder a inmensas cantidades de información procedente de todo el mundo.⁷⁴

El predecesor histórico de Internet fue la red militar ARPA net (1969). La idea básica era construir una red estadounidense digitalizada que permitiese a los ordenadores del ejército, de los contratistas que trabajaban para el ejército y de las universidades participantes en investigaciones relacionadas con la defensa comunicarse entre sí a través de canales redundantes, incluso en caso de que algunas partes de la red resultasen dañadas en una guerra.⁷⁵

Los primeros programas de correo electrónico aparecieron en 1972. En 1985, la Fundación Nacional de la Ciencia de E.U.A. construyó la red "NSFNET" con el fin de enlazar seis grandes centros informáticos del país. En los años ochenta, dicha red se transfirió a un grupo de universidades llamado "MERIT" y se fue abriendo paulatinamente a instituciones no académicas y organizaciones no estadounidenses. En 1990, Tim Berners Lee, que trabajaba en el Centro Europeo para la Investigación Nuclear de Ginebra, diseñó el primer navegador y aplicó el concepto de "hipervínculo", tras lo cual se han ido añadiendo continuamente gran variedad de nuevos servicios y funciones.⁷⁶

En la actualidad, "TCP/IP" sigue siendo el protocolo básico de transmisión de datos en Internet y todos los servicios dependen de él. Este protocolo, cuyo diseño

⁷³ Grupo de trabajo sobre protección de datos del artículo 29, *Privacidad en Internet: Enfoque comunitario integrado de la protección de datos en línea*. Documento de trabajo 5063/00/ES/FINAL WP 37, adoptado el 21 de noviembre de 2000, p.p. 8.

⁷⁴ Véase: Sentencia Reno contra ACLU de 26 de junio de 1997, Tribunal Supremo de los Estados Unidos, Recuperado de: www2.epic.org/cda/cda_decision.html (consultado en enero 2021)

⁷⁵ Comunicación de la Comisión al Consejo y al Parlamento Europeo, *La organización y gestión de Internet, Cuestiones de política europea e internacional 1998 – 2000*, COM (2000) 202 final, 11 de abril de 2000.

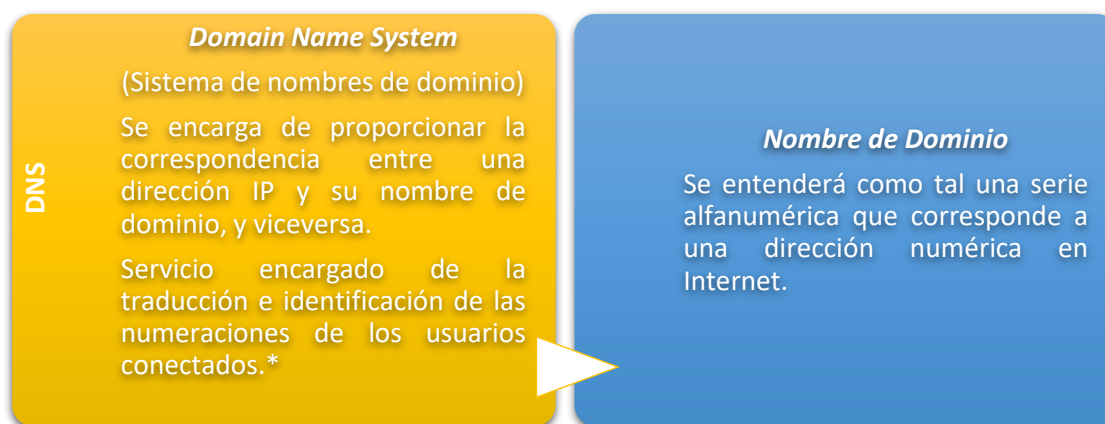
⁷⁶ Grupo de trabajo sobre protección de datos del artículo 29, *Privacidad en Internet: Enfoque comunitario integrado de la protección de datos en línea*. Documento de trabajo 5063/00/ES/FINAL WP 37, adoptado el 21 de noviembre de 2000, p.p. 8-9.

permite una instalación muy sencilla, no depende de ningún sistema operativo ni informático específico. En Internet, cada ordenador se identifica con una dirección “IP” numérica única de la forma A.B.C.D, en la que A, B, C y D son números del 0 al 255 (por ejemplo, 194.178.86.66).⁷⁷

Para mejor comprensión de lo anterior, existe una corporación llamada *Internet Corporation for Assigned Names and Numbers* (ICANN), quien es una organización que opera a nivel multinacional/internacional y es la responsable de asignar las direcciones del protocolo IP, de los identificadores de protocolo, de las funciones de gestión del sistema de dominio y de la administración del sistema de servidores raíz.⁷⁸

Bajo ese contexto, ICANN coordina la administración de los elementos técnicos del Sistema de Nombres de Dominio (DNS) para garantizar la resolución unívoca de los nombres, de esta manera los usuarios pueden encontrar todas las direcciones IP sin ser repetidas.⁷⁹

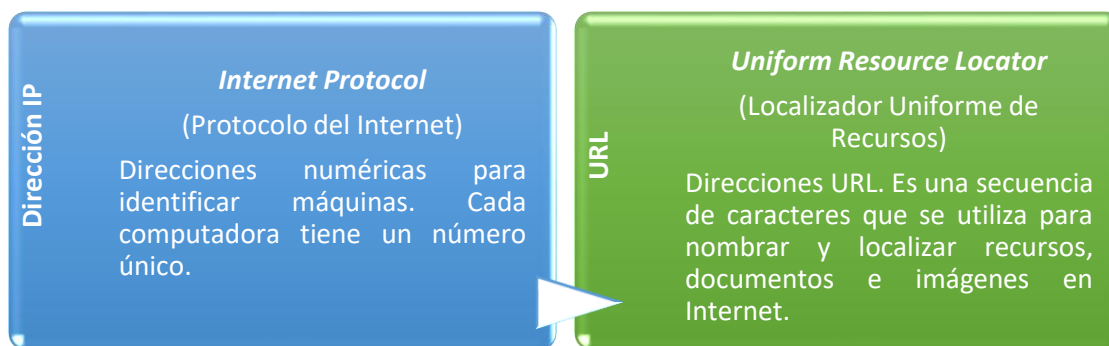
Para ejemplificar lo expuesto con antelación y comprender los conceptos de sistema de nombres de dominio, nombres de dominio, el protocolo IP y su diferencia con un localizador uniforme de recursos, mejor conocida como URL, se desarrolla el esquema siguiente:



⁷⁷ *Idem.*

⁷⁸ *Internet Corporation for Assigned Names and Numbers* (ICANN), Recuperado de: www.icann.org (consultado en enero 2021)

⁷⁹ *Idem.*



*Cada vez que se inicia una comunicación con un nombre de dominio, el ordenador realiza una petición a su servidor DNS para que le proporcione la IP asociada a ese nombre.

Figura 1. Aspectos Generales. Nombres de dominio y protocolo de internet.

Fuente: Elaboración propia.⁸⁰

En México, NIC México (*Network Information Center México*), es la organización encargada de la administración del nombre de dominio territorial (*ccTLD, country code Top Level Domain*) “.MX”, que es el código de dos letras asignado a cada país según el ISO 3166. Entre sus funciones están el proveer los servicios de información y registro para “.MX”, así como la asignación de direcciones de IP y el mantenimiento de las bases de datos respectivas a cada recurso⁸¹. En el año 2018, los dominios “.MX” alcanzaron el millón de nombres registrados y en 2019, NIC celebró su 30 aniversario de los dominios “.MX” en México.

Visto todo lo anterior, es importante denotar que, según la Unión Internacional de Telecomunicaciones, en su Informe sobre el Desarrollo Mundial de las Telecomunicaciones/TIC y base de datos, estimó que, a finales de 2019, un poco más del 51% de la población mundial o 4,000 millones de personas, tienen acceso y eso de Internet, tal y como se muestra en el gráfico siguiente:

⁸⁰ Video: *IP addresses and DNS | Internet 101 | Computer Science | Khan Academy*. Recuperado de: <https://www.youtube.com/watch?v=MwxMsaFFycg&feature=youtu.be> (consultado en febrero 2021)

⁸¹ NIC México, (*Network Information Center México*), Recuperado de: www.nicmexico.mx (consultado en febrero 2021)

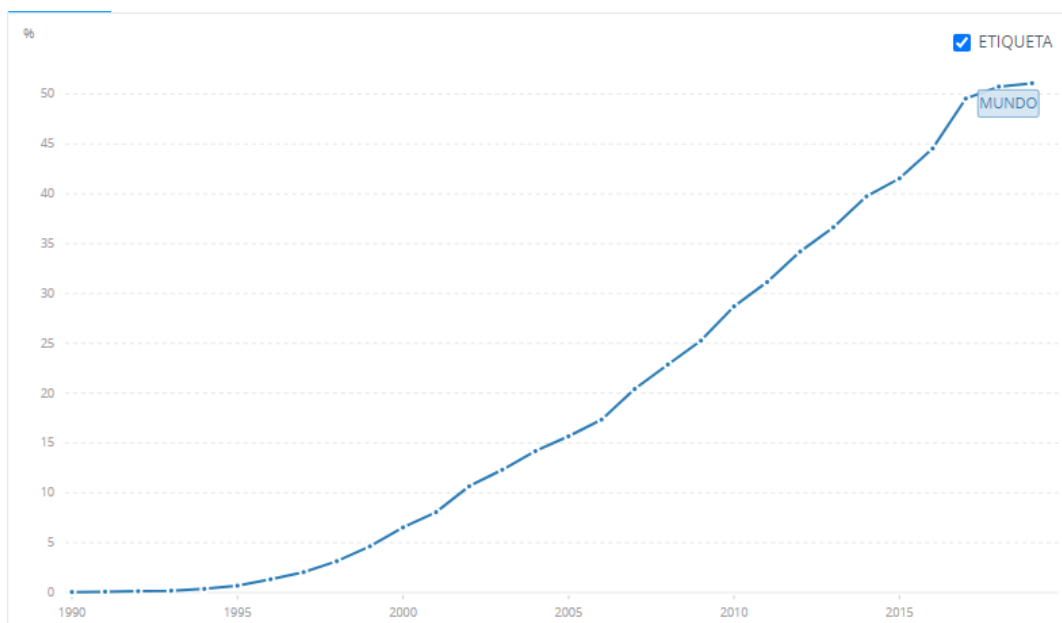


Figura 2. Personas que usan Internet (% de la población a nivel mundial).

Fuente: Unión Internacional de Telecomunicaciones (UIT) ⁸²

En México, el Instituto Nacional de Estadística y Geografía (INEGI) presentó en mayo de 2019, las estadísticas obtenidas de la Encuesta Nacional sobre Disponibilidad y Uso de Tecnologías de la Información en los Hogares (ENDUTIH), de la cual, entre otros datos se desprende que el 70.1% de la población de seis años o más en México es usuaria de Internet y cerca de 20.1 millones de hogares (56.4% del total nacional) disponen de conexión a Internet, asimismo, las principales actividades realizadas en Internet durante 2019 son: para entretenimiento (91.5%), para obtener información (90.7%) y para comunicarse (90.6%).⁸³

En conclusión, podemos observar que el Internet, al igual que la energía, los mercados o el transporte, se ha convertido en una parte esencial de la infraestructura de los países⁸⁴, constituyendo un factor esencial de comunicación y producción en casi cualquier actividad de toda sociedad y economía moderna.

⁸² Unión Internacional de Telecomunicaciones, *Informe sobre el Desarrollo Mundial de las Telecomunicaciones/TIC y base de datos*. Recuperado de: <https://datos.bancomundial.org/indicador/IT.NET.USER.ZS?end=2019&start=1990&view=chart> (consultado en febrero 2021)

⁸³ INEGI, *Estadísticas a propósito del Día Mundial del Internet Datos Nacionales*, 17 de mayo 2019.

⁸⁴ Forbes, *¿De qué manera el internet impulsa a la economía?*, Forbes Staff, mayo 2016. Recuperado de: <https://www.forbes.com.mx/manera-internet-impulsa-la-economia/> (consultado en febrero 2021)

Pues, después de un siglo y medio de investigación e innovaciones, Internet ha quedado firmemente establecido como un recurso accesible para muchas personas, ofreciendo una amplia variedad de beneficios potenciales, a través de los cuales, los usuarios tienen un mayor acceso a todo tipo de información.

Por su parte, los gobiernos y negocios disponen de una nueva plataforma para proporcionar información y servicios, asimismo, por su parte, el comercio electrónico trajo consigo un gran crecimiento económico, mayor amplitud de oferta para los consumidores y oportunidades para productores para llegar a nuevos mercados; por otro lado, se proporciona una gran variedad de opciones de comunicación, desde un correo electrónico hasta elaboradas redes sociales⁸⁵, que sin duda han impulsado a una interconexión social en la era digital.

Sin embargo, aún existen muchos desafíos a los que se enfrenta Internet. En dónde los usuarios son víctimas de prácticas abusivas como el spam (correo comercial no deseado), ciberdelincuencia, usurpación de identidad, entre otros, por lo que a pesar de que los expertos técnicos responden con soluciones que intentan minimizar estos peligros continuos diseñando sistemas anti-virus, filtros, transacciones seguras y otras medidas, lo cierto, es que la tecnología continúa evolucionando día a día.⁸⁶

Aunado a lo anterior, debemos tomar en cuenta que aún existe una gran brecha digital para asegurar y garantizar el servicio a todos y en todos los rincones del mundo, pues en 2019, casi el 87% de las personas en países desarrollados utilizaban Internet, en comparación con el 47% de los países en desarrollo.⁸⁷

También se observan brechas digitales dentro de los países, como por ejemplo, a Internet se conectan más hombres, residentes de ciudades y jóvenes que habitantes de zonas rurales y personas mayores. En lo que respecta a la penetración de Internet, la brecha digital de género es relativamente pequeña en

⁸⁵ Varios autores, Traducción Laura Vidal y Mar Ozores, Sirk Traducciones, *Fronteras del Conocimiento*, BBVA-Turner, Noviembre 2008, p.p. 23, recuperado de: <http://www.bbvaopenmind.com/> (consultado en febrero 2021)

⁸⁶ *Idem*.

⁸⁷ Unión Internacional de Telecomunicaciones (UIT), *Inclusión digital para todo*, Disponible en: [https://www.itu.int/es/mediacentre/backgrounders/Pages/digital-inclusion-of_all.aspx#:~:text=SDG\)%20para%202030.Retos,digitales%20dentro%20de%20los%20pa%C3%ADses.](https://www.itu.int/es/mediacentre/backgrounders/Pages/digital-inclusion-of_all.aspx#:~:text=SDG)%20para%202030.Retos,digitales%20dentro%20de%20los%20pa%C3%ADses.) (consultado en febrero 2021).

países desarrollados, más pronunciada en países en desarrollo e importante en países menos adelantados.⁸⁸

Esas diferencias suelen deberse a una conectividad insuficiente o lenta, al coste de la conexión y a la falta de contenidos pertinentes en las lenguas locales. Por lo tanto, esas barreras suelen estar relacionadas con edad, género, discapacidades, estatus socioeconómico y geografía, lo cual, nos lleva a nuestro tema siguiente.

2.2. La sociedad de la información frente al uso de Internet

En la actualidad, derivado del incremento en las tecnologías, la propagación de información a través de Internet, comercio electrónico, el acceso a las redes sociales y la interconexión en general, nos vemos en la necesidad de regular y proteger a los usuarios ante el uso inadecuado de dichas herramientas, procurando la protección de su privacidad y sus datos personales.

Ante la inminente preocupación, la Cumbre Mundial sobre la Sociedad de la Información (CMSI), que se celebró en dos fases, a saber, en Ginebra del 10 al 12 de diciembre de 2003 y en Túnez del 16 al 18 de noviembre de 2005, se aprobaron los documentos de resultados de la CMSI, en los que se estableció el sólido compromiso de *“construir una sociedad de la información centrada en la persona, abierta a todos y orientada al desarrollo, en la que todas las personas puedan crear, consultar, utilizar y compartir información y el conocimiento, para que las personas, las comunidades y los pueblos puedan emplear plenamente sus posibilidades en la promoción de su desarrollo sostenible y en la mejora de su calidad de vida, sobre la base de los propósitos y principios de la Carta de las Naciones Unidas y respetando plenamente y defendiendo la Declaración Universal de Derechos Humanos.”*⁸⁹

Bajo ese contexto, es claro que la creación de la Sociedad de la Información ha implicado un gran desafío global para el nuevo milenio, sin embargo, es importante denotar que siempre se ha reafirmado la implementación y

⁸⁸ *Idem.*

⁸⁹ Cumbre Mundial sobre la Sociedad de la Información (CMSI). Ginebra 2003 y Túnez 2005, p.p. 10-11. Recuperado de: <http://www.itu.int/net/wsis/basic/index-es.html> (consultado en febrero 2021)

reconocimiento de diversos instrumentos internacionales para su construcción, entre los cuales se encuentran los siguientes:

1. Artículo 19 de la Declaración Universal de Derechos Humanos, todo individuo tiene derecho a la libertad de opinión y de expresión, que este derecho incluye el de no ser molestado a causa de sus opiniones, el de investigar y recibir información y opiniones, y el de difundirlas, sin limitación de fronteras, por cualquier medio de expresión. La comunicación es un proceso social fundamental, una necesidad humana básica y el fundamento de toda organización social.
2. Artículo 29 de la Declaración Universal de Derechos Humanos, a saber, que toda persona tiene deberes respecto a la comunidad, puesto que sólo en ella puede desarrollar libre y plenamente su personalidad, y que, en el ejercicio de sus derechos y en el disfrute de sus libertades, toda persona estará solamente sujeta a las limitaciones establecidas por la ley con el único fin de asegurar el reconocimiento y el respeto de los derechos y libertades de los demás, y de satisfacer las justas exigencias de la moral, del orden público y del bienestar general en una sociedad democrática.⁹⁰

Adicionalmente, la declaración de la Sociedad de la Información, en adelante la “declaración”, por una parte, reconoce la importancia del papel que desempeña la ciencia, produciendo los grandes avances técnicos en las nuevas tecnologías de las comunicación e información, así como la importancia que tiene la educación, el conocimiento, la información y comunicación, para un debido proceso de la Sociedad de la Información, teniendo plena conciencia de que las TIC deben de considerarse un medio y no un fin en sí mismas.

Lo anterior, resulta de vital importancia, toda vez que, en condiciones favorables, estas tecnologías pueden ser un instrumento eficaz para acrecentar la productividad, generar crecimiento económico, crear empleos y fomentar la ocupabilidad, así como mejorar la calidad de la vida de todos. Pueden, además, promover el diálogo entre las personas, las naciones y las civilizaciones.⁹¹

⁹⁰ *Idem*

⁹¹ *Idem*

En relatadas condiciones, mediante la “declaración”, se establecieron que para la creación de una Sociedad de la Información “para todos”, es necesario tomar en cuenta los siguientes principios fundamentales siguientes:⁹²

- 1) La función de los gobiernos y de todas las partes interesadas en la promoción de las TIC para el desarrollo: Los gobiernos, al igual que el sector privado, la sociedad civil, las Naciones Unidas y otras organizaciones internacionales, tienen una función y una responsabilidad importantes en el desarrollo de la Sociedad de la Información y, en su caso, en el proceso de toma de decisiones.
- 2) Infraestructura de la información y las comunicaciones: fundamento básico de una Sociedad de la Información integradora: La conectividad, la infraestructura de la red y aplicación de las TIC, son de acceso universal, ubicuo, equitativo y asequible a la infraestructura y los servicios, mismas que deberán de adaptarse a las condiciones regionales, siempre en busca de un progreso económico y social de los países, en beneficio de todas las personas.
- 3) Acceso a la información y al conocimiento: La capacidad universal de acceder y contribuir a la información, las ideas y el conocimiento es un elemento indispensable en una Sociedad de la Información integradora.
- 4) Creación de capacidad: Toda persona tendrá la posibilidad de adquirir las competencias y los conocimientos necesarios para comprender la Sociedad de la Información y la economía del conocimiento, participar activamente en ellas y aprovechar plenamente sus beneficios.
- 5) Fomento de la confianza y seguridad en la utilización de las TIC: El fomento de un clima de confianza, incluso en la seguridad de la información y la seguridad de las redes, la autenticación, la privacidad y la protección de los consumidores, es requisito previo para que se desarrolle la Sociedad de la Información y para promover la confianza entre los usuarios de las TIC.

