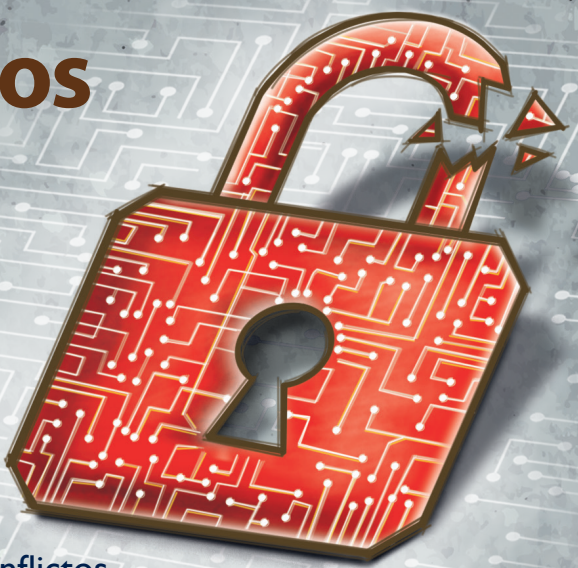
Revista Mexicana de Ciencias Penales

ISSN 0187-0416

Año 3 • Número 10 • enero-abril de 2020 • $100.00

Ciberdelitos



- Tecnología, derecho y conflictos
  Bibiana Beatriz Luz Clara
- Convertir una debilidad en fortaleza. Primeras experiencias acumuladas
  Damián Paret Francia
- Los Estados, las criptomonedas y la ciberseguridad
  Humberto Martín Ruani
- Las operaciones con recursos de procedencia ilícita y las *fintech*: responsabilidad penal de las personas morales
  Alberto Enrique Nava Garcés

INACIPE
INSTITUTO NACIONAL DE CIENCIAS PENALES

LA IDENTIDAD EN LA ERA DIGITAL

Alicia Rubí Guerra Valdivia*

*Actualmente labora en el Consejo de la Judicatura Federal. Cuenta con la certificación Ethical Hacking and Countermeasures (CEHv7).

PALABRAS CLAVE *KEYWORDS*

Biometría	*Biometrics*
Datos	*Data*
Derecho	*Law*
Identidad	*Identity*

Resumen. Las tecnologías de la información y comunicación representan un gran avance en la sociedad, así como un reto en cuanto a una adecuada legislación y tratamiento. En el presente artículo se destacan algunos retos que enfrentamos al respecto, evidenciando el papel tan trascendente que también nos corresponde a los que hacemos uso de la tecnología.

Abstract. The information and communication technologies represent a great development in society, but also implies a huge challenge in terms of its adequate legislation. This article highlights some challenges we face as a society in this regard and prove the important role that also come into those who make use of technology in daily basis.

SUMARIO:

I. IDENTIDAD E IDENTIDAD DIGITAL

La identidad es un término multívoco, su significado variará dependiendo del área de aplicación; por lo que, en un sentido general, podemos precisar dos características principales: la primera señala las particularidades de un objeto que lo distinguen de los demás; y la segunda determina las peculiaridades que permiten asegurar que es el mismo objeto en distintos momentos del tiempo. Estas dos características nos permiten forjar una correlación, ya que podemos distinguir un objeto de otros si este dura en el tiempo, y, solamente tiene sentido decir que un objeto permanece si podemos singularizarlo frente a los demás