⁹² *Ibidem*, p.p. 14-22

- 6) Entorno propicio: El estado de derecho, acompañado por un marco de política y reglamentación propicio, transparente, favorable a la competencia, tecnológicamente neutro, predecible y que refleje las realidades nacionales, es insoslayable para construir una Sociedad de la Información centrada en la persona.

Internet se ha convertido en un recurso global disponible para el público, y su gestión debe ser una de las cuestiones esenciales del programa de la Sociedad de la Información. La gestión internacional de Internet debe ser multilateral, transparente y democrática, y contar con la plena participación de los gobiernos, el sector privado, la sociedad civil y las organizaciones internacionales. Esta gestión debería garantizar la distribución equitativa de recursos, facilitar el acceso a todos y garantizar un funcionamiento estable y seguro de Internet, teniendo en cuenta el plurilingüismo.

- 7) Aplicaciones de las TIC: beneficios en todos los aspectos de la vida: En la utilización y despliegue de las TIC se debe tratar de generar beneficios en todos los ámbitos de nuestra vida cotidiana.
- 8) Diversidad e identidad culturales, diversidad lingüística y contenido local: La diversidad cultural es el patrimonio común de la humanidad. La Sociedad de la Información debe fundarse en el reconocimiento y respeto de la identidad cultural, la diversidad cultural y lingüística, las tradiciones y las religiones, además de promover un diálogo entre las culturas y las civilizaciones.
- 9) Medios de comunicación: Adheridos a los principios de libertad de la prensa y libertad de la información, así como la independencia, el pluralismo y la diversidad de los medios de comunicación, que son esenciales para la Sociedad de la Información. También es importante la libertad de buscar, recibir, difundir y utilizar la información para la creación, recopilación y divulgación del conocimiento.
- 10) Dimensiones éticas de la Sociedad de la Información: La Sociedad de la Información debe respetar la paz y regirse por los valores fundamentales

de libertad, igualdad, solidaridad, tolerancia, responsabilidad compartida y respeto a la naturaleza, asimismo, se reconoce la importancia de la ética, justicia y dignidad humana.

11) Cooperación internacional y regional: La Sociedad de la Información es por naturaleza intrínsecamente global y los esfuerzos nacionales deben ser respaldados por una cooperación eficaz, a nivel internacional y regional entre los gobiernos, el sector privado, la sociedad civil y las demás partes interesadas.

Como podemos ver hasta lo aquí analizado, la declaración de principios de la Sociedad de la Información, a grandes rasgos, busca la reducción de la brecha digital entre la sociedad y naciones, teniendo en cuenta el desarrollo y evolución de la misma, bajo la premisa de una colectividad que ejerza plenamente y disfrute de los beneficios que otorgan las TIC, bajo una evolución y transformación digital que garantice y reconozca los derechos fundamentales de las personas.

En ese sentido, se proyecta un “Plan de acción”, que todas las partes interesadas pueden prestar una contribución importante en la Sociedad de la Información, especialmente a través de asociaciones, a saber:⁹³

a) A los gobiernos incumbe la función de dirigir la formulación y aplicación de “ciberestrategias” nacionales exhaustivas, orientadas al futuro y sostenibles. El sector privado y la sociedad civil, en diálogo con los gobiernos, tienen una importante función consultiva en la formulación de esas “ciberestrategias” nacionales.

b) La aportación del sector privado es importante para el desarrollo y la difusión de las tecnologías de la información y la comunicación (TIC) en ámbitos como infraestructura, contenido y aplicaciones. El sector privado no es sólo un actor del mercado, sino que desempeña un papel en el contexto más amplio de desarrollo sostenible.

c) El compromiso y la participación de la sociedad civil es igualmente importante en la creación de una Sociedad de la Información equitativa y en

⁹³ *Ibidem*, p.p. 27

la instrumentación de las iniciativas para el desarrollo relacionadas con las TIC.

d) Las instituciones internacionales y regionales, incluidas las instituciones financieras internacionales, desempeñan un papel clave a la hora de integrar la utilización de las TIC en el proceso de desarrollo y proporcionar los recursos necesarios para construir la Sociedad de la Información y evaluar los progresos alcanzados.

Visto lo anterior, es importante denotar que en México se han implementado diversos esfuerzos para fomentar el desarrollo de la Sociedad de la Información, ya que no puede dejarse de lado la dinámica de la globalización digital, pues ignorar todos estos acontecimientos, traería consigo un gran rezago tanto social, cultural y económico a nuestro país.

Un hecho importante al respecto, ha sido el compromiso del Gobierno Federal y de importantes sectores sociales con relación al apoyo que se le ha dado a la Corporación Universitaria para el Desarrollo de Internet⁹⁴ cuyos beneficios para México han sido canalizados principalmente a la educación presencial y a distancia; investigación en diversas disciplinas (por ejemplo innovación en telemedicina, astronomía, física, química, ingeniería, arqueología, etcétera) y; en infraestructura para el desarrollo de bibliotecas digitales. Un aspecto importante ha sido contemplar estrategias de apropiación de tecnologías a través de una intensa labor en formación de recursos humanos.⁹⁵

Entre los programas más relevantes vinculados con la Sociedad de la Información en México, se ha impulsado el desarrollo de un “Gobierno Electrónico”, en el cual se incluye todas aquellas actividades basadas en las modernas tecnologías informáticas, en particular Internet, que el Estado desarrolla para aumentar la eficiencia de la gestión pública, mejorar los servicios ofrecidos a los

⁹⁴ Poder Ejecutivo Federal, *Plan Nacional de Desarrollo 1995-2000. Programa de Desarrollo Informático: México*, Secretaría de Hacienda y Crédito Público, México, mayor, 1995.

⁹⁵ Garduño Vera Roberto, “La sociedad de la información en México frente al uso de internet”, *Revista Digital Universitaria*, UNAM, 10 de septiembre 2004, Volumen 5 Número 8, p. p. 7-13.

ciudadanos y proveer a las acciones de gobierno de un marco mucho más transparente que el actual.⁹⁶

Aunado a dichas acciones, en México, aún hace falta fomentar muchos esfuerzos tanto institucionales a nivel público, como en el sector privado, privilegiando el libre acceso a Internet y otorgando los mecanismos o herramientas necesarias para que, por un lado, se disminuya la brecha digital y garantizar la conexión, y por otro lado, otorgar seguridad de la información, privacidad, confidencialidad y protección de datos personales a los usuarios.

Lo anterior, se ejemplifica conforme a la Encuesta Nacional sobre Disponibilidad y Uso de Tecnologías de la Información en los Hogares, elaborada por el INEGI en 2019, a través de la cual se reporta que, en dicho año, 80.6 millones de las personas de seis años o más en el país, hacen uso de Internet (70.1% de la población).

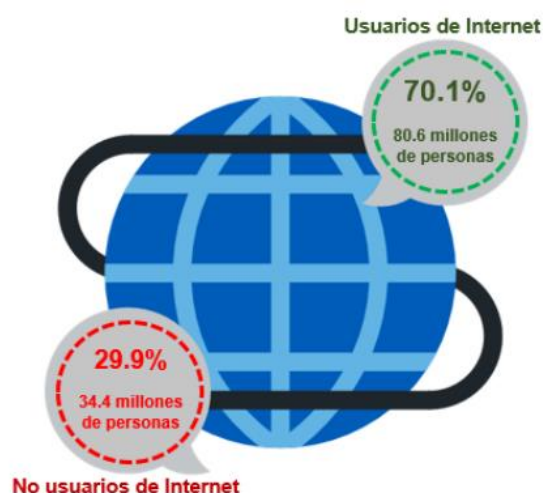


Figura 3. Porcentaje de la población de seis años o más según condición de uso de Internet. Fuente: Secretaría de la Función Pública, 2019.⁹⁷

Sin embargo, por zona urbano-rural presenta una diferencia de 28.9 puntos porcentuales, ya que los resultados reflejan un 76.6% en las zonas urbanas y 47.7% en las rurales.

⁹⁶ Secretaría de la Función Pública, *Gobierno Digital o Electrónico, Mejores Prácticas Internacionales*, Gobierno de México, Documento, 09 de diciembre de 2013.

⁹⁷ INEGI, *Estadísticas a propósito del Día Mundial del Internet Datos Nacionales*, 17 de mayo 2019.

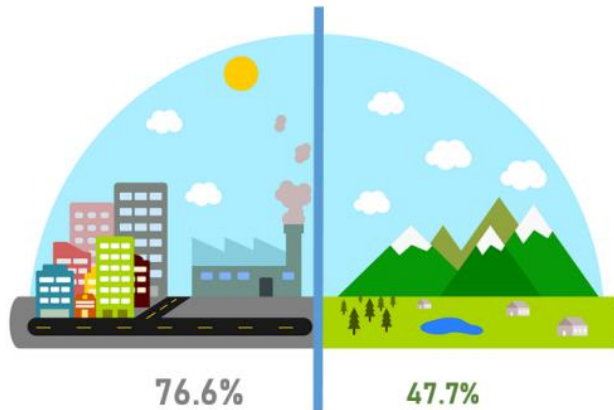


Figura 4. Distribución de los usuarios de Internet en áreas urbano-rural,
Fuente: Secretaría de la Función Pública, 2019.⁹⁸

2.3. Internet y sociedad, su impacto en derecho

Definitivamente el Internet, ha sido el gran fenómeno que ha dado pie a la acelerada evolución de las nuevas tecnologías de la información y la comunicación. Como lo hemos visto a lo largo del presente capítulo, la transformación digital impacta en todos los sectores como la economía, gobierno y la sociedad en general, transformando nuestra manera de vivir, trabajar y comunicar.

La interconexión que nos permite el Internet ha dejado claro que no existen fronteras, distancias ni autoridad centralizada que pueda regularla.⁹⁹Bajo ese contexto, sí bien, el uso de Internet en nuestra vida diaria trae innumerables ventajas derivadas a las posibilidades que nos brinda esta herramienta de conocimiento y comunicación, lo cierto es que, el Internet se ha convertido en un terreno en dónde han surgido diversos tipos de criminalidad, fraudes, virus, vulneraciones a la privacidad de los usuarios, entre otros problemas.

Internet implica, por tanto, un riesgo de un efecto multiplicador de los atentados contra derechos, bienes e intereses jurídicos. Su potencialidad en la difusión ilimitada de imágenes e informaciones la hace un vehículo especialmente poderoso para perpetrar atentados criminales, de forma enunciativa el Maestro

⁹⁸ *Idem*

⁹⁹ Pérez Luño Antonio Enrique, "Impactos Sociales y Jurídicos de Internet", *Revista Argumentos de Razón Técnica*, Universidad de Sevilla, No. 19980, p.p. 33-18.

Pérez Luño, analiza cuatro tipos de bienes jurídicos básicos que pudieran verse afectados, a saber:¹⁰⁰

- I. *La intimidad, la imagen, la dignidad y el honor de las personas*, al posibilitar la intromisión indebida en datos personales, su transmisión no autorizada, el acoso informático, la propagación universal de difamaciones, calumnias e injurias, la incitación al odio o la discriminación.
- II. *La libertad sexual* al permitir la propagación de imágenes o informaciones que entrañen formas de exhibicionismo, provocación sexual o fomenten la pornografía entre menores de edad.
- III. *La propiedad intelectual e industrial*, ya que Internet puede contribuir a la distribución ilícita de obras registradas como propiedad intelectual o industrial, a la piratería de programas, así como a la difusión de contenidos publicitarios ilegítimos.
- IV. *La seguridad nacional y el orden público*, en cuanto que pueden contribuir a facilitar atentados y desórdenes públicos, e incluso actividades terroristas.

Cabe aclarar que dichas conductas, únicamente son de manera enunciativa, más no limitativa, en dónde incluso debemos tomar en cuenta el carácter internacional e ilimitado de esas conductas, lo cual hace más difícil su descubrimiento, prevención y castigo, ya que incluso en los casos en que puedan ser detectadas pueden plantearse conflictos sobre la jurisdicción sancionadora competente.¹⁰¹

Al respecto, el mismo Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos personales, en México, dentro de sus recomendaciones a la sociedad, reconoce algunos riesgos que podríamos sufrir en Internet, entre los cuales se encuentran los siguientes:

¹⁰⁰ *Idem*

¹⁰¹ *Ibidem*, p.p. 36.

¿Qué riesgos puedes sufrir en Internet?

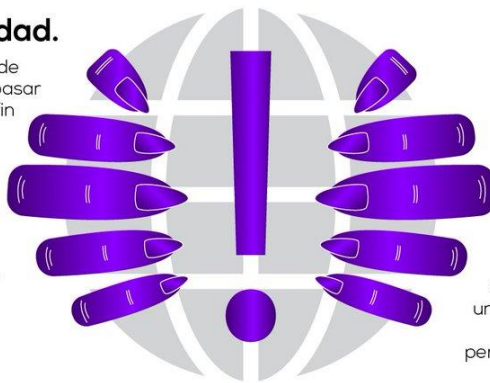
Una protección adecuada de tus Datos Personales contribuirá a que no seas víctima de delitos en la web como:

1. Robo de identidad.

Apropiación de la identidad de una persona para hacerse pasar por ella frente a terceros a fin de obtener ciertos recursos o beneficios a su nombre.

2. Phishing.

Modalidad de usurpación de identidad cuyo objetivo es obtener información confidencial o bancaria de usuarios para beneficio económico.



3. Sexting.

Generación y envío de fotos o videos de contenido sexual con alguien de confianza. El problema se presenta cuando se rompe este vínculo y se hace un uso y divulgación indebida de los contenidos.

4. Extorsión.

Radica en obligar a otro a realizar u omitir un acto a cambio de no difundir imágenes con el objetivo de obtener un beneficio económico.

5. Secuestro.

Mediante información difundida en redes sociales, un tercero puede identificar y privar de la libertad a una persona, o grupo de personas, con el objeto de obtener un rescate.

Fuente: Secretaría de Protección de Datos Personales del INAI.



 @INAIMexico

 INAI mx


 inaimexico

Figura 5. ¿Qué riesgos puedes sufrir en Internet? Fuente: INAI.¹⁰²

Conforme a lo anterior, podemos aseverar que el uso del Internet plantea una preocupante paradoja, que deriva de su eficacia global e ilimitada para atentar contra bienes y derechos, mientras que la capacidad de respuesta jurídica se halla fraccionada por las fronteras nacionales. Por ello, la reglamentación jurídica del flujo interno e internacional de datos es uno de los principales retos que hoy se plantean a los ordenamientos jurídicos nacionales y al orden jurídico internacional.¹⁰³

¹⁰² INAI, Secretaría de Protección de Datos Personales, 18 de noviembre de 2017, Twitter, recuperado de: <https://twitter.com/inaimexico/status/1051132995086761984> (consultado en febrero 2021)

¹⁰³ Pérez Luño Antonio Enrique, "Impactos Sociales y Jurídicos de Internet", *Revista Argumentos de Razón Técnica*, Universidad de Sevilla, No. 19980, p.p. 36.

Aunado a lo anterior, debemos reconocer que Internet es una herramienta de expresión cultural, de acceso a la información y comunicación, que dio origen a la Sociedad de la Información, sin embargo, para su debido progreso, no debe dejar de lado el cumplimiento, observancia y garantía de los derechos humanos y civiles de los usuarios, preservando los principios rectores del estado de derecho de cada nación.

La Asamblea General de la Organización de las Naciones Unidas (ONU) en el año 2011 declaró el acceso a Internet como un derecho humano por ser una herramienta que favorece el crecimiento y el progreso de la sociedad en su conjunto.¹⁰⁴

Al respecto, la Comisión Interamericana de Derechos Humanos, ha establecido que el Internet cuenta con una serie de principios orientadores en su desarrollo, entre los que destacan:¹⁰⁵

- a) *El acceso*, El principio de acceso universal se refiere a la necesidad de garantizar la conectividad y el acceso universal, ubicuo, equitativo, verdaderamente asequible y de calidad adecuada, a la infraestructura de Internet y a los servicios de las TIC, en todo el territorio del Estado, tal como ha sido reconocido por los jefes de Estado en las Cumbres de las Américas.¹⁰⁶
- b) *El pluralismo*, Maximizar el número y la diversidad de voces que puedan participar de la deliberación pública es al mismo tiempo condición y finalidad esencial del proceso democrático.
- c) *La no discriminación*, de conformidad con los artículos 1.1 y 24 de la Convención Americana, los Estados están obligados a “adoptar medidas positivas (legislativas, administrativas o de cualquier otra naturaleza) para

¹⁰⁴ Bonilla, Haideer Miranda, “El Acceso a Internet como Derecho Fundamental”, *Revista Jurídica IUS Doctrina*, Facultad de Derecho de la UCR, Costa Rica, N° 15, 2016, p.p. 16.

¹⁰⁵ Comisión Interamericana de Derechos Humanos, *Informe Libertad de Expresión e Internet*, Relatoría Especial para la Libertad de Expresión, OEA/Ser.L/V/II. CIDH/RELE/INF. 11/13, 31 diciembre 2013, p.p.7-9.

¹⁰⁶ Organización de los Estados Americanos, *Sexta Cumbre de las Américas, Mandatos derivados de la Sexta Cumbre de las Américas. 23 de mayo de 2012. Acceso y uso de las tecnologías de la información y las comunicaciones*, OEA/Ser.E CA-VI/doc.6/12 Rev.2, Cartagena de Indias, Colombia, 14 y 15 de abril de 2012, Párr. 1-4.

revertir o cambiar situaciones discriminatorias existentes que comprometan el goce y ejercicio efectivo del derecho a la libertad de expresión de ciertos grupos, en condiciones de igualdad y no discriminación”¹⁰⁷; y

- d) *La privacidad*, el artículo 11 de la Convención Americana de Derechos Humanos establece que “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”, y que “Toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques”. De esta forma, le corresponde al Estado respetar la privacidad de los individuos y velar por que terceras personas no incurran en conductas que puedan afectarla arbitrariamente.

Sobre este último punto, es importante denotar que, tal y como fue observado por la Asamblea General de las Naciones Unidas en la resolución “El derecho a la privacidad en la era digital”, adoptada por consenso, los Estados tienen la obligación de respetar y proteger el derecho a la privacidad de conformidad con el derecho internacional de los derechos humanos, incluyendo en el contexto de las comunicaciones digitales.¹⁰⁸

En consecuencia, es claro que en el ámbito del derecho los avances tecnológicos que ha generado que el uso de Internet nuevos desafíos, tanto desde un punto de vista de tutela jurisdiccional, hasta cuestiones de implementación, en dónde aún se encuentra en desarrollo el sistema jurídico ideal para brindar solución y protección a cada uno de los riesgos o problemas que se originen en la red.

Ante ello, aunado a los instrumentos internacionales que se han citado con antelación, una de las iniciativas más importantes sobre la regulación, prevención y sanción de los delitos en Internet es el Convenio sobre Ciberdelincuencia, más conocido como “Convenio de Budapest”¹⁰⁹. El convenio entró en vigor en 2004 y constituye

¹⁰⁷ Comisión Interamericana de Derechos Humanos, *Informe Anual 2008. Informe de la Relatoría Especial para la Libertad de Expresión. Capítulo III (Marco Jurídico Interamericano del Derecho a la Libertad de Expresión)*. OEA/Ser. L/V/II.134. Doc 5 rev. 1. 25 de febrero de 2009. Párr. 230.

¹⁰⁸ ONU, Asamblea General, *El derecho a la privacidad en la era digital*, Resolución aprobada por la Asamblea General el 18 de diciembre de 2013, Párr. 4. Recuperado de: http://www.un.org/Depts/dhl/resguide/r68_es.shtml (consultado en febrero 2021)

¹⁰⁹ Consejo de Europa, *Convenio sobre la ciberdelincuencia*, Budapest, 2001. Recuperado de: https://www.oas.org/juridico/english/cyb_pry_convenio.pdf (consultado en febrero 2021)

hasta el momento el único instrumento internacional que aborda de manera específica el tema de “cibercrimen”.

Los delitos que se cometen en y a través de la red suelen tener carácter transnacional, ya sea porque son cometidos por personas que operan en diferentes países, porque las víctimas están en un país distinto o porque la prueba está alojada en servidores ubicados en países distintos al que lleva adelante la investigación. Es por ello que, las investigaciones suelen requerir la intervención de diferentes Estados. A su vez, esto dio impulso a que hayan surgido iniciativas de regulación por parte de organismos internacionales.¹¹⁰

Si bien el tratado fue creado en el seno de una institución europea, está abierto para que otros estados puedan adherirse, por lo que actualmente 65 estados son miembros del Convenio de Budapest, incluso algunas naciones de Latinoamérica y el Caribe como Colombia, Costa Rica, Panamá, República Dominicana, Perú, Paraguay, Chile y Argentina. Por su parte, México se encuentra como observador, pero no se ha adherido, toda vez que resulta necesario que el Presidente de la República celebre la adhesión al Convenio de Budapest y esta deberá ser aprobada por el Senado, obligando al país a realizar las reformas pertinentes.

A pesar de todos los esfuerzos legislativos, económicos y estructurales que pudieran realizarse, para un mejor y seguro entorno en el Internet, es necesario que el usuario, desarrolle una cultura de legalidad sobre el uso del Internet, es decir, cuente con el conocimiento necesario e implemente diversas medidas para un uso informado y consiente de la red, ante dicha situación, el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, en México, realiza en materia de ciberseguridad las recomendaciones siguientes:

¹¹⁰ Asociación por los Derechos Civiles. “La Convención de Cibercrimen de Budapest y América Latina: Breve guía acerca de su impacto en los derechos y garantías de las personas”, *Área digital*, volumen 1, *Creative Commons*, 2018, p.p.8-9.



Figura 6. Protección de datos personales y ciberseguridad. Fuente: INAI.¹¹¹

Al respecto, debemos denotar que el pasado 1° de septiembre de 2020, se presentó la iniciativa para expedir una ley que regule la materia de ciberseguridad en México, la cual busca modificar el Código Penal Federal y la Ley General del Sistema Nacional de Seguridad para que tanto las regulaciones en materia de seguridad de la información como los delitos cibernéticos que se cometan sean normados y sancionados por una nueva “Ley General de Ciberseguridad”.¹¹²

A manera de contexto, la iniciativa tiene entre otros, los objetivos siguientes:

¹¹¹ INAI, 27 de octubre de 2020, recuperado de: https://twitter.com/INAI_Mexico/status/1352798337553072130/photo/1 (consultado en febrero 2021)

¹¹² Iniciativa con aval del grupo parlamentario que contiene proyecto de decreto por el que se modifica la denominación del Capítulo II, Del Título Noveno, del Libro Segundo y se reforma el artículo 211 BIS 1 y se derogan diversos artículos del Código Penal Federal; se reforman y adicionan diversos artículos de la Ley General del Sistema Nacional de Seguridad Pública; se adiciona una fracción XIV al artículo 5° de la Ley de Seguridad Nacional; y se expide la Ley General de Ciberseguridad, recuperado de: http://sil.gobernacion.gob.mx/Archivos/Documentos/2020/09/asun_4064516_20200902_1599062884.pdf (consultado en enero de 2021)

1) Establecer tipos penales en la materia e integrar la forma y los términos en que las autoridades de las entidades federativas y los municipios colaborarán con la Federación en dicha tarea;

2) Garantizar el derecho de acceso a las tecnologías de la información y comunicación, así como a los servicios de telecomunicaciones, incluido el de banda ancha e internet en forma segura;

3) Crear la Comisión Permanente de Ciberseguridad dentro de la estructura del Consejo Nacional de Seguridad Pública;

4) Originar el Centro Nacional de Ciberseguridad dentro de la estructura del Secretariado Ejecutivo del Sistema Nacional de Seguridad Pública;

5) Definir la infraestructura de información crítica y lo relativo al Centro Nacional de Ciberseguridad, así como sus atribuciones integración y funcionamiento;

6) Determinar los proveedores de servicios de ciberseguridad;

7) Describir la Estrategia Nacional de Ciberseguridad;

8) Tipificar los delitos en la materia; y,

9) Estipular los convenios internacionales en materia de ciberseguridad.

Conforme a lo anterior, es evidente que, con el surgimiento del Internet, nos enfrentamos a grandes y diversos desafíos, en dónde la implementación de la normativa aplicable siempre irá de la mano de las necesidades sociales, conforme a los principios generales del derecho.



Capítulo 3.
La identidad digital

Capítulo 3. La identidad digital

El uso de internet y de las redes sociales se ha convertido en una extensión de la vida tanto personal como profesional de las personas¹¹³, la interacción e interconexión en el mundo digital ha generado la creación de una representación digital del usuario, misma que se conforma por el conjunto de datos personales, atributos, acciones y actividades que realiza una persona en la red, es decir, su identidad digital.

La identidad digital ha ganado tanta importancia como la identidad física, implicando el reconocimiento de una persona en su vida diaria, su individualización y actuar en el uso de las nuevas tecnologías, lo cual se encuentra directamente vinculada con sus datos personales y su privacidad, trascendiendo a su reputación y vida diaria, sin embargo, han comenzado a suscitar diversos problemas y riesgos que acechan a la integridad de los usuarios.

Dicha representación no significa necesariamente que sea un reflejo de nosotros mismos, incluso que constituya una identidad completa, lo anterior, es así toda vez que mediante el uso de las nuevas tecnologías se permite seleccionar ciertos atributos e información para conformar la identidad digital, concediendo hacer uso de dicha identidad para contextos diferentes.

Ante ello, es clara la problemática que pretendemos analizar, en particular, es respecto a la acreditación y verificabilidad de la identidad de los sujetos en la red, resultando necesario contar con reglas, procedimientos y componentes técnicos que implementen una política de organización relacionada con el establecimiento, uso e intercambio de información de una identidad digital,¹¹⁴ lo anterior, fomentando una cultura de legalidad sobre los usuarios y su identidad en la red.

Para tener una noción sobre la importancia de la identidad digital, a medida que las tecnologías crecen y evolucionan, la cantidad de información personal que poseen las empresas sobre los usuarios en línea ha aumentado exponencialmente

¹¹³Morales Sandoval Miguel Ángel, "Nuestra identidad digital después de la muerte", *Revista Hechos y Derechos*, Instituto de Investigaciones Jurídicas UNAM, Número 58, julio-agosto 2020.

¹¹⁴ OCDE, *The Role of Digital Identity Management in the Internet Economy: A Primer for Policy Makers*, Documentos sobre economía digital, núm. 160, 2009.

también. De hecho, según IBM, el 90% de todos los datos del mundo se han creado en los últimos años.¹¹⁵

Aunado a lo anterior, también se analiza un nuevo reto que enfrentamos, al momento de tratar de determinar que sucede con ese “ser digital” después de la muerte del individuo, como la ha llamado el Dr. Guillermo Tenorio “la muerte digital”, toda vez que, al fallecer el titular de esa identidad digital, los contenidos digitales continuaran vinculados a la persona y activos en la red, incluso el Dr. Tenorio, los denomina un patrimonio multimedia, es decir, “nuestro legado digital”¹¹⁶, está situación la analizaremos más adelante.

3.1. ¿Qué es la identidad digital?

La identidad digital, no es más que la versión en Internet de la identidad física de una persona. Está compuesta por una gran cantidad de datos personales que proporcionamos en la red, más allá de nuestro correo electrónico y dirección, ella puede incluir aquella información que nos haga identificables, es decir, nuestros datos personales, imágenes, contraseñas, datos bancarios, preferencias y actividad en la red, entre otros.¹¹⁷

Cuando hablamos de identidad digital, debemos ubicarnos en las últimas décadas, en donde se ha consumado una revolución tecnológica que ha dando paso al origen de la “Sociedad de la Información”¹¹⁸, definida por la generación, la gestión y el uso de datos¹¹⁹, dicha revolución gira en torno a las nuevas tecnologías de la información y comunicación (TIC). En ese sentido, al hablar de identidad digital podemos comprenderla como aquella versión en la red sobre la identidad de una

¹¹⁵ IBM, *Diez tendencias clave de marketing para 2017*, recuperado de: <https://www01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=WRL12345USEN> (consultado en diciembre 2020)

¹¹⁶ Tenorio Cueto Guillermo A., *La muerte digital, Desafíos de la protección de datos de las personas fallecidas*, Conferencia IDAIP Quintana Roo, 25 de septiembre de 2020. Recuperado de: http://www.idaipqroo.org.mx/archivos/institucion/capacitacion/pdf/2020/conferencia_muerte_digital_desafios_proteccion_de_datos_de_personas_fallecidas.pdf (consultado en diciembre de 2020)

¹¹⁷ Álvarez Carmen, *Identidad digital: ¿Qué es y cómo protegerla?*, BBVA Research, Regulación financiera, marzo, 2018. Recuperado de: <https://www.bbva.com/es/identidad-digital-protegerla/> (consultado en noviembre de 2020)

¹¹⁸ Cumbre Mundial sobre la Sociedad de la Información (CMSI). Ginebra 2003 y Túnez 2005. Recuperado de: <http://www.itu.int/net/wsis/basic/index-es.html> (consultado en febrero de 2021)

¹¹⁹ Castells Manuel, *La revolución de la tecnología de la información*, Barcelona: UOC, 2003, p.p. 61–113.

persona, es decir, su representación y reconocimiento digital como individuo y usuario, lo cual permite hacerlo identificable en el uso de las nuevas tecnologías, como lo es el Internet.

El concepto de identidad digital ha sido abordado a partir de diversas perspectivas, como, por ejemplo, para la Doctora Estela Santos Díaz¹²⁰, cuando hablamos de identidad digital, se puede hacer referencia a dos aspectos diferentes: “uno basado en lo tangible material y otro fundamentado en la *autoadscripción*.”

Conforme a lo anterior, la Doctora Santos, comprende como identidad digital “tangible”, entendida como: “a los datos personales que introducimos en el mundo online y que nos identifican instrumentalmente: los datos bancarios, contraseñas, fechas de nacimiento o códigos. Estos datos pueden facilitar la monitorización o la extracción de información del individuo por parte de terceros”, por otro lado, se encuentra la identidad digital “autorrepresentativa”, la cual es creada por los propios usuarios y se genera en espacios de la red, como pueden ser a través de las redes sociales, para dicho prototipo de identidad, la Doctora Santos, indica que “en estos espacios generan formas del “yo” autoconstruidas, públicas y gestionadas por el individuo.”, las cuales pueden variar a la realidad.

Conforme a lo anterior, diversas instituciones y organizaciones internacionales han tratado de conceptualizar a la identidad digital, entendiéndola como:

- ✓ La Unión Internacional de Telecomunicaciones (UIT) define la identidad digital como una "representación digital de la información conocida sobre un determinado individuo, grupo u organización."¹²¹
- ✓ La Organización Internacional de Normalización (ISO) establece que la identidad digital es un "elemento dentro o fuera de un sistema de tecnología de la información y la comunicación, como una persona, una organización,

¹²⁰ Santos Díaz, “Construcción de la identidad digital a través del yo-objeto: proceso de auto-objetivación y su relación con la cosificación del cuerpo de las mujeres” *Revista E. Teknokultura*, No. 15 (2), 2018, p.p. 301-309.

¹²¹ International Telecommunication Union (ITU). *Baseline identity management terms and definitions. Recommendation*, ITU-T X.1252, 2010. Recuperado de: http://www.itu.int/SG-CP/example_docs/ITU-T-REC/ITU-TREC_E.pdf (consultado en enero de 2020)

un dispositivo, un subsistema o un grupo de tales elementos, que tiene una existencia reconociblemente distinta.”¹²²

- ✓ Asimismo, el Foro Económico Mundial, en el año 2016 definió a la identidad digital como una "colección de atributos individuales que describe una entidad y determinar las transacciones en las que esa entidad puede participar.”¹²³

Al respecto, el concepto de identidad digital se encuentra íntimamente ligado con la llamada “reputación online”, la cual, según el Instituto Nacional de Tecnologías de la Comunicación de España, conceptualiza como la opinión o consideración social que otros usuarios tienen de la vivencia online de una persona o incluso una organización.¹²⁴

La identidad en el entorno físico, o identidad analógica, se ha venido basando tradicionalmente en la asignación e inscripción registral de unos determinados datos y su acreditación mediante documentos físicos seguros, con carácter oficial y exclusivo.¹²⁵

La identidad digital es, en contraste, un concepto muy amplio, enfocado en la vivencia de los ciudadanos en la Red, que incluye las funciones de la identidad analógica, y las supera, debido a las nuevas posibilidades que ofrece.¹²⁶

De forma progresiva, la identidad analógica y la identidad digital forman parte de una misma realidad, en la que no se distingue entre la actuación realizada en el mundo físico y en la Red, de forma que se puede hablar de convergencia hacia la identidad híbrida.¹²⁷

3.2. Reconocimiento de la identidad digital

En la actualidad, como lo hemos mencionado con anterioridad, derivado del incremento en el desarrollo de las nuevas tecnologías, la propagación de

¹²² ISO/IEC 24760-1:2019. *IT Security and Privacy — A framework for identity management — Part 1: Terminology and concepts.*

¹²³ World Economic Forum, *A Blueprint for Digital Identity. The Role of Financial Institutions in Building Digital Identity*, Part of the Future of Financial Services Series, 2016. p. 41.

¹²⁴ INCIBE, “Ciberseguridad en la identidad digital y la reputación online: una guía de aproximación para el empresario”, *Identidad y Reputación*, 2016, p. 5.

¹²⁵ *Ibidem*, p. 7.

¹²⁶ *Idem*.

¹²⁷ *Idem*.

información a través de Internet, el acceso a las redes sociales y la interconexión en general, nos vemos en la necesidad de regular y proteger, entre otras cuestiones a la figura de identidad digital.

Al respecto, el uso y aprovechamiento de estas nuevas tecnologías nos llevan, por un lado, a obtener un beneficio y ahorro para el intercambio de información, incluidos los datos personales de los usuarios, y, por otro lado, se intenta comprender y en su caso controlar, el posible impacto en la seguridad y privacidad de los mismos.

La identidad digital es la nueva frontera de la privacidad y la seguridad, pues derivado al incremento en el uso de las tecnologías de la información y la comunicación (TIC), los usuarios se encuentran en una situación de vulnerabilidad donde el titular pierde el control en el uso que se hace de su información personal.

Bajo ese contexto, se ha buscado el efectivo ejercicio del derecho de autodeterminación informativa, el cual, radica en la potestad que tiene un titular para decidir cuáles de sus datos proporciona a un tercero, asimismo, el derecho en cuestión busca proteger la identidad del individuo, máxime en el desarrollo y uso de las nuevas tecnologías, en dónde con el desarrollo de la identidad digital existe un intercambio de información personal sin restricciones y cuya recopilación masiva puede poner en riesgo el libre desarrollo de la personalidad, vulnerando diversos derechos humanos y el respeto a la dignidad humana.¹²⁸

Actualmente, para el efectivo ejercicio del derecho a la autodeterminación informativa, la protección de datos personales y la salvaguarda de la identidad digital, es necesario la intervención de diversos elementos, como por ejemplo, la inclusión de una responsabilidad proactiva¹²⁹, a partir del usuario, así como la inserción de una cultura de legalidad, pero sobre todo la implementación de una

¹²⁸ SCJN. Tesis 1a. CCCLIV/2014. DIGNIDAD HUMANA. CONSTITUYE UNA NORMA JURÍDICA QUE CONSAGRA UN DERECHO FUNDAMENTAL A FAVOR DE LAS PERSONAS Y NO UNA SIMPLE DECLARACIÓN ÉTICA. Gaceta del Semanario Judicial de la Federación. Décima época. Tomo I, octubre, 2014, p. 602.

¹²⁹ *Diccionario de Protección de Datos Personales. Conceptos Fundamentales*, Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI), Primera edición, noviembre de 2019, p. 85.

ética aplicable para todos los que intervienen en el tratamiento, todo esto con el objetivo de realizar un lícito tratamiento de la información personal.¹³⁰

La identidad digital en nuestros días constituye una gran preocupación, toda vez que cada vez se expone a los usuarios ante posibles intromisiones a su privacidad y al tratamiento intensivo de datos personales, dejando vulnerable a los titulares. Ante dicha situación y conforme a los nuevos retos que hay que enfrentar en materia de protección de datos personales, existe un debate en el cual se cuestiona sobre la eficacia y suficiencia de los diversos instrumentos normativos, para garantizar la protección de la identidad digital y salvaguardar la dignidad de las personas. En este sentido, el supervisor europeo de protección de datos ha reconocido que urge considerar la ética y la posición de la dignidad humana en las tecnologías del futuro y evaluar si las tendencias actuales requerirán de un nuevo enfoque.¹³¹

Bajo ese contexto, el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, ha generado una serie de recomendaciones para mantener segura nuestra privacidad y datos personales en el entorno digital, entre dichas recomendaciones se encuentran las siguientes:

¹³⁰ *Idem*

¹³¹ Dictamen 4/2015. "Hacia una nueva ética digital: Datos, dignidad y tecnología", *Supervisor Europeo de Protección de Datos*. Septiembre, 2015.

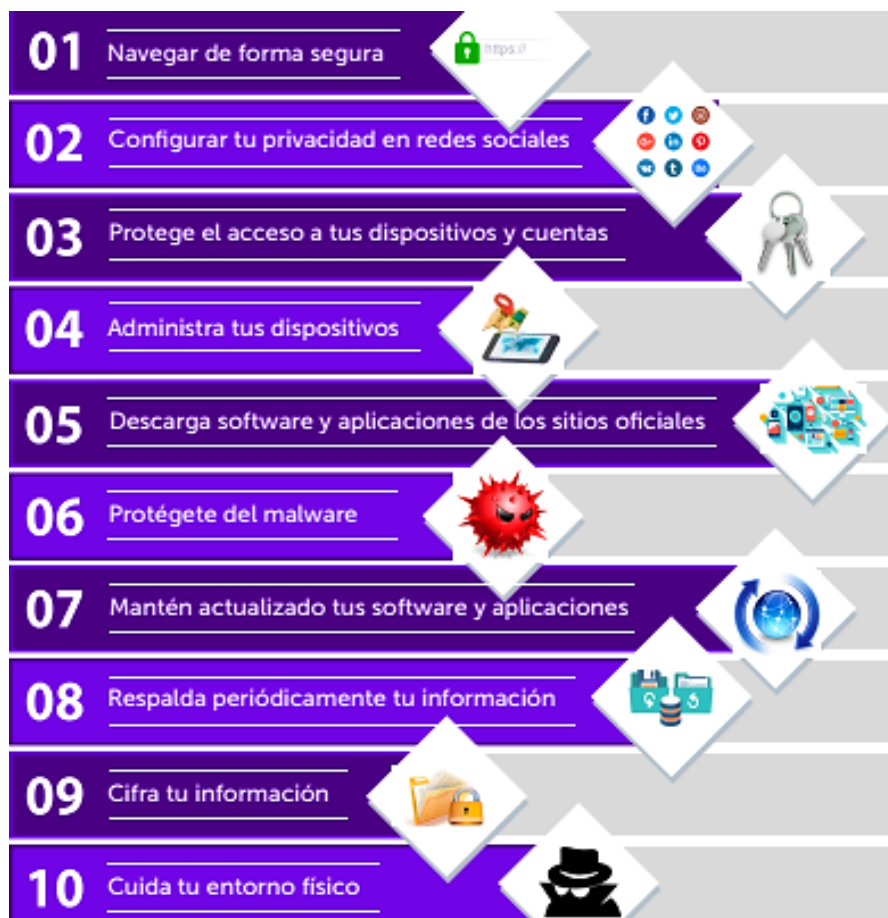


Figura 7. 10 ejes principales de las recomendaciones en el entorno digital.

Fuente: INAI.¹³²

Lo anterior, resulta nuestro argumento toral, toda vez que la problemática que se analiza en el presente estudio, radica en la falta de una cultura de legalidad en los usuarios sobre su identidad digital, ya que si se promoviera, se ayudaría a sensibilizar a los usuarios, quienes podrían desarrollar una noción más educada y consiente sobre su identidad digital, pues como lo hemos visto con antelación, el desarrollo de la identidad dentro del entorno digital se ha vuelto una rutina diaria y habitual en los seres humanos, desde el simple hecho de buscar información, como una herramienta de comunicación, así como realizar actividades económicas o bancarias.

¹³² INAI, *Recomendaciones para mantener segura nuestra privacidad y datos personales en el entorno digital*, Marzo, 2018.

De forma particular, podemos conocer que actualmente los usuarios de internet en México principalmente realizan las actividades siguientes:



Figura 8. Usuarios de internet en México, Fuente: We are social e INEGI.¹³³

Al respecto, según cifras calculadas por Estadística Digital, y la Asociación de Internet.MX, con base en información disponible de Consejo Nacional de Población, el Instituto Nacional de Estadística y Geografía e Instituto Federal de Telecomunicaciones. Actualmente se calcula que 82 millones 700 mil mexicanos acceden a Internet en México.¹³⁴

¹³³ *Periódico Milenio*, "Hottsuite, We are social e INEGI", Información: Lenina Ramos, Gráficos: Luis Moor. México, marzo, 2021.

¹³⁴ Asociación de Internet.MX, *6° Estudio sobre los Hábitos de los Usuarios de Internet en México 2020*, Enero 2021, recuperado de: <https://irp-cdn.multiscreensite.com/81280eda/files/uploaded/16%20Estudio%20sobre%20los%20Ha%CC%81bitos%20de%20los%20Usuarios%20de%20Internet%20en%20Me%CC%81xico%202020%20versi%20o%CC%81n%20pu%CC%81blica.pdf> (consultado en enero 2021)

Bajo ese contexto, para conocer las actividades más habituales de los usuarios en internet, la Asociación de Internet.MX, realizó un estudio en 2020, a través del cual se denota que en México aumentó significativamente la mayoría de las actividades digitales, ganando terreno: mail, comercio electrónico y la banca, sin embargo, transporte decrece debido al confinamiento, tal como lo muestra a continuación:¹³⁵

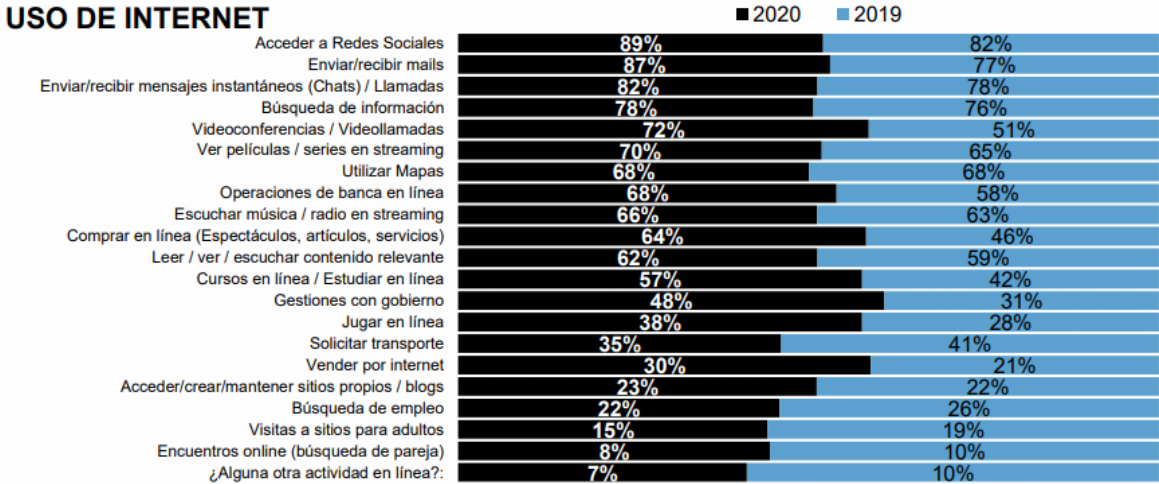


Figura 9. 6° Estudio sobre los Hábitos de los Usuarios de Internet en México 2020. Fuente: Asociación de Internet.MX.¹³⁶

Con ello, podemos generar una noción muy general del cómo y dónde se desarrolla la identidad digital de los usuarios en México.

3.3. Atribuciones de la identidad digital.

Una vez visto lo anterior, y para conocer más sobre los atributos de la identidad digital, mediante un estudio desarrollado por el Foro Económico Mundial (2016), se procedió a identificar tres elementos atribuibles a la identidad digital, mismos que se describen a continuación para mejor referencia:

| | Para las personas físicas | Entidades jurídicas | Para los bienes |
|-----------------------------|--|---|---|
| ATRIBUTOS INHERENTES | <ul style="list-style-type: none"> Edad Altura | <ul style="list-style-type: none"> Industria Estado del negocio | <ul style="list-style-type: none"> Naturaleza del activo |

¹³⁵ *Ibidem*, p. 13.
¹³⁶ *Idem*.

| | Para las personas físicas | Entidades jurídicas | Para los bienes |
|---|--|--|--|
| <p>atributos que son intrínsecos a una entidad y no se definen por su relación con entidades externas.</p> | <ul style="list-style-type: none"> • Fecha de nacimiento • Huellas dactilares | | <ul style="list-style-type: none"> • Emisor de activos |
| <p>ATRIBUTOS ACUMULADOS atributos que se recogen o desarrollado a lo largo del tiempo. estos atributos pueden cambiar varias veces o evolucionar a lo largo de la vida de una entidad.</p> | <ul style="list-style-type: none"> • Registros de salud • Preferencias y comportamientos | <ul style="list-style-type: none"> • Registro de negocios • Registro legal | <ul style="list-style-type: none"> • Historia de la propiedad • Historia de la transacción |
| <p>ATRIBUTOS ASIGNADOS atributos que se adjuntan a la entidad, pero no están relacionados con su naturaleza intrínseca. estos atributos pueden cambio y en general son</p> | <ul style="list-style-type: none"> • Número de identificación nacional • Número de teléfono • Dirección de correo electrónico | <ul style="list-style-type: none"> • Número de identificación • Jurisdicción legal | <ul style="list-style-type: none"> • Número de identificación • Tutela / Custodia |

| | Para las personas físicas | Entidades jurídicas | Para los bienes |
|---|------------------------------|------------------------|-----------------|
| reflejo de las relaciones que esa entidad mantiene con otros. | | | |

Cuadro 2. Atributos que constituyen la Identidad. Fuente: Elaboración propia.¹³⁷

Conforme a lo anterior, podemos afirmar que una identidad digital es una colección de atributos de identidad capturados y almacenados electrónicamente que describen a una persona dentro de un contexto dado y se utilizan para transacciones electrónicas, incidiendo en la representación digital de la persona en la red.

Una identidad digital se refiere a los sistemas y procesos que gestionan el ciclo de vida de las identidades digitales individuales. La identidad digital de una persona puede estar compuesta por una variedad de atributos, incluidos datos personales, preferencias, redes sociales, entre otras actividades que pueda un individuo generar en la red.

Cuando estos datos se recopilan y verifican, se pueden utilizar para identificar una persona y su presencia en Internet, generando una “reputación” en la red.¹³⁸

Para el Instituto Nacional de Tecnologías de la Comunicación Español¹³⁹, la identidad digital presenta una serie de propiedades, identificadas por la OCDE¹⁴⁰, mismas que se enlistan a continuación para mejor referencia:

- *La identidad digital es esencialmente social.* A medida que el individuo proyecta su personalidad en la Red, especialmente en las redes sociales, sus vecinos digitales le caracterizan y reconocen de forma efectiva,

¹³⁷ World Economic Forum, *A Blueprint for Digital Identity, The Role of Financial Institutions in Building Digital Identity*, 2016.

¹³⁸ INCIBE, “Ciberseguridad en la identidad digital y la reputación online: una guía de aproximación para el empresario”, *Identidad y Reputación*, 2016.

¹³⁹ INTECO, *Guía para usuarios: identidad digital y reputación online*, 2012, p. p. 7-8.

¹⁴⁰ Rundle, M.; Trevithick, P. *At a crossroads: ‘Personhood’ and digital identity in the information society*, Directorate for Science, Technology and Industry, STI Working Paper 2007/7, OECD, 2008.

incluso en ocasiones en que no se ha producido una verificación presencial de la identidad.

- *La identidad digital es subjetiva.* Tanto la percepción del “yo” como del “nosotros” están basadas en la experiencia que personas diferentes construyen y que les permiten reconocerse.
- *La identidad digital es valiosa.* La propia actividad de los sujetos genera capital informacional que puede ser empleado para establecer relaciones personalizadas y para tomar decisiones en las relaciones con las personas, con un mayor grado de confianza.
- *La identidad digital es referencial.* De hecho, una identidad no es una persona o un objeto, sino una referencia a dicha persona u objeto.
- *La identidad digital es compuesta.* Mientras que algunas informaciones son suministradas de forma voluntaria por los propios usuarios, otras informaciones sobre los mismos son construidas por terceros, sin la participación del sujeto en cuestión.
- *La identidad digital produce consecuencias.* La divulgación de la información en ocasiones puede generar efectos, y en otros casos, es la no divulgación la que constituye una amenaza por sí misma.
- *La identidad es dinámica.* porque se encuentra en cambio y modificación permanente. Especialmente en Internet, la identidad digital se debe ver como un flujo de informaciones, en lugar de como una foto fija de una persona.
- *La identidad es contextual.* Dado que la divulgación de la información puede generar un impacto negativo empleada en un contexto erróneo, o sencillamente ser irrelevante, mantener las identidades segregadas entre sí permite tener más autonomía.

En relatadas condiciones, el mismo Instituto Nacional de Tecnologías de la Comunicación, considera que la identidad digital se compone por los rasgos de identidad se suelen encontrar agrupados o relacionados entre ellos, formando identidades parciales, es decir, las personas físicas utilizan diferentes identidades parciales en función de los diferentes roles y actividades que desarrollan a lo largo

de su existencia online. Cada identidad parcial está sustentada en un servicio o aplicación de Internet.¹⁴¹

Así, por ejemplo, un usuario mantiene sus perfiles en *Facebook*, *Twitter* y *LinkedIn*, participa con el mismo alias en distintos foros de profesionales, gestiona un blog de viajes y aparece ocasionalmente en prensa y webs especializadas, relacionadas con su ámbito profesional. Todo ello conforma la identidad digital del sujeto, pero cada uno de los servicios mencionados sustenta una identidad parcial, que puede aparecer relacionada o no con el resto de su presencia en la red. La vivencia online, esto es, la suma de las diferentes identidades parciales permite construir una identidad digital: una imagen de la persona en Internet.¹⁴²

3.4. Sistemas de identificación digital.

Uno de los retos a los que se enfrenta la identidad digital es su pleno reconocimiento y autenticación, elementos que se pueden realizar a través de un sistema de identificación que permita identificar al usuario, facilitando y agilizando la ejecución de diversos procesos, otorgando la digitalización del usuario en todas sus actividades que realiza a través de la red, sin embargo, los mismos depende de la captura de la información y datos que proporcionen los mismos usuarios para su efectividad.

Los sistemas de identificación digital recopilan y ayudan a validar los atributos de identidad para determinar y verificar la identidad de una persona, emitiendo una prueba de esa identidad, ya sea en forma de credencial, por ejemplo, un número de identificación único, un usuario, un certificado, entre otros instrumentos.¹⁴³

Dichos instrumentos de identificación pueden ser utilizados por la persona a través de algún método de autenticación, por ejemplo, mediante el uso de contraseñas, incluso de doble verificación o a través de una firma electrónica, ante

¹⁴¹ INTECO, *Guía para usuarios: identidad digital y reputación online*, 2012, pág. 9.

¹⁴² *Idem*

¹⁴³ Banco Mundial, *Sistemas de identificación digitales fiables e inclusivos pueden abrir oportunidades para las personas más vulnerables del mundo*, Recuperado de: <https://www.bancomundial.org/es/news/immersive-story/2019/08/14/inclusive-and-trusted-digital-id-can-unlock-opportunities-for-the-worlds-most-vulnerable>, (consultado en diciembre 2020)

los sectores que requieran cierta seguridad para acreditar fehacientemente quiénes son.¹⁴⁴

Para que los sistemas de identificación estén en posibilidad de acreditar la identidad de un sujeto, efectúan un análisis de los atributos personales, con el objetivo de responder una o más de las preguntas siguientes:¹⁴⁵

1. ¿Quién eres?
2. ¿Eres quien dices ser?
3. ¿Está autorizado o es elegible para algo?

Estas tres preguntas resultan fundamentales para la prestación de servicios de identificación digital, así como el cumplimiento de derechos y obligaciones.

En algunos casos, el mismo sistema de identificación utilizado para la identificación y autenticación puede proporcionarla información necesaria para la autorización o la determinación de elegibilidad. En muchos otros casos, las partes que confían deben ingresar información adicional que está más allá del alcance del sistema de identificación en sí para permitir dicha verificación.¹⁴⁶

Estos sistemas de identificación pueden o no identificar de manera única a las personas dentro de un determinado sector, además se enfrentan a factores externos en dónde una persona reclama múltiples identidades dentro el sistema o en su caso cada identidad solo es reclamada por una persona.

En general, los más fundamentales de los sistemas de identificación funcional están pensados para ser únicos. Sin embargo, algunos pueden tener registros menos confiables debido a la duplicación o generación de identificadores no únicos, por ejemplo, ante la presencia de homónimos, identidades falsas, el reciclaje de números de identificación o incluso procedimientos de prueba de identidad débiles.¹⁴⁷

¹⁴⁴ *Idem*

¹⁴⁵ Banco Mundial, *Guía para profesionales que trabajan en el área de la ID4D*, 2019, p. 11, recuperado de: <https://id4d.worldbank.org/guide>, (consultado en diciembre 2020)

¹⁴⁶ *Ibidem*, p. 12.

¹⁴⁷ *Ibidem*, p. 14.

3.5. Identidad digital y las redes sociales.

Según la Real Académica Española, una red social es un: “servicio de la sociedad de la información que ofrece a los usuarios una plataforma de comunicación, a través de internet para que estos generen un perfil con sus datos personales, facilitando la creación de comunidades con base en criterios comunes y permitiendo la comunicación de sus usuarios, de modo que pueden interactuar mediante mensajes, compartir información, imágenes o vídeos, permitiendo que estas publicaciones sean accesibles de forma inmediata por todos los usuarios de su grupo.”¹⁴⁸

La popularidad de las redes sociales en Internet se ha incrementado exponencialmente en los últimos años, convirtiéndose en un medio de comunicación que ha despertado el interés no sólo de los jóvenes, sino de toda la población en general.¹⁴⁹

Como lo hemos mencionado con antelación, el Internet constituye una herramienta que ha permitido la interconexión de las personas en la era digital, y sobre este aspecto en particular, dicho crecimiento a trascendido a partir del avance tecnológico para alcanzar una dimensión social que ha marcado las redes sociales.

Alrededor de 3,810 millones de personas en el mundo utilizan las redes sociales, según el último informe de “Data Reportal”¹⁵⁰. Es casi la mitad de la población del planeta, que cuenta actualmente con casi 7,800 millones de personas, según “Worldometers”¹⁵¹. Hasta el año 2020, la más popular sigue siendo “Facebook” con 2,498 millones, seguida con 2.000 millones por “WhatsApp” y “YouTube”, tal y como se muestra en la gráfica siguiente:

¹⁴⁸ *Diccionario de la lengua española*, 23 ed., [versión 23.3 en línea]. Disponible en: <https://dle.rae.es> (consultado en febrero de 2021).

¹⁴⁹ García Ricci Diego, *El derecho a la privacidad en las redes sociales en internet*, Instituto de Investigaciones Jurídicas, UNAM, México, p. 183.

¹⁵⁰ Véase: <https://datareportal.com/reports/digital-2021-global-overview-report> (consultado en febrero de 2021).

¹⁵¹ Véase: <https://www.worldometers.info/world-population/> (consultado en febrero de 2021).

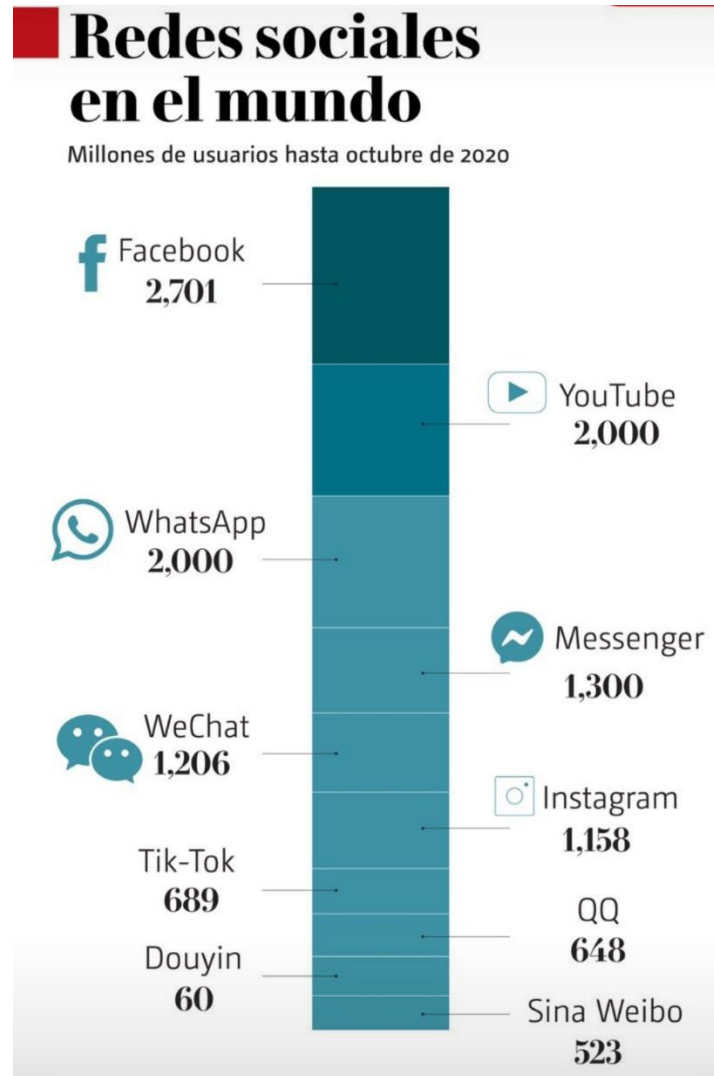


Figura 10. Redes sociales en el mundo. Fuente: We are social e INEGI.¹⁵²

Al respecto, en México, conforme a la Encuesta Nacional sobre Disponibilidad y Uso de Tecnologías de la Información en los Hogares (ENDUTIH) elaborada por el Instituto Nacional de Estadística y Geografía (INEGI) en mayo de 2019, se observa que las principales actividades realizadas en Internet durante 2019 son: para entretenimiento (91.5%), para obtener información (90.7%) y para comunicarse (90.6%). Otras como para acceder a redes sociales y para apoyar la educación/capacitación, registran porcentajes del 87.8% y el 83.8%, respectivamente.

¹⁵² *Periódico Milenio*, "Hottsuite, We are social e INEGI", Información: Lenina Ramos, Gráficos: Luis Moor. México, marzo, 2021.

Como podemos observar, cada vez son más los individuos que eligen a las redes sociales como medio efectivo para comunicarse con el resto de la sociedad, pues la facilidad de conexión, la inmediatez y la generalización dentro de una red social, ha llevado a generar nuevos modelos de expresión y comunicación entre los usuarios, ya que el uso de estas herramientas posibilita por un lado exponer y exponerse de manera distinta a como lo haría en la realidad.¹⁵³

Uno de los aspectos que debemos tomar en cuenta y que la implementación de las redes sociales ha permitido es la materialización de una nueva identidad del usuario, ya sea de forma real o ficticia, ya que con el uso de este medio de comunicación se posibilita una socialización sin fronteras, a través de la cual, no resulta necesario conocer al interlocutor original.¹⁵⁴

Como previamente analizamos, la conformación de la identidad en la vida cotidiana surge a partir del registro oficial y reconocimiento del Estado, mediante la emisión de documentos oficiales, mientras que en el ámbito digital, específicamente por cuanto hace en el ámbito de las redes sociales se construye a través del conjunto de informaciones publicadas en Internet sobre nosotros y que componen la imagen que los demás tienen de nosotros, incluyendo, datos personales, imágenes, noticias, comentarios, gustos, amistades, aficiones, preferencias, entre otros. Todos estos datos nos describen en Internet ante los demás y determinan nuestra reputación digital, es decir, la opinión que los demás tienen de nosotros en la red.¹⁵⁵

De lo anterior, podemos determinar que la identidad digital que se crea a través de una red social, genera una reputación la cual se encuentra conectada a la dignidad personal, el control de la imagen personal, al honor y a la intimidad de los individuos,¹⁵⁶ pues como coloquialmente se dice sobre el uso de las redes sociales

¹⁵³ “La desigualdad de género y el sexismo en las redes sociales. Una aproximación cualitativa al uso que hacen de las redes sociales las y los jóvenes de la CAPV”, *Colección Gazteak Bilduma*, Gobierno Vasco, 2013.

¹⁵⁴ *Idem*.

¹⁵⁵ Gobierno de Canarias, “¿Qué es la identidad digital”, Consejería de Educación y Universidades, recuperado de: <https://www3.gobiernodecanarias.org/medusa/ecoescuela/seguridad/identidad-digital-profesorado/que-es-la-identidad-digital/> (consultado en febrero de 2021).

¹⁵⁶ INCIBE, “Ciberseguridad en la identidad digital y la reputación online: una guía de aproximación para el empresario”, *Identidad y Reputación*, 2016, p. 13.

“Uno es lo que publica, cuándo lo publica y cómo lo publica”¹⁵⁷, por lo que a partir de este concepto, al momento de compartir nuestra información, fotos, comentarios, videos y demás actividad en la red, se configura nuestra identidad en el plano digital.

Por su propia naturaleza, las redes sociales son espacios de comunicación, dónde el intercambio de información resulta indispensable, sin embargo, el nivel de detalle de los datos personales intercambiados varía según el sitio web que se utilice, pero en una práctica generalizada la presentación del individuo se efectúa mediante la creación de un perfil, el cual incluye el nombre real o el pseudónimo del usuario, así como la red de sus contactos (conocidos o no).¹⁵⁸

Los perfiles también pueden contener otro tipo de información personal como la fotografía del usuario, lugares de estudio o trabajo, preferencias políticas o sexuales, gustos musicales o literarios, estado civil, edad, *hobbies* e intereses, dirección de correo electrónico e incluso domicilio, incluyendo la geolocalización real y hasta números telefónicos.¹⁵⁹

Visto lo anterior, una de las encrucijadas entre las que se encuentra el derecho a la privacidad, entendido como aquel derecho que tiene todo individuo de sustraer aspectos de su vida privada del escrutinio público, y que previamente hemos analizado, nos lleva a preguntarnos, ¿Cómo hemos llegado a la exposición de nuestra privacidad en las redes sociales?, al respecto Gross y Acquisti, explican la compleja relación que existen entre ambas:¹⁶⁰

“La relación entre la privacidad y la red social de una persona es multifacética. En ciertas ocasiones queremos que información nuestra sólo sea del conocimiento de un pequeño círculo de amigos cercanos y no de extraños. En otras, buscamos revelar información personal a anónimos extraños, pero no a aquellos que nos conocen mejor.”¹⁶¹

¹⁵⁷ INFOBAE, *Identidad digital: ¿quiénes somos en las redes sociales?*, recuperado de: <https://www.infobae.com/2012/07/02/656704-identidad-digital-quienes-somos-las-redes-sociales/> (consultado en febrero de 2021).

¹⁵⁸ García Ricci Diego, *El derecho a la privacidad en las redes sociales en internet*, Instituto de Investigaciones Jurídicas, UNAM, México, p. 192.

¹⁵⁹ *Idem*.

¹⁶⁰ *Ibidem*, p. 193.

¹⁶¹ Gross Ralph y Alessandro Acquisti, op. cit., supra nota 18, p.p. 2 y 3. Citado por: García Ricci Diego, “El derecho a la privacidad en las redes sociales en internet”, Instituto de Investigaciones Jurídicas, UNAM, México, p. 193.

Al respecto, podemos afirmar que de forma general solemos preservar nuestra privacidad y tener cierto cuidado en la divulgación de nuestros datos personales, sin embargo, en un ambiente virtual, como lo son las redes sociales, estas acciones suelen relajarse, a este comportamiento se el denomina como la “paradoja de la privacidad” (*privacy paradox*), mientras al individuo le preocupa el uso que se le pueda dar a su información personal, suponiendo una inminente preocupación sobre el mal uso que pudiera darse a sus datos personales al momento de difundirlo, en la práctica, es común encontrar que ese mismo individuo difunde descuidadamente e indiscriminadamente su información, a través de las redes sociales.¹⁶²

Por este motivo, la reputación online se relaciona directamente con la posibilidad de controlar la visibilidad de las propias vivencias digitales, de forma que, en su caso, sólo las personas autorizadas puedan acceder a las mismas.¹⁶³

Twitter, Facebook, Instagram, Snapchat, LinkedIn y otras muchas redes sociales funcionan como un escaparate de la vida de millones de personas. Sin embargo, aunque nos encanta compartir nuestras experiencias con nuestros contactos, debemos tener en cuenta que, si lo hacemos sin tomar una serie de precauciones, toda la información que publicamos puede terminar siendo accesible por otros usuarios de la red social, quienes si se lo propusieran podrían realizar una radiografía de nuestras vidas, y perjudicar nuestra identidad digital. Esta es una táctica muy utilizada por los ciberdelincuentes. Ellos utilizan nuestras publicaciones para conseguir información personal, suplantar identidades, robar credenciales o incluso chantajearnos pidiéndonos algo a cambio de no distribuir una imagen o publicación.¹⁶⁴

Una de las fórmulas más sencillas para controlar la reputación en línea es la gestión adecuada de la visibilidad de los perfiles en redes sociales. Se trata de un

¹⁶² Norberg Patricia, Horne Daniel y Horne David, “The Privacy Paradox, Personal Information Disclosure Intentions versus Behaviors”, *The Journal Of Consumer Affairs*, Vol. 41, núm. I, Estados Unidos de América, 2007, p. 101.

¹⁶³ INCIBE, “Ciberseguridad en la identidad digital y la reputación online: una guía de aproximación para el empresario”, *Identidad y Reputación*, 2016, p. 13.

¹⁶⁴ Iberdrola, “Redes sociales, ¡cuidado con lo que compartes!”, *Privacidad y Seguridad en Redes Sociales*, recuperado de: <https://www.iberdrola.com/innovacion/redes-sociales-privacidad-seguridad> (consultado en febrero de 2021).

primer paso, necesario, en la construcción de una identidad digital coherente con lo que el usuario desea comunicar sobre sí mismo.¹⁶⁵

Asimismo, el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, realiza 7 recomendaciones para proteger nuestros datos personales en las redes sociales:



Figura 11. Como proteger tus datos personales en las redes sociales.

Fuente: INAI.¹⁶⁶

3.6. Identidad digital y protección de datos personales.

Como previamente se ha conceptualizado, de manera enunciativa podemos afirmar que una identidad digital es una colección de información, datos personales y

¹⁶⁵ INCIBE, "Ciberseguridad en la identidad digital y la reputación online: una guía de aproximación para el empresario", *Identidad y Reputación*, 2016, p. 14.

¹⁶⁶ INAI, 23 de febrero de 2020, recuperado de: <https://twitter.com/inaimexico/status/1231806068541530113> (consultado en febrero 2021)

atributos de la identidad de un usuario, capturados y almacenados electrónicamente que describen a una persona dentro de un contexto dado y se utilizan para transacciones electrónicas, es decir, en el mundo digital.

La identidad digital de una persona puede estar compuesta por una variedad de atributos, incluidos datos personales, como lo son los datos biográficos: nombre, edad, sexo, dirección, entre otros, datos patrimoniales y financieros: número de cuentas bancarias, tarjetas de créditos, usuario de banca electrónica, y más, así como datos biométricos: huellas dactilares, escáneres de iris o huellas de manos, así como otros atributos que están más ampliamente relacionados con lo que realiza la persona, datos laborales y profesionales, correos electrónicos o redes sociales.

Cuando estos datos se recopilan y verifican, se pueden utilizar para identificar a una persona respondiendo la pregunta "¿Quién eres?", asimismo, estos atributos, junto con las credenciales emitidas por el proveedor de servicios como contraseñas, usuarios, número de identificación único, documento electrónico o identificación electrónica, coadyuvan como factores de autenticación para responder a la pregunta "¿Es usted quien dice ser?".¹⁶⁷

Bajo ese contexto, como se analizó con antelación, los sistemas de identificación digital pueden respaldar múltiples objetivos de desarrollo de la identidad digital, sin embargo, también pueden crear diversos riesgos para la privacidad y la protección de datos digitales, sí bien estos riesgos son inherentes a cualquier sistema de identificación, la digitalización puede elevar su escala y frecuencia.¹⁶⁸

De forma general los sistemas de identificación digital plantean una preocupación sobre la privacidad de los datos personales que recopilan, basándose en el cumplimiento de la normatividad y estableciendo esquemas de buenas prácticas para la protección de datos personales.

¹⁶⁷ Banco Mundial, *Identificación para el marco estratégico de desarrollo*, documento de trabajo, Washington D. C., 2016, p.p. 11-12.

¹⁶⁸ Banco Mundial, *Impactos económicos de los sistemas de identificación en el sector privado*, Washington, D. C. 2018, recuperado de: <http://id4d.worldbank.org/research> (consultado en diciembre 2020)

Sin embargo, la red está llena de riesgos que pueden tener consecuencias graves y a menudo irreparables, para las personas y, por lo tanto, requieren una protección adecuada, incluyendo métodos legales, operativos y técnicos que permitan que los datos personales compartidos o procesados mantengan su confidencialidad en todo momento, lo cual resulta fundamental para garantizar la privacidad de las personas.

Conforme a lo anterior, el Banco Mundial¹⁶⁹, considera que los datos y la privacidad relacionados con la información personal se encuentran vulnerables y algunas veces en peligro en la red, enfatizando que cualquier actividad que recopile, almacene o procese datos personales, puede enfrentarse a los riesgos siguientes:

- *Brechas de seguridad*: consistente en ataques físicos o ciberataques a datos en tránsito o en reposo.
- *Divulgación no autorizada*: transferencia inapropiada de datos entre agencias gubernamentales, gobiernos extranjeros, empresas privadas u otros terceros.
- *Exposición de información personal confidencial*: divulgar información personal confidencial, como, por ejemplo: Biometría, religión, origen étnico, género, historial médico, los cuales constituyen de forma particular datos personales de carácter sensible, mismos que pueden ser utilizados para fines no autorizados.
- *Función furtiva*: el uso (e incluso el intercambio) de datos para fines más allá de aquellos para los que se dio el consentimiento.
- *Robo de identidad*: el robo de identidad en el mundo digital puede tener consecuencias que son al menos tan graves como las del mundo físico y, dada la naturaleza global y descentralizada de Internet, daños que a menudo son más difícil de reparar. En un mundo digitalizado, cualquier persona puede realizar la suplantación de identidad.¹⁷⁰

¹⁶⁹ Banco Mundial, *Combatir la ciberdelincuencia: herramientas y creación de capacidad para economías emergentes*, Washington, D. C., 2017, recuperado de: <http://www.combattingcybercrime.org/> (consultado en diciembre 2020)

¹⁷⁰ Gercke, Marco, *Robo de identidad relacionado con Internet*, documento de debate del Consejo de Europa. 2007, recuperado de: <https://rm.coe.int/16802fa3a0> (consultado en noviembre 2020)

- *Riesgos de vigilancia*: la capacidad de correlacionar la información de identificación en las bases de datos, como, por ejemplo, a través del reconocimiento facial, aumenta los riesgos de vigilancia, especialmente cuando se trata de biometría¹⁷¹, información que se caracteriza por ser universal, única, permanente, irrepetible y medible de forma cuantitativa,¹⁷² por lo que su tratamiento requiere de medidas de seguridad especiales para garantizar la protección de los titulares.
- *Discriminación o persecución*: los atributos de identidad pueden usarse para discriminar o perseguir a personas de forma particular o grupos, asimismo, pueden originar un trato injusto, al contar con datos incompletos o inexactos que pueden dar lugar a errores o tratos injustos.

La red se encuentra repleta de riesgos y los sistemas de identificación digital se encuentran aún más vulnerables que los sistemas tradicionales basados en papel toda vez que puede permitir:

- *Violaciones de seguridad de datos masivas*: la consolidación y almacenamiento de datos aumenta el impacto de las vulneraciones hacia las bases de datos, siendo un objetivo de ataque más atractivo,¹⁷³ generando la necesidad de contar con las medidas de ciberseguridad necesarias para su debida protección y resguardo.
- *Destrucción de registros digitales*: la digitalización permite la eliminación fácil o masiva de datos, como cualquier persona que haya borrado la información de su teléfono. Sin las salvaguardas de datos adecuadas, registros completos, los usuarios podrían "desaparecer". Por ejemplo, en la atención médica, el uso de registros médicos electrónicos (EHR) ha

¹⁷¹ Barbero, Gregory, *San Francisco prohíbe el uso de tecnología de reconocimiento facial por parte de la agencia*, Wired.com. 2019. recuperado de: <https://www.wired.com/story/san-francisco-prohibe-utilizar-tecnología-de-reconocimiento-facial/> (consultado en noviembre 2020)

¹⁷² Dictamen 3/2012 del Grupo de Trabajo del Artículo 29 y Documento, Privacy & Biometrics. Building a conceptual foundation". National Science and Technology Council. Committee on Technology. Committee on Homeland and National Security, Subcommittee on Biometrics, Estados Unidos de América, 2006.

¹⁷³ Cameron F. Kerry. *Por qué la protección de la privacidad es un juego perdido hoy en día y cómo cambiar el juego*, Brookings Institute, 2017, recuperado de: <https://www.brookings.edu/research/porqué-proteger-la-privacidad-es-un-juego-perdido-hoy-y-cómo-cambiar-el-juego> (consultado en noviembre 2020)

expresado su preocupación de que la pérdida de la integridad de la documentación podría comprometer la atención, la coordinación y los informes del paciente e investigación, e incluso permitir el fraude y el abuso.¹⁷⁴

- *Copia de registros digitales*: la exposición masiva de información permite contar con un registro completo sobre los individuos, vulnerando su privacidad y confidencialidad.
- *Exposición de datos personales*: procesamiento automático de datos, compatible con sistemas de Inteligencia Artificial y aprendizaje automático, lo cual hace posible la automatización de patrones y otra información relativa al usuario, que permite su identificación o en el peores de los casos suplantación de identidad.

Cabe enfatizar que sí bien la digitalización de los sistemas de identificación fomenta ciertos riesgos, también representa nuevas oportunidades para una mayor protección a través de medios tecnológicos, permitiendo entre otras cuestiones lo siguiente:

- *Identificación y autenticación*: a medida que los sistemas de identificación digital aprovechan el procesamiento informático y tecnologías, pueden ofrecer un mayor nivel de garantía y precisión que la autenticación manual basada en papel procesos que están sujetos a error humano y discreción. Hacerlo aumenta la confianza, reduce los costos y respalda sistemas sostenibles y flexibles.¹⁷⁵
- *Integridad de datos*: los sistemas de identificación digital también pueden asegurar una mejor integridad y calidad en el uso de los datos recopilados en comparación con sistemas de registros en papel que se pueden destruir, dañar o alterar fácilmente. Además, la automatización,

¹⁷⁴ Arrowood, D, E Choate, E Curtis et al. "Integridad del expediente sanitario: Mejores prácticas para la documentación de HCE", *Revista de AHIMA*, 2013, p.p.58-62, recuperado de: <https://library.ahima.org/doc?oid=300257#.XNt9so5JE2w> (consultado en septiembre 2020)

¹⁷⁵ Banco Mundial, *Combatir la ciberdelincuencia: herramientas y creación de capacidad para economías emergentes.*, Washington, D. C., 2017, recuperado de: <http://www.combattingcybercrime.org/> (consultado en septiembre 2020)

proporciona registros auditables del procesamiento de datos, lo que mejora la responsabilidad y ayuda a abordar las brechas de seguridad.¹⁷⁶

- *Garantías de privacidad de datos:* la tecnología digital permite nuevas funciones que mejoran la privacidad que antes no eran posibles. En los sistemas tradicionales que utilizan credenciales no digitales, la transacción normalmente implica presentar una tarjeta de identificación física a un proveedor de servicios y, por lo tanto, revelar más información de la estrictamente necesaria. La tecnología digital puede ayudar a resolver este problema a través de credenciales digitales que ocultarían o mostrarían selectivamente solo los datos necesarios, preservando la integridad de la persona.¹⁷⁷
- *Mayor agencia y control:* Las nuevas tecnologías y estrategias de diseño brindan a las personas un mayor control sobre sus datos personales, incluidos portales de acceso que permiten a los usuarios verificar la precisión de sus datos y monitorear el uso de su información.¹⁷⁸

3.7. Identidad digital post mortem.

Como se ha mencionado con antelación, la identidad es el elemento esencial del ser humano, como parte de su existencia y reconocimiento en la sociedad, la cual se conforma por el cumulo de características y aptitudes del sujeto, incluidos sus datos personales que lo permiten ser identificable.

Sin embargo, para comprender la coexistencia del reconocimiento de la identidad, existen dos aspectos esenciales, para poder comprender la capacidad en el ejercicio del derecho a la identidad en cuestión; por un lado, la aptitud legal para ser titular de derechos y obligaciones; y por el otro, la posibilidad jurídica que tiene la persona de ejercer sus derechos y cumplir sus obligaciones.

¹⁷⁶ *Idem*

¹⁷⁷ World Bank Group, *ID4D Practitioner's Guide, Identification for Development*, Washington, D.C., 2019, recuperado de: <http://documents.worldbank.org/curated/en/248371559325561562/ID4D-Practitioner-s-Guide> (consultado en agosto 2020)

¹⁷⁸ *Idem*

La identidad, como se analizó previamente, es reconocida como un derecho fundamental y por tanto se encuentran garantizados, sin ningún tipo de discriminación social, económica, jurídica, política, ideológica, cultural o sexual.¹⁷⁹

Bajo ese contexto, es importante traer a colación lo que determina el propio Ferrara, en dónde a su consideración, el término persona, tiene tres significados: en el sentido fisio-antropológico, hombre; en el sentido teológico-filosófico, como un sujeto racional, consciente, capaz de querer; y en el sentido jurídico, como ente que tiene una función jurídica, cualidades en el derecho y capacidad.¹⁸⁰

Así, la personalidad jurídica es reconocida por el derecho moderno como un medio para el que los seres humanos podemos realizar en la vida nuestros fines individuales y temporales¹⁸¹, que se extinguen con la muerte del sujeto, por tanto, en este sentido la personalidad es la cualidad que distingue al hombre del resto de los seres vivos.

Acorde a lo analizado con antelación es preciso señalar que, para el Doctor Sánchez Cordero Dávila, “La vida humana se sitúa entre dos extremos perfectamente identificables: el nacimiento y la muerte. Respecto a este último extremo puede aún llegar a haber incertidumbre: es lo que se conoce en derecho como el desaparecido o el ausente”.¹⁸²

En relatadas condiciones, cuando se habla de disfrute, se hace en referencia al aspecto genérico de la capacidad, esto es, su goce, y, por otro lado, cuando se hace referencia al cumplimiento de derechos y obligaciones, nos encontramos ante la capacidad de ejercicio.

Para mejor referencia, el Código Civil Federal señala respecto a la capacidad lo siguiente:

¹⁷⁹ Pacheco, Máximo G., *Los derechos fundamentales de la persona humana*, Instituto Interamericano de Derechos Humanos, Serie de Estudios de Derechos Humanos, Tomo II, 1999, p.p. 67.

¹⁸⁰ Ferrara, Francisco, *Teoría de las Personas Jurídicas*, Traducción de Eduardo Ovejero y Maury, Madrid, 1929, p.p. 313-314.

¹⁸¹ Muñozcano Eternod, Antonio, *El derecho a la intimidad frente al derecho a la información*, Primera Edición, Editorial Porrúa, México, 2010, p.p. 50.

¹⁸² Sánchez-Cordero Dávila, Jorge A, *Derecho Civil, Introducción al derecho mexicano*, Universidad Nacional Autónoma de México, México, 1981, recuperado de: <http://biblio.juridicas.unam.mx/libros/libro.htm?l=598> (consultado en diciembre de 2020).

“Artículo 22.- La capacidad jurídica de las personas físicas se adquiere por el nacimiento y se pierde por la muerte; pero desde el momento en que un individuo es concebido, entra bajo la protección de la ley y se le tiene por nacido para los efectos declarados en el presente Código”.

Conforme a lo anterior, Código Civil Federal nos señala claramente el inicio y pérdida de la capacidad de la persona física. Esto es, que la capacidad jurídica de las personas físicas comienza al momento de su nacimiento y se pierde con la muerte.

En consecuencia, cuando nos referimos al reconocimiento de la identidad, incluida la figura de la identidad digital, como una extensión de la identidad del sujeto en la red, no se advierte alguna figura jurídica que otorgue legitimación a un tercero para el ejercicio de sus derechos respecto de una persona fallecida.

Aunado al hecho de que los datos de carácter personal son aquellos que pertenecen al individuo, a la persona física, o son propios de él y que, por tanto, afectan en mayor o menor medida a la vida privada y consecuentemente, a la intimidad, que los eleva a la calidad de personalísimos, entrando en la esfera y el ámbito de que solo hay un único poder de decisión y disposición sobre ellos: el de su titular.

En consecuencia, es claro que, los activos digitales son un recurso cada vez más valioso y relevante, pues son un conjunto de información personal, bienes y derechos con valor monetario, propiedad intelectual, empresarial, institucional o individual en el campo virtual como lo es el Internet. Asimismo, conforme a lo expuesto por el Maestro Miguel Ángel Morales Sandoval, los activos digitales se dividen en varios tipos:¹⁸³

- Perfiles en redes sociales (Facebook, Twitter, LinkedIn, Instagram, Youtube).
- Bienes digitales (e-books, música, usuarios de cuentas en juegos virtuales, plataformas de compra online).
- Medios de pago o monedas virtuales (bitcoins, PayPal).

¹⁸³ Morales Sandoval Miguel Ángel, “Nuestra identidad digital después de la muerte”, *Revista Hechos y Derechos*, Instituto de Investigaciones Jurídicas UNAM, Número 58, julio-agosto 2020.

- Documentos y cuentas de correo electrónico (datos guardados en la nube).
- Blogs, entre otros.


Por lo que el Maestro Morales, concluye, que sí bien, todos los bienes, derechos y obligaciones de una persona que no se extinguen con su muerte, como señala nuestro Código Civil, se puede ultimar que sí existe un patrimonio digital respecto de los activos digitales y que es posible constituirlo como herencia y posteriormente hacer la transmisión a los futuros herederos o legatarios, sin embargo, aún dicho aspecto en México no ha sido contemplado por la ley, ni regulado para subsanar dicha deficiencia, resultado un tema vanguardista y de importante observancia para contar con una certeza jurídica sobre el destino de la identidad digital al momento del fallecimiento de tu titular.

Cabe mencionar que, algunos países, como Francia y Estados Unidos, han contemplado la cuestión del legado digital, adoptando algunas medidas y regulaciones sobre el tema.

España es pionera en una legislación, pues se ha promulgado la Ley 10/2017, de 27 de junio, sobre las Voluntades digitales del Código Civil de Cataluña, que establece que los testamentos ahora podrán contener voluntades digitales y para que el heredero, el legatario, el albacea, el administrador, el tutor o la persona designada para su ejecución actúen ante los prestadores de servicios digitales después de su muerte o en caso de tener la capacidad judicialmente modificada.

La Ley contempla que las voluntades digitales no sólo se pueden ordenar a través de testamento, sino también a través de un documento de voluntades digitales que se tiene que inscribir en el Registro Electrónico de Voluntades Digitales dependiente del Departamento de Justicia de la Generalidad de Cataluña, un nuevo instrumento registral de carácter administrativo que permitirá la designación telemática del heredero digital desde cualquier ordenador si se dispone de firma electrónica. Ante los prestadores de servicios, la inscripción al Registro de Voluntades Digitales tendrá el mismo valor que el testamento.¹⁸⁴

¹⁸⁴ *Idem*



Capítulo 4.
**Instrumentos de regularización de
la identidad digital**

Capítulo 4. Instrumentos de regularización de la identidad digital

Dada la necesidad fundamental de una conexión en línea segura y precisa, que permita la identificación, autenticación y otros servicios de confianza, tanto el sector público como el privado se han visto en la necesidad de evolucionar para tener la capacidad de interactuar con los usuarios.

En ese sentido, las economías y sociedades cada vez se han ido integrando a una era digital, en dónde la identificación ha sido clave para una interconexión viable, lo cual ha fomentado la adopción de la tecnología digital, incluyendo la generación de bases de datos y credenciales electrónicas, reconocimiento biométrico, automatización de procesos, autenticación de identidades, aplicaciones móviles, plataformas de interoperabilidad entre muchos más.

Todos estos sistemas e innovaciones tecnológicas han mejorado y fomentado la precisión y verificación de la identidad digital de las personas, aumentando su eficiencia, creando oportunidades de desarrollo y ha incitado para la consolidación de los sistemas de identificación digital.

Para lograr lo anterior, las naciones se han dado a la tarea de generar las políticas y mecanismos necesarios para generar sistemas de identificación que cumplan con los objetivos ante el desafío multifacético que representa el surgimiento de la identidad digital, buscando mitigar a toda costa los riesgos potenciales que, representada la digitalización, preservando la privacidad y protegiendo los datos personales de las personas.

Lo cierto es que hasta el momento y conforme a diversas experiencias globales no existe un sistema perfecto, sin embargo, concurren factores de éxito que han permitido mitigar dichos riesgos, preservando la integridad de los usuarios, mediante la adopción de estándares internacionales y prácticas sostenibles que permiten enfrentar los desafíos que representa la identificación digital.

4.1. Análisis de casos internacionales prácticos aplicables al reconocimiento de la identidad digital.

4.1.1. Unión Europea (*eIDAS -Regulation*)

El Reglamento (UE) N° 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza en las transacciones electrónicas en el mercado interior y por el que se deroga la Directiva 1999/93/CE (Reglamento eIDAS), tiene como objetivo reforzar el Mercado Único europeo otorgando un nivel de seguridad adecuado a los medios de identificación electrónica y los servicios de confianza, es una norma de aplicación directa en el ámbito de la Unión Europea.¹⁸⁵

En ese sentido, el Reglamento eIDAS, en su artículo 1°, busca garantizar que sean posibles la identificación y la autenticación electrónicas seguras para el acceso a los servicios transfronterizos en línea ofrecidos por los Estados miembros, asimismo, determina que el objeto del Reglamento será:

A) establecer las condiciones en que los Estados miembros deberán reconocer los medios de identificación electrónica de las personas físicas y jurídicas pertenecientes a un sistema de identificación electrónica notificado de otro Estado miembro,

B) establecer normas para los servicios de confianza, en particular para las transacciones electrónicas, y

C) establecer un marco jurídico para las firmas electrónicas, los sellos electrónicos, los sellos de tiempo electrónicos, los documentos electrónicos, los servicios de entrega electrónica certificada y los servicios de certificados para la autenticación de sitios web.

Asimismo, en su artículo 3°, se conceptualiza a la identificación electrónica como el “proceso de utilizar los datos de identificación de una persona en formato electrónico que representan de manera única a una persona física o jurídica o a una persona física que representa a una persona jurídica” y se genera un “régimen para

¹⁸⁵ REGLAMENTO eIDAS Identificación y firma, Ministerio de Política Territorial y Función Pública, Secretaría de Estado de Función Pública, Secretaria General de Administración Digital, Madrid, 2018.

la identificación electrónica en virtud del cual se expiden medios de identificación electrónica a las personas físicas o jurídicas o a una persona física que representa a una persona jurídica, tipificándolo como un sistema de identificación electrónica, con ello se permite realiza un proceso de autenticación, definido como “un proceso electrónico que posibilita la identificación electrónica de una persona física o jurídica, o del origen y la integridad de datos en formato electrónico”.

En consecuencia, por medio del Reglamento eIDAS, se genera un proceso de autenticación de los usuarios, permitiendo una interoperabilidad entre los países miembros de la Unión Europea, otorgando seguridad a las transacciones que se lleven a cabo en la red, lo cual se realiza a través de diversos instrumentos como la firma electrónica, otorgando reconocimiento a la identidad de los usuarios.

4.1.2. Bélgica (Belgian Mobile ID)

En cumplimiento al artículo 9.3 del Reglamento (UE) N° 910/2014 (Reglamento eIDAS) Bélgica notificó a la Comisión Europea un sistema de identificación electrónica que puede utilizarse para acceder a diversos servicios prestados por el sector público en Bélgica.

El sistema de identificación, fue fundado en 2016 y se le denomina *Belgian Mobile ID NV/SA* (BMID), el cual se constituye como un consorcio de empresas conjuntas de cuatro instituciones financieras líderes en el país, así como las tres compañías móviles belgas operadoras de red, quienes juntos, querían facilitar a la gente la posibilidad de identificarse digitalmente de forma segura y rápida.

En un mundo cada vez más digital BMID, se dio a la tarea de crear una aplicación llamada “itsme”, la cual permite a los ciudadanos o residentes belgas confirmar su identidad de forma segura, fácil y fiable e iniciar sesión en cualquier momento en cualquier lugar con un solo código.

Los usuarios instalan la aplicación en su dispositivo móvil personal, los parámetros de identificación son activados y personalizados basados en una identificación previa cara a cara con el ciudadano belga, así como con documentos oficiales como *eCard* o *Foreigner eCard* a través de los "Registradores de Identidad" (IDR) o a través de una firma electrónica cualificada, cotejándose la identificación

mediante la tarjeta electrónica de ciudadano belga o la tarjeta electrónica de extranjero.

Una vez activado, los usuarios tienen a su disposición diferentes servicios, como la autenticación, el cual conforme al artículo 9 de la ley de 18 de julio de 2017 sobre la identificación electrónica, BOSA / DG DT opera el sistema federal Servicio de Autenticación (FAS), como resultado de este reconocimiento, “itsme” es una de las autenticaciones y métodos ofrecidos por el FAS.

En consecuencia, a través de BMID, se genera una única identificación digital que se puede usar para todas las interacciones digitales, desde iniciar sesión o registrarse en varios sitios web, realizar pagos seguros y validar contratos, adaptándose a las necesidades del usuario.¹⁸⁶

4.1.3. Reino Unido (GOV.UK Verify)

GOV.UK Verify, es una herramienta implementada por el gobierno británico, a través del cual se busca autenticar de manera segura y demostrar quién es el usuario en línea, a fin de acceder a servicios gubernamentales, como presentar su declaración de impuestos o verificar la información en su licencia de conducir, entre otros.

Para poder hacer uso de la herramienta, el usuario debe de tener una dirección en el Reino Unido para usar GOV.UK Verify, cabe aclarar que no es necesario ser ciudadano del Reino Unido para ejecutarla.

Asimismo, para realizar la autenticación el usuario debe de registrarse y elegir entre una lista de proveedores de identidad (también llamados “empresas certificadas”), la empresa que elija para verificar su identidad pedirá algunos datos personales, verificarán y cotejará la información con los registros que tienen los proveedores de telefonía móvil, las agencias de crédito, la Oficina de Pasaportes o la Agencia de Licencias de Conductores y Vehículos. Los proveedores o “empresas certificadas” de identidad autorizados son los siguientes:¹⁸⁷

- *Barclays*
- *Experian*
- *Digidentidad*
- *Oficina postal*

¹⁸⁶ Para más información véase: <https://www.belgianmobileid.be/en>

¹⁸⁷ *Guidance GOV.UK Verify*, Recuperado de: <https://www.gov.uk/government/publications/introducing-govuk-verify/introducing-govuk-verify> (consultado en agosto 2020)

- *Secure Identity*

Una vez realizado el proceso de autenticación, la compañía puede confirmar su identidad al servicio gubernamental que busca utilizar, por ejemplo, el servicio que usa para iniciar sesión y presentar su declaración de impuestos de autoevaluación si presenta su declaración de impuestos.

La herramienta ha tenido gran éxito en el Reino Unido, cerca de 22 servicios gubernamentales lo emplean para verificar la identidad de los usuarios, asimismo, cerca de 7,165,021 se han registrado para usar *GOV.UK Verify*.

Finalmente, en la página del gobierno británico, se exponen diversos motivos por los cuales se considera que *GOV.UK Verify*, es una herramienta segura, enunciando las siguientes:

- ✓ La información no se almacena en un solo lugar;
- ✓ No hay intercambio innecesario de información;
- ✓ El departamento gubernamental no sabe qué proveedor de identidad ha elegido
- ✓ Todos los proveedores de identidad deben cumplir con los estándares gubernamentales e internacionales de seguridad y protección de datos.¹⁸⁸

4.1.4. Iniciativa ID4D de la ONU y el Banco Mundial.

Esta Guía fue creada por la “Iniciativa de Identificación para el Desarrollo” (ID4D) del Grupo del Banco Mundial para ayudar a diseñar e implementar sistemas de identificación (ID) que sean inclusivos y confiables, de acuerdo con los diez Principios de Identificación para el Desarrollo Sostenible y otras normas internacionales y buenas prácticas. Su objetivo es servir como un recurso central para las contrapartes de los países, el personal del Grupo del Banco Mundial y otros actores involucrados en la planificación, gestión y financiación de los sistemas de identificación.¹⁸⁹

¹⁸⁸ *Idem*

¹⁸⁹ Banco Mundial, *Guía para profesionales que trabajan en el área de la ID4D*, 2019, recuperado de: <https://id4d.worldbank.org/guide>, (consultado en diciembre 2020)

Existen ciertos estándares de alto nivel que los profesionales deben seguir para garantizar que los sistemas de identificación sean inclusivos, confiables y útiles para las personas, los gobiernos y el sector privado. Esto incluye los diez Principios de Identificación para el Desarrollo Sostenible, a partir de 2019, estos principios han sido respaldados por 25 organizaciones internacionales, asociaciones y socios para el desarrollo. Los Principios están organizados según tres pilares: inclusión, diseño y gobernanza, tal y como se muestra a continuación:

| PILARES | PRINCIPIOS |
|--|---|
| INCLUSIÓN: COBERTURA Y ACCESIBILIDAD UNIVERSAL | 1. Garantizar la cobertura universal para las personas desde el nacimiento hasta la muerte, sin discriminación. 2. Eliminar las barreras de acceso y uso y las disparidades en la disponibilidad de información y tecnología. |
| DISEÑO: ROBUSTO, SEGURO, RESPONSABLE Y SOSTENIBLE | 3. Establecer una identidad sólida, única, segura y precisa. 4. Crear una plataforma que sea interoperable y que responda a las necesidades de varios usuarios. 5. Usar estándares abiertos y garantizar la neutralidad de proveedores y tecnología. 6. Protección de la privacidad y el control del usuario mediante el diseño del sistema 7. Planificación de la sostenibilidad financiera y operativa sin comprometer la accesibilidad |
| GOBERNANCIA: CONSTRUYENDO CONFIANZA PROTEGIENDO LA PRIVACIDAD Y LOS DERECHOS DEL USUARIO | 8. Salvaguardar la privacidad, la seguridad y los derechos del usuario de los datos a través de un marco legal y regulatorio integral. 9. Establecer mandatos institucionales claros y rendición de cuentas. 10. Hacer cumplir los marcos legales y de confianza a través de la supervisión independiente y la adjudicación de quejas. |

Figura 12. Principios de identificación para el desarrollo sostenible. Fuente: Banco Mundial. ¹⁹⁰.

Para el Banco Mundial, la identidad digital, o identidad electrónica (eID), ofrece las naciones en desarrollo una oportunidad única para acelerar el ritmo de su progreso nacional, cambiando la forma en que se prestan los servicios, ayuda al crecimiento de la economía digital de un país, lo anterior, ante el uso y desarrollo de las nuevas tecnologías que en combinación con los teléfonos móviles y el Internet, permite que los servicios se presten electrónicamente, dando un impulso a la eficiencia del gobierno y llevando a la creación de nuevos productos y servicios en línea, bajo un esquema de identificación eficiente.

¹⁹⁰ Banco Mundial, *Guía para profesionales que trabajan en el área de la ID4D*, 2019, p. 26-29, recuperado de: <https://id4d.worldbank.org/guide>, (consultado en diciembre 2020)

Asimismo, sí bien la implementación de sistemas de identificación digital, conlleva un reto en materia de privacidad y protección de datos personales, lo cierto es que el reconocimiento de la identidad digital, proporciona soluciones basadas en la tecnología para la identificación para establecer de manera única la identidad de una persona y acreditarla, de modo que la identidad pueda ser afirmada y verificada de manera segura e inequívoca a través de los medios electrónicos y así poder tener acceso a diversos servicios en todos los sectores, incluidos la atención sanitaria, las redes de seguridad, los servicios financieros y el transporte.¹⁹¹

Bajo ese contexto, el sector privado y el público juegan un papel importante a efecto de facilitar el desarrollo de tales sistemas, y crear la confianza necesaria para establecer y mantener a través de la creación de políticas y reglamentos bien informados, sobre la implementación de dichos sistemas de identificación digital.¹⁹²

4.2. Análisis de casos nacional prácticos aplicables al reconocimiento de la identidad digital.

4.2.1. Mecanismos de “identidad digital” implementados por el Gobierno Mexicano (<https://www.gob.mx/identidad>)

El gobierno de México, a través de la página <https://www.gob.mx/identidad> da a conocer diversos mecanismos de identificación digital que permiten verificar la identidad de un usuario, para tener acceso a trámites y servicios gubernamentales que por sus características propias así lo requieren, a través del proceso siguiente:¹⁹³

¹⁹¹ Atick, Joseph J; Gelb, Alan Harold; Pahlavooni, Seda; Gasol Ramos, Elena; Safdar, Zaid, *Digital identity toolkit: a guide for stakeholders in Africa*, Washington, D.C., World Bank Group, 2014. <http://documents.worldbank.org/curated/en/147961468203357928/Digital-identity-toolkit-a-guide-for-stakeholders-in-Africa> (consultado en septiembre 2020)

¹⁹² *Idem*

¹⁹³ Gobierno de México, recuperado de: <https://www.gob.mx/identidad> (consultado en agosto 2020)



Figura 13. Pasos para autenticarte en trámites y servicios gov.mx

Fuente: <https://www.gob.mx/identidad>

Para llevar a cabo la autenticación del usuario las instituciones gubernamentales son responsables de los mecanismos de identificación digital que se requieran para acceder a cada servicio, actualmente las dependencias y entidades cuentan con cuatro niveles de autenticación relativos a los mecanismos de identificación digital los cuales se describen a continuación:¹⁹⁴

- Tipo "A" o Usuario anónimo: este mecanismo no requiere de ninguna autenticación, se considera como una interacción donde el usuario mantiene secreta su identidad.
- 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.
- 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.
- 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.
- Tipo "E" o Autenticación a través de datos biométricos: este mecanismo requiere que una persona física ingrese su CURP¹⁹⁵ y uno o más datos

¹⁹⁴ 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. Publicado en el Diario Oficial de la Federación: 10/05/2018.

¹⁹⁵ Por su acrónimo: Clave Única de Registro de Población.

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.

A la fecha más de 1,000 trámites y servicios digitales utilizan dichos mecanismos de autenticación, que permiten a una persona física o moral acreditar su identidad con la finalidad de que pueda acceder a trámites o servicios que así lo requieran con certeza jurídica.¹⁹⁶

4.2.2. Iniciativa para expedir la Ley General de Identidad y Ciudadanía Digital.

El pasado 19 de marzo de 2020, el diputado por la Ciudad de México Javier Hidalgo Ponce, propuso una iniciativa para expedir la Ley General de Identidad y Ciudadanía Digital¹⁹⁷, la cual a grandes rasgos propone que el Estado debe otorgar a los ciudadanos una cédula de identidad digital que incluya datos personales y biométricos y cuyo objetivo es regular la identificación de los ciudadanos por medios digitales y garantizar el ejercicio de los derechos y obligaciones de los mexicanos, a través del uso de Tecnologías de la Información y la Comunicación.

Con independencia de las discusiones que se produzcan respecto de dicha iniciativa, lo cierto es que el proyecto de ley constituye un esfuerzo para impulsar el desarrollo de una sociedad de la información, la cual, se destaca por el aprovechamiento de las nuevas tecnologías de la información y comunicación, sin embargo, aún hace falta la creación de políticas públicas necesarias que fomenten la innovación en el uso de estas herramientas, establecer los mecanismos de seguridad necesarios, que permitan corroborar la veracidad de la información por un lado, y por otro lado se genere la confianza a los ciudadanos para formar parte de dicho proyecto.

En consecuencia, la implementación de una normatividad vinculada a la identidad digital de los ciudadanos deberá de apoyarse y seguir lo ya establecido en la normatividad en materia de protección de datos personales, vigilando en todo momento la implementación de los principios rectores en pro de la protección del

¹⁹⁶ Gobierno de México, recuperado de: <https://www.gob.mx/identidad> (consultado en agosto 2020)

¹⁹⁷ Ley General de Identidad y Ciudadanía Digital, Gaceta Parlamentaria, año XXII, número 5482-I, jueves 19 de marzo de 2020.

derecho humano y amparando la autodeterminación informativa de los titulares de datos personales.

Aunado a lo anterior, cabe traer a colación, que el pasado primero de septiembre de 2020, se presentó la iniciativa para expedir una ley que regule la materia de ciberseguridad en México, la cual busca modificar el Código Penal Federal y la Ley General del Sistema Nacional de Seguridad para que tanto las regulaciones en materia de seguridad de la información como los delitos cibernéticos que se cometan sean normados y sancionados por una nueva “Ley General de Ciberseguridad”.¹⁹⁸

Lo anterior, es importante destacar, ya que, conforme al Reporte Global para Riesgos, realizado por el Foro Económico Mundial en el año 2020¹⁹⁹ el robo y fraude de información, así como los ciberataques, se encuentran entre los diez riesgos con más probabilidades de concurrencia, lo cual definitivamente, atañe a nuestro tema de identidad digital, al ser necesario un ambiente seguro y confiable para su desarrollo.

¹⁹⁸ INICIATIVA CON AVAL DEL GRUPO PARLAMENTARIO QUE CONTIENE PROYECTO DE DECRETO POR EL QUE SE MODIFICA LA DENOMINACIÓN DEL CAPÍTULO II, DEL TÍTULO NOVENO, DEL LIBRO SEGUNDO Y SE REFORMA EL ARTÍCULO 211 BIS 1 Y SE DEROGAN DIVERSOS ARTÍCULOS DEL CÓDIGO PENAL FEDERAL; SE REFORMAN Y ADICIONAN DIVERSOS ARTÍCULOS DE LA LEY GENERAL DEL SISTEMA NACIONAL DE SEGURIDAD PÚBLICA; SE ADICIONA UNA FRACCIÓN XIV AL ARTÍCULO 5° DE LA LEY DE SEGURIDAD NACIONAL; Y SE EXPIDE LA LEY GENERAL DE CIBERSEGURIDAD, recuperado de: http://sil.gobernacion.gob.mx/Archivos/Documentos/2020/09/asun_4064516_20200902_15990628_84.pdf (consultado en noviembre 2020)

¹⁹⁹ World Economic Forum, *The Global Risks Report 2020*, 15th Edition, Recuperado de: http://www3.weforum.org/docs/WEF_Global_Risk_Report_2020.pdf (consultado en enero de 2021)



Cuadro 3. “The Global Risks Report 2020”, 15th Edition. Fuente: World Economic Forum.²⁰⁰

En ese sentido, como aspectos relevantes de dicha iniciativa, la misma tiene por objeto establecer las bases de integración y acción coordinada de las instituciones y autoridades encargadas de preservar la ciberseguridad en las instituciones del Estado y la sociedad. Entre lo propuesto destaca lo siguiente:²⁰¹

- 1) Establecer tipos penales en la materia e integrar la forma y los términos en que las autoridades de las entidades *federativas* y los municipios colaborarán con la Federación en dicha tarea;
- 2) Garantizar el derecho de acceso a las tecnologías de la información y comunicación, así como a los servicios de telecomunicaciones, incluido el de banda ancha e internet en forma segura;
- 3) Crear la Comisión Permanente de Ciberseguridad dentro de la estructura del Consejo Nacional de Seguridad Pública;

²⁰⁰ World Economic Forum, *The Global Risks Report 2020, 15th Edition*, Shareable Infographics. Recuperado de: <https://reports.weforum.org/global-risks-report-2020/shareable-infographics/> (consultado en enero de 2021)

²⁰¹ Llamas Covarrubias Jersain, *Observaciones y estudio de la iniciativa que expide la Ley General de Ciberseguridad en México*, Universidad de Guadalajara, Septiembre 2020. Recuperado de: <https://www.researchgate.net/deref/https%3A%2F%2Fforojuridico.mx%2Fauthor%2Fjersain-llamas-covarrubias%2F> (consultado diciembre de 2020)

- 4) Originar el Centro Nacional de Ciberseguridad dentro de la estructura del Secretariado Ejecutivo del Sistema Nacional de Seguridad Pública;
- 5) Definir la infraestructura de información crítica y lo relativo al Centro Nacional de Ciberseguridad, así como sus atribuciones integración y funcionamiento;
- 6) Determinar los proveedores de servicios de ciberseguridad;
- 7) Describir la Estrategia Nacional de Ciberseguridad;
- 8) Tipificar los delitos en la materia; y,
- 9) Estipular los convenios internacionales en materia de ciberseguridad.²⁰²

Este tema resulta de vital importancia en nuestro tema de investigación, ya que con ello podrían generarse un marco jurídico protector en el ámbito de la identidad digital y a su vez, un seguimiento a los delitos que pudieran suscitar en temas de ciberseguridad en donde la identidad digital de los usuarios se viera vulnerada, por lo que no se debe dejar de lado la evolución de dicha iniciativa.

²⁰² *Idem*



Conclusiones

Conclusiones

Sin duda el Internet ha cambiado de forma radical la forma en que interactuamos, por lo que es claro que la forma tradicional de como nuestros sistemas de identidad se han basado en interacciones físicas y mediante la acreditación de documentos tangibles, para demostrar quienes somos, como un factor fundamental en del desarrollo social, económico, financiero y gubernamental, poco a poco ha dejado de ser funcional.

Ya que tomando en consideración que el derecho a la identidad es reconocido como un derecho humano fundamental que brinda existencia jurídica a los seres humanos²⁰³, y se encuentra íntimamente ligado a la individualidad, información o datos personales y vida privada de los sujetos, resulta necesario ver más allá del mundo físico para adentrarnos a la era digital.

Lo anterior tomando en consideración el aumento exponencial en el uso del Internet y las nuevas tecnologías de la información y comunicación, se ha generado la necesidad de demostrar quienes somos en la red, es decir, acreditar nuestra identidad de forma digital. Lo anterior, a fin de encontrar soluciones de acreditación de identidad válidas y seguras para la prestación de servicios, mercados, estándares y reconocimiento digital, tanto para los usuarios como para los proveedores de servicios (públicos o privados)

En consecuencia, es claro que el uso de internet y de las redes sociales se ha convertido en una extensión de la vida tanto personal como profesional, laboral y más ámbitos de las personas²⁰⁴, pues la interacción e interconexión en el mundo digital ha generado la creación de una representación digital del usuario, misma que se conforma por el conjunto de datos personales, atributos, acciones y actividades que realiza una persona en la red, es decir, su identidad digital.

La identidad digital ha ganado tanta importancia como la identidad física, implicando el reconocimiento de una persona en su vida diaria, su individualización

²⁰³ López Velarde Campa, Jesús Armando Coordinador, *El derecho a la identidad como base para el ejercicio de los derechos humanos de niñas, niños y adolescentes en situación de calle en la Ciudad de México*, Instituto de Investigaciones Jurídicas UNAM, Primera edición, México, 2017.

²⁰⁴ Morales Sandoval Miguel Ángel, "Nuestra identidad digital después de la muerte", *Revista Hechos y Derechos*, Instituto de Investigaciones Jurídicas UNAM, Número 58, julio-agosto 2020.

y actuar en el uso de las nuevas tecnologías, se encuentra directamente vinculada con sus datos personales y su privacidad, ello trasciende a su reputación y vida diaria, sin embargo, han comenzado a suscitar diversos problemas y riesgos que acechan a la integridad de los usuarios.

Además de las dificultades de acreditación y verificabilidad de la identidad de los sujetos en la red, resulta necesario contar con reglas, procedimientos y componentes técnicos que implementen una política de protección, organización, uso e intercambio de información de una identidad digital²⁰⁵, dada la necesidad fundamental de una conexión en línea segura y precisa, que genere confianza, tanto el sector público como el privado.

En ese sentido, las naciones, economías y sociedades cada vez se han ido integrando a una era digital, en dónde la identificación ha sido clave para una interconexión viable, lo cual ha fomentado la adopción de la tecnología digital, incluyendo la generación de bases de datos y credenciales electrónicas, reconocimiento biométrico, automatización de procesos, autenticación de identidades, aplicaciones móviles, plataformas de interoperabilidad entre muchos más.

Por lo que, para lograr lo anterior, las naciones y proveedores de servicios digitales, deberán de darse a la tarea de generar las políticas y mecanismos necesarios para generar sistemas de identificación que cumplan con los objetivos ante el desafío multifacético que representa el surgimiento de la identidad digital, tratando de mitigar a toda costa los riesgos potenciales que, representada la digitalización, preservando la privacidad y protegiendo los datos personales de las personas y claro, una cultura de legalidad de los usuarios para un uso responsable y confiable por parte de los mismos, para acreditar quién dicen ser.

Conforme a todo lo anterior, debemos considerar que la identidad digital, implica el reconocimiento de una persona en su vida diaria y su identificación en el uso de las nuevas tecnologías (TIC), lo cual se encuentra directamente vinculada con sus datos personales y su privacidad, ello trasciende a su vida diaria, sin

²⁰⁵ OCDE, *The Role of Digital Identity Management in the Internet Economy: A Primer for Policy Makers*, Documentos sobre economía digital, núm. 160, 2009.

embargo, como se analizó en el presente trabajo de investigación, en la actualidad no se cuenta con un reconocimiento de la misma, que coadyuve a proteger sus atributos, otorgue seguridad y veracidad ante los riesgos que existen en la red.

Ante ello, podemos denotar que la identidad digital en los últimos años ha ganado tanta importancia como la identidad física, por ello, el presente trabajo desarrolla y presenta un manual didáctico, que busca informar y auxiliar en la educación y formación de los usuarios, buscando generar o fomentar una conciencia social y cultura de legalidad sobre la trascendencia de la identidad digital en la vida diaria como usuarios en la red.

El manual didáctico que se presenta, además:

- a. Detalla brevemente los problemas actuales, reconocimiento y protección de la identidad digital.
- b. Realiza un breve estudio y análisis sobre una cultura de legalidad, trascendencia y los posibles riesgos para la privacidad y los datos personales en el desarrollo de la identidad digital.

Lo anterior, a fin de facilitar la información, enseñanza y aprendizaje sobre la identidad digital de todos los usuarios.

Bibliografía

- ÁLVAREZ Carmen, *Identidad digital: ¿Qué es y cómo protegerla?*, BBVA Research, Regulación financiera, Act. 09 marzo 2018. Recuperado de: <https://www.bbva.com/es/identidad-digital-protegerla/>
- ÁLVAREZ, Caro María y Recio, Gayo Miguel. Coordinadores, *Reglamento general de protección de datos. hacia un nuevo modelo europeo de protección de datos*, Editorial Reus, Madrid, 2016.
- AMPARO en Revisión 134/2008. Sentencia del treinta de abril de dos mil ocho. México, p. 22 y 23. Tesis 2a. LXIII/2008, "DERECHO A LA PRIVACIDAD O INTIMIDAD. ESTÁ PROTEGIDO POR EL ARTÍCULO 16, PRIMER PÁRRAFO, DE LA CONSTITUCIÓN POLÍTICA DE LOS ESTADOS UNIDOS MEXICANOS". Semanario Judicial de la Federación y su Gaceta, Novena Época, México, t. XXVII, mayo de 2008, página 229. Reg. IUS. 169700.
- ANDERS, V. et al. *Etimología*, 2001-2020. Recuperado de <http://etimologias.dechile.net/?identidad>
- ARROWOOD, D, E Choate, E Curtis et al. "Integridad del expediente sanitario: Mejores prácticas para la documentación de HCE", *Revista de AHIMA*. 2013, Recuperado de: <https://library.ahima.org/doc?oid=300257#.XNt9so5JE2w>
- ASOCIACIÓN MEXICANA DE INTERNET, A.C. Recuperado de: <http://www.amipci.org.mx/>
- ATICK, Joseph J; Gelb,Alan Harold; Pahlavooni,Seda; Gasol Ramos,Elena; Safdar,Zaid, Digital identity toolkit: a guide for stakeholders in Africa, Washington, D.C., World Bank Group, 2014. <http://documents.worldbank.org/curated/en/147961468203357928/Digital-identity-toolkit-a-guide-for-stakeholders-in-Africa>
- AVETISOVA, Ksenia & Antti Kettunen. *Digital identity management as key component of future customer experience*. Tieto. Recuperado de: <https://perspectives.tieto.com/blog/2017/01/digital-identity-management-as-keycomponent-of-future-customer-experience/>

- AYMERICH Ignacio, *Identidad individual y personalidad jurídica*, Facultad de Derecho Depto. de Filosofía del Derecho Universidad de Castellón, 12080 Castellón España, 2008.
- Banco Interamericano de Desarrollo, *La gestión de la identidad y su impacto en la economía digital*, División de Innovación para Servir al Ciudadano, Agosto, 2017.
- BANCO MUNDIAL, *Guía para profesionales que trabajan en el área de la ID4D*, 2019, Recuperado de: <https://id4d.worldbank.org/guide>.
- BANCO MUNDIAL, *Identificación para el marco estratégico de desarrollo*, documento de trabajo, Washington D. C., 2016
- BANCO MUNDIAL, *Sistemas de identificación digitales fiables e inclusivos pueden abrir oportunidades para las personas más vulnerables del mundo*. Recuperado de: <https://www.bancomundial.org/es/news/immersive-story/2019/08/14/inclusive-and-trusted-digital-id-can-unlock-opportunities-for-the-worlds-most-vulnerable>
- BANCO MUNDIAL, *ID4D Practitioner's Guide* (English). Identification for Development Washington, D.C.: World Bank Group. Recuperado de: <http://documents.worldbank.org/curated/en/248371559325561562/ID4D-Practitioner-s-Guide>
- BANCO MUNDIAL, *Combatir la ciberdelincuencia: herramientas y creación de capacidad para economías emergentes*. Washington, D. C: Banco Mundial Grupo. 2017. Recuperado de: <http://www.combattingcybercrime.org/>
- BANCO MUNDIAL, *Impactos económicos de los sistemas de identificación en el sector privado*. Washington, DC. 2018. Recuperado de: <http://id4d.worldbank.org/research>
- BARBERO, Gregory, "San Francisco prohíbe el uso de tecnología de reconocimiento facial por parte de la agencia". *Wired.com*, 2019. Recuperado de: <https://www.wired.com/story/san-francisco-prohíbe-utilizar-tecnología-de-reconocimiento-facial/>

- BOSTON CONSULTING GROUP. *The value of our digital identity*. Recuperado de: <http://www.libertyglobal.com/PDF/public-policy/The-Value-of-Our-Digital-Identity.pdf>
- BRANDEIS, Samuel D. Warren and Louis D., *The Right to Privacy*, Harvard Law Review, Vol. 4, No. 5, E.U.A., 1890. Publicado por: *The Harvard Law Review Association*.
- CAMERON F. Kerry, *Por qué la protección de la privacidad es un juego perdido hoy en día y cómo cambiar el juego*. Brookings Institute, 2017. Recuperado de: <https://www.brookings.edu/research/porqué-proteger-la-privacidad-es-un-juego-perdido-hoy-y-cómo-cambiar-el-juego>
- CÁSARES García Leonel, "Noción básica del derecho a la identidad en México", *Revista Hechos y Derechos*, Instituto de Investigaciones Jurídicas UNAM, Número 27, Publicado el 6 de mayo de 2015.
- CASTELLS, Manuel, *La revolución de la tecnología de la información*. Barcelona: UOC, 2003.
- CLARK JONES, A, Fitzpatrick, G., Hartenstein M., and others, *The value of our digital identity*. *Digital Identity*. UBS. 2016. Recuperado de: https://www.ubs.com/magazines/innovation/en/teasers/_jcr_content/mainpar/gridcontrol_956493814/col1/actionbutton_261770367.0591371767.file/bGluay9wYXRoPS9jb250ZW50L2RhbS91YnMvbWFnYXppbmVzL2lubm92YXRpb24vZG9jdW1lbnRzL2RpZ2l0YWxJZGVudGI0eS13aGI0ZXBhcGVyLXNjc mVlbi5wZGY=/digitalIdentity-whitepaper-screen.pdf
- CLARKE, Roger (1994). "The Digital Persona and its Application to Data Surveillance". *The Information Society*. Recuperado de: <http://www.rogerclarke.com/DV/DigPersona.html>
- COLLE Raymond "La identidad digital en la internet futura con *blockchain*", *Asociación Chilena de Investigadores en Comunicación*. Recuperado de: https://www.academia.edu/36613066/La_identidad_digital_en_la_internet_futura_con_blockchain
- 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. Recuperado de:
<http://cdhdf.org.mx/wp-content/uploads/2014/09/poblaciones-callejeras-integrado-imprenta.pdf>

COMISIÓN NACIONAL DE LOS DERECHOS HUMANOS, *Niñas, niños y adolescentes tienen derecho a la identidad*, CNDH, Coordinación del Programa sobre Asuntos de la Niñez y la Familia.

CONDE Ortiz Concepción, *La protección de datos personales Un derecho autónomo con base en los conceptos de intimidad y privacidad*, Editorial Dykinson, S.L., Madrid, 2005.

CONVENCIÓN AMERICANA DE DERECHOS HUMANOS, recuperado de:
<http://ordenjuridico.gob.mx/TratInt/Derechos%20Humanos/D1BIS.pdf>

CONVENCIÓN AMERICANA SOBRE DERECHOS HUMANOS, aprobada y suscrita en la Conferencia Especializada Interamericana sobre Derechos Humanos, San José de Costa Rica, 22 de noviembre de 1969; entrada en vigor el 18 de julio de 1978, artículos 18. Derecho al nombre, y 20. Derecho a la nacionalidad.

CONVENCIÓN INTERNACIONAL sobre la Eliminación de Todas las Formas de Discriminación Racial, adoptada y abierta a la firma y ratificación por la Asamblea General de las Naciones Unidas en su Resolución 2106 A (XX) del 21 de diciembre de 1965; entrada en vigor el 4 de enero de 1969, artículo 5º.

CONVENCIÓN SOBRE LA ELIMINACIÓN de Todas las Formas de Discriminación contra la Mujer, adoptada y abierta a la firma y ratificación, o adhesión, por la Asamblea General de las Naciones Unidas en su Resolución 34/180 del 18 de diciembre de 1979; entrada en vigor el 3 de septiembre de 1981, artículo 9º.

CONVENCIÓN SOBRE LOS DERECHOS DEL NIÑO, adoptada y abierta a la firma y ratificación por la Asamblea General de las Naciones Unidas en su Resolución 44/25 del 20 de noviembre de 1989; entrada en vigor el 2 de septiembre de 1990, artículo 7º.

- CORRIPIO Gil-Delgado, R., *Regulación jurídica de los tratamientos de datos personales por el sector privado en internet*. Agencia de Protección de Datos. Premio Protección de Datos, Madrid, 2000.
- CUMBRE MUNDIAL SOBRE LA SOCIEDAD DE LA INFORMACIÓN (CMSI). Ginebra 2003 y Túnez 2005. Recuperado de: <http://www.itu.int/net/wsis/basic/index-es.html>
- DAVARA F. DE MARCOS, Isabel, *Hacia la estandarización de la protección de datos personales: propuesta sobre una "tercera vía o tertium genus" internacional*. Editorial La Ley, 2011.
- DAVARA F. DE MARCOS, Isabel, *Protección de datos de carácter personal en México: Problemática jurídica y estatus normativo actual*, Protección de Datos Personales, Editorial Tiro Corto Editores, México, 2010.
- DE PINA, Rafael, *Elementos de Derecho Civil Mexicano, Introducción- Personas-familia*, Vol. Primero, Editorial Porrúa, S. A., México, 1963, Tercera Edición.
- Declaración Americana de los Derechos y Deberes del Hombre, aprobada en la Novena Conferencia Internacional Americana, Bogotá, 1948, artículo 19.
- Declaración Universal de los Derechos Humanos, aprobada y proclamada por la Asamblea General de las Naciones Unidas en su Resolución 217 A (III) del 10 de diciembre de 1948, artículo 15.
- DENHAM, Elizabeth, *Report of Findings into the Complaint Filed by The Canadian Internet Policy And Public Interest Clinic (CIPPIC) against Facebook Inc. under the Personal Information Protection and Electronic Documents Act*, Assistant Privacy Commissioner of Canada, Julio, 2009.
- DICCIONARIO DE LA LENGUA ESPAÑOLA, 23 ed., [versión 23.3 en línea]. Recuperado de: <https://dle.rae.es>
- DICCIONARIO DE PROTECCIÓN DE DATOS PERSONALES. *Conceptos Fundamentales*, Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI), Primera edición, noviembre de 2019.
- DICCIONARIO JURÍDICO MEXICANO: TOMO I, A-B México: Universidad Nacional Autónoma de México, Instituto de Investigaciones Jurídicas, 1982.

DICTAMEN 02/2013 *sobre las aplicaciones de los dispositivos inteligentes*, Grupo de Trabajo sobre la Protección de Datos del Artículo 29, Unión Europea, Febrero, 2013.

DICTAMEN 3/2012 del Grupo de Trabajo del Artículo 29 *Privacy & Biometrics. Building a conceptual foundation. National Science and Technology Council. Committee on Technology. Committee on Homeland and National Security, Subcommittee on Biometrics*, Estados Unidos de América, 2006.

DICTAMEN 4/2007 *sobre el concepto de datos personales*, Grupo de Trabajo del artículo 29 de la Unión Europea, 01248/07/ES WP 136, Adoptado el 20 de junio de 2007.

DICTAMEN 4/2015. *Hacia una nueva ética digital: Datos, dignidad y tecnología*, Supervisor Europeo de Protección de Datos. Septiembre, 2015.

DICTAMEN 5/2009 *sobre las redes sociales en línea*, Grupo de Trabajo sobre la Protección de Datos del Artículo 29, Unión Europea, Junio, 2009.

DICTAMEN 8/2014 *sobre la evolución reciente de la Internet de los objetos*, Grupo de Trabajo sobre la Protección de Datos del Artículo 29, Unión Europea, Septiembre, 2014.

DIEZ DÍAZ, Joaquín, “¿Derecho de la Personalidad o Bienes de la Persona?”, *Revista General de Legislación y Jurisprudencia*, Madrid, Reus, 1963.

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*. Publicado en el Diario Oficial de la Federación: 10/05/2018.

ESCAJEDO SAN EPIFANIO, L., *Tecnologías biométricas, identidad y derechos fundamentales*, Aranzadi, España, 2017.

ESTÁNDARES *de Protección de Datos Personales para los Estados Iberoamericanos*, Red Iberoamericana de Protección De Datos, 20 de junio de 2017. Recuperado de: http://www.redipd.es/documentacion/common/Estandares_Esp_Con_logor_RIPD.pdf

- FERNÁNDEZ Elisa, "Identity and personality: or as we know we are different from others", *Revista Digital de Medicina Psicosomática y Psicoterapia*, Sociedad Española de Medicina Psicosomática y Psicoterapia, 2011.
- FERNÁNDEZ Sessarego, Carlos, *¿Qué es persona para el derecho? "Derecho Privado"*, Libro en Homenaje a Alberto J. Bueres, Editorial Hammurabi, Buenos Aires, 2001.
- FERRARA, Francisco, *Teoría de las Personas Jurídicas*. Traducción de Eduardo Ovejero y Maury, Madrid, 1929.
- Gaceta Parlamentaria, año XXII, número 5482-I, jueves 19 de marzo de 2020.
- GALINDO Garfias, Ignacio, "*Derecho Civil*", *Primer Curso, Parte general, Personas, Familia*, Editorial Porrúa, S.A., México, 1991, Décima Edición.
- GARCÍA GONZÁLEZ, Aristeo. "La Protección de Datos Personales: Derecho Fundamental del Siglo XXI. Un Estudio Comparado", *Boletín Mexicano de Derecho Comparado*, Instituto de Investigaciones Jurídica, UNAM, nueva serie, año XL, núm. 120, septiembre-diciembre de 2007.
- GELB, A., J. Clark. 2013. *Identification for Development: The Biometrics Revolution*. Center for Global Development Working Paper no. 315.
- GELLMAN Robert & Dixon Pam, *Online Privacy, Contemporary World Issues*, ABC-CLIO, California, E. U. A., 2011.
- GERCKE, Marco. *Robo de identidad relacionado con Internet*, documento de debate del Consejo de Europa. 2007, Recuperado de: <https://rm.coe.int/16802fa3a0>
- GRANT, J. (n.d.). "Identity in Cyberspace: Improving Trust", *Public-Private Partnerships*". NIST. Recuperado de: https://www.healthit.gov/sites/default/files/nstic_onc_7.11.12_mtg_grant.pdf
- GRUPO DE EXPERTOS EN IDENTIDAD LEGAL DE LAS NACIONES UNIDAS (LIEG) y Definición Operacional de Legalidad del Banco Mundial. *Identidad*, recuperado de: <https://www.unhcr.org/en-us/1951-refugeeconvention.html>
- GSMA (2016b). *The future of digital identity in building a successful digital society*. Recuperado de: <https://www.gsma.com/identity/the-future-of-digital-identity-in-building-a-successful-digital-society>

- GUIDANCE GOV.UK VERIFY. Recuperado de:
<https://www.gov.uk/government/publications/introducing-govuk-verify/introducing-govuk-verify>
- H. CONGRESO DE LA UNIÓN, Cámara de Diputados, Leyes Federales Vigentes, *Constitución Política de los Estados Unidos Mexicanos*. Recuperado de:
http://www.diputados.gob.mx/LeyesBiblio/pdf/1_241220.pdf
- H. CONGRESO DE LA UNIÓN, Leyes Federales Vigentes, *Ley General de los Derechos de Niñas, Niños y Adolescentes*. Recuperado de:
<http://www.ordenjuridico.gob.mx/Documentos/Federal/pdf/wo99957.pdf>
- IBM, “Diez tendencias clave de marketing para 2017”. Recuperado de:
<https://www01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=WRL12345USEN>
- IDENTIFICACIÓN DIGITAL GOBIERNO DE MÉXICO (gob.mx identidad): *Gobierno de México*. Recuperado de: <https://www.gob.mx/identidad>
- INCIBE, *Ciberseguridad en la identidad digital y la reputación online: una guía de aproximación para el empresario*, Identidad y Reputación, 2016.
- INICIATIVA con aval del Grupo Parlamentario que contiene proyecto de decreto por el que se modifica la denominación del Capítulo II, del Título Noveno, del libro segundo y se reforma el Artículo 211 Bis 1 y se derogan diversos artículos del Código Penal Federal; se reforman y adicionan diversos artículos de la Ley General Del Sistema Nacional De Seguridad Pública; se adiciona una Fracción XIV al Artículo 5° de la Ley De Seguridad Nacional; y se expide la Ley General De Ciberseguridad. Recuperado de:
http://sil.gobernacion.gob.mx/Archivos/Documentos/2020/09/asun_4064516_20200902_1599062884.pdf
- INSTITUTO NACIONAL ELECTORAL, “INE colabora con instituciones bancarias para prevenir robo de identidad y fraudes a partir de la identificación de huellas dactilares”, *Central Electoral*, publicado el 17 de febrero de 2019. Recuperado de: <https://centralectoral.ine.mx/2019/02/17/ine-colabora-instituciones-bancarias-prevenir-robo-identidad-los-fraudes-partir-la-identificacion-huellas-dactilares/>

INSTITUTO NACIONAL ELECTORAL, “Tarjeta Informativa: Sobre el Padrón Electoral y los Datos Biométricos”, *Central Electoral*, publicado el 24 de enero de 2020. Recuperado de: <https://centralectoral.ine.mx/2020/01/24/tarjeta-informativa-padron-electoral-los-datos-biometricos/>

INTECO, “Guía para usuarios: identidad digital y reputación online”, 2012.

INTERNATIONAL BAR ASSOCIATION. “Digital identity: principles on collection and use of information”. 2016. Recuperado de: https://www.ibanet.org/LPD/Digital_Identity.aspx

INTERNATIONAL TELECOMMUNICATION UNION (ITU) (2010). “Baseline identity management terms and definitions”. *Recommendation ITU-T X.1252*. Recuperado de: http://www.itu.int/SG-CP/example_docs/ITU-T-REC/ITU-TREC_E.pdf

ISO/IEC 24760-1:2019. *IT Security and Privacy — A framework for identity management — Part 1: Terminology and concepts*.

JIMÉNEZ García, Hilda Adriana A., López Velarde Campa, Jesús Armando Coordinador. *El derecho a la identidad como base para el ejercicio de los derechos humanos de niñas, niños y adolescentes en situación de calle en la Ciudad de México*, Instituto de Investigaciones Jurídicas UNAM, Primera edición, México, 2017.

KROTOSKI, Aleks (2016). “Online identity: is authenticity or anonymity more important?”. *The Guardian*. 19 Abril 2016. Recuperado de: <https://www.theguardian.com/technology/2012/apr/19/online-identity-authenticity-anonymity>

LEY Federal de Protección de Datos Personales en Posesión de Particulares. Publicada en el Diario Oficial de la Federación el 5 de julio de 2010. Recuperado de: <http://www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf>

LEY General de Protección de Datos Personales en Posesión de los Sujetos Obligados. Publicada en el Diario Oficial de la Federación el 26 de enero de 2017. Recuperado de: https://www.dof.gob.mx/nota_detalle.php?codigo=5469949&fecha=26/01/20

- LÓPEZ Velarde Campa, Jesús Armando Coordinador. *El derecho a la identidad como base para el ejercicio de los derechos humanos de niñas, niños y adolescentes en situación de calle en la Ciudad de México*, Instituto de Investigaciones Jurídicas UNAM, Primera edición, México, 2017.
- LLAMAS Covarrubias Jersain, *Observaciones y estudio de la iniciativa que expide la Ley General de Ciberseguridad en México*, Universidad de Guadalajara, Septiembre 2020. Recuperado de: <https://www.researchgate.net/deref/https%3A%2F%2Fforojuridico.mx%2Fauthor%2Fjersain-llamas-covarrubias%2F>
- MAGALLANES Martínez Víctor Hugo Hiram, *Derecho a la protección de datos personales. su diseño constitucional, the right of personal data protection and its constitutional design*, Instituto de Investigaciones Jurídicas-UNAM, 2016.
- MARITAN Grisel Galiano, "REFLEXIONES CONCEPTUALES SOBRE LAS CATEGORÍAS: PERSONA, PERSONALIDAD, CAPACIDAD Y SUJETO DE DERECHO", *Revista Derecho y Cambio Social*, Depósito legal: 2005-5822, Publicado enero 2013.
- REGLAMENTO eIDAS Identificación y firma, Ministerio de Política Territorial y Función Pública, Secretaría de Estado de Función Pública, Secretaria General de Administración Digital, Madrid, 2018.
- MORA Chinchilla, Carolina. *Los derechos humanos. Multiculturalidad y ciudadanía en un mundo globalizado*. Costa Rica: UCR, Universidad Costa Rica, Escuela de estudios Generales, Sección de Historia de la Cultura, 2016.
- MORALES Sandoval Miguel Ángel "Nuestra identidad digital después de la muerte", *Revista Hechos y Derechos*, Instituto de Investigaciones Jurídicas UNAM, Número 58, julio-agosto 2020.
- MORALES Sandoval Miguel Ángel "Nuestra identidad digital después de la muerte", *Revista Hechos y Derechos*, Instituto de Investigaciones Jurídicas UNAM, Número 58, julio-agosto 2020.
- MUÑOZCANO ETERNOD, Antonio, *El derecho a la intimidad frente al derecho a la información*, Primera Edición, Editorial Porrúa, México, 2010.P.p. 50.

- Observación General No.14 sobre el derecho del niño a que su interés superior sea una consideración primordial (artículo 3, párrafo 1). CRC/C/GC/14, 29 de mayo de 2013.
- OCDE (2009). "The Role of Digital Identity Management in the Internet Economy: A Primer for Policy Makers", OCDE, *Documentos sobre economía digital*, núm. 160.
- OECD (2007). "At a crossroads: "Personhood" and Identity in the information society". *STI Working Paper 2007/7*. Recuperado de: <https://www.oecd.org/sti/ieconomy/40204773.doc>
- OECD (2008). "The Scoping Paper on Online Identity Theft: Ministerial Background Report" DSTI/CP(2007)3/FINAL. Recuperado de: <http://www.oecd.org/sti/40644196.pdf>
- OECD (2015). "Developments in digital identity". SPDE Roundtables 1-2 December 2015. Recuperado de: [https://one.oecd.org/document/DSTI/ICCP/REG\(2015\)12/en/pdf](https://one.oecd.org/document/DSTI/ICCP/REG(2015)12/en/pdf)
- ORGANIZACIÓN MUNDIAL DE LA SALUD, "Registro civil: por qué es importante contabilizar los nacimientos y las defunciones", *Centro de Prensa, notas descriptivas*, OMS, 30 de mayo de 2014.
- Pacto Internacional de Derechos Civiles y Políticos, adoptado y abierto a la firma, ratificación y adhesión por la Asamblea General de las Naciones Unidas en su Resolución 2200 A (XXI) del 16 de diciembre de 1966; entrada en vigor el 23 de marzo de 1976, artículo 24
- PACHECO, Máximo G., *Los derechos fundamentales de la persona humana*, Instituto Interamericano de Derechos Humanos, Serie de Estudios de Derechos Humanos, Tomo II, 1999.
- PROGRAMA NACIONAL DE DERECHOS HUMANOS 2020-2024, publicado en el Diario Oficial de la Federación el 10 de diciembre de 2020. Recuperado de: http://dof.gob.mx/nota_detalle.php?codigo=5607366&fecha=10/12/2020
- PEREZ Burgueño, P. (2012). "Aspectos jurídicos de la identidad digital y la reputación online." 2012. Recuperado de: <http://www.adcomunicarevista.com/ojs/index.php/adcomunica/article/view/50>

- REGISTRO NACIONAL DE POBLACIÓN, Acciones y Programas, “Derecho a la identidad, la puerta de acceso a tus derechos”, Agosto, 2019. Recuperado de: <https://www.gob.mx/segob/renapo/acciones-y-programas/derecho-a-la-identidad-la-puerta-de-acceso-a-tus-derechos>
- REGISTRO NACIONAL DE POBLACIÓN, Acciones y Programas, “Derecho a la identidad, la puerta de acceso a tus derechos”, SEGOB, Agosto, 2019.
- 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. Publicado el 4 de mayo de 2016 en el Diario Oficial de la Unión Europea, Hecho en Bruselas, el 27 de abril de 2016 y será aplicable a partir del 25 de mayo de 2018.
- SÁNCHEZ-CORDERO DÁVILA, Jorge A, *Derecho Civil, Introducción al derecho mexicano*, México, Universidad Nacional Autónoma de México, 1981.
- SANTOS, Díaz, “Construcción de la identidad digital a través del yo-objeto: proceso de auto-objetivación y su relación con la cosificación del cuerpo de las mujeres”, *Revista E. Teknokultura* 15(2), 2018.
- SECRETARÍA DE GOBERNACIÓN, *El derecho a la identidad como derecho humano*, México, SEGOB, 2010.
- SUPREMA CORTE DE JUSTICIA de la Nación. (2014, octubre). Tesis 1a. CCCLIV/2014. DIGNIDAD HUMANA. CONSTITUYE UNA NORMA JURÍDICA QUE CONSAGRA UN DERECHO FUNDAMENTAL A FAVOR DE LAS PERSONAS Y NO UNA SIMPLE DECLARACIÓN ÉTICA. Gaceta del Semanario Judicial de la Federación. Décima época. Tomo I, p. 602.
- TAMARGO María del Carmen, “Identidad legal, ciudadanía y vulnerabilidad social. Notas para el estudio del subregistro de nacimientos y la indocumentación con perspectiva de género y etnicidad.”, *XXVII Congreso de la Asociación Latinoamericana de Sociología*. VIII Jornadas de Sociología de la Universidad de Buenos Aires. Asociación Latinoamericana de Sociología, Buenos Aires, 2009.

- TÉLLES Valdés, Julio. *Derecho Informático*, Instituto de Investigaciones Jurídicas, Textos y Estudios Legislativos, Núm. 75, 1ª ed. Ed., Instituto de Investigaciones Jurídicas, UNAM, México 1991.
- TÉLLEZ, Carvajal Evelyn, *Derecho y TIC. Vertientes Actuales*. Instituto de Investigaciones Jurídica, UNAM, INFOTEC, Serie Doctrina Jurídica, num. 751, México, 2016.
- TENORIO Cueto Guillermo A. “La muerte digital, Desafíos de la protección de datos de las personas fallecidas”. *Conferencia IDAIP Quintana Roo*, 25 de septiembre de 2020. Recuperado de: http://www.idaipqroo.org.mx/archivos/institucion/capacitacion/pdf/2020/conferencia_muerte_digital_desafios_proteccion_de_datos_de_personas_fallecidas.pdf
- TREVIÑO García Ricardo, *La persona y sus atributos*, Universidad Autónoma de Nuevo León Facultad de Derecho y Criminología, 2002.
- UNICEF, “Derecho a la identidad. La cobertura del registro de nacimiento en México.” Enero, 2019. Recuperado de: https://www.unicef.org/mexico/media/1016/file/UNICEF_Derecho%20a%20a%20identidad.pdf
- UNICEF, “Registro de Nacimiento en América Latina y el Caribe, Panorama regional”, Oficina Regional de UNICEF para América Latina y el Caribe, *Boletín No. 1*, 15 de julio de 2011. Recuperado de: [http://www.unicef.org/lac/UNICEF_TACRO_boletin_registro_de_nacimiento_06152011\(3\).pdf](http://www.unicef.org/lac/UNICEF_TACRO_boletin_registro_de_nacimiento_06152011(3).pdf)
- WESTIN, Alan, “Privacy and Freedom”, *Nueva York, Ateneum*, 1967.
- WORLD BANK, “*Digital Identity Toolkit*”, *Working Paper*, Washington DC. 2014. Recuperado de: <http://documents.worldbank.org/curated/en/2014/06/20272197/digital-identity-toolkit-guide-stakeholders-africa>
- WORLD BANK, “Identification for Development Strategic Framework”, *Working Paper*, Washington D.C. 2016.

WORLD ECONOMIC FORUM. "A Blueprint for Digital Identity The Role of Financial Institutions in Building Digital Identity", *Part of the Future of Financial Services Series*, 2016.

WORLD ECONOMIC FORUM. *The Global Risks Report 2020*, 15th Edition.
Recuperado de:
http://www3.weforum.org/docs/WEF_Global_Risk_Report_2020.pdf

Imágenes del Anexo (Manual): Imágenes de uso libre, Recuperado de:
<https://www.canva.com/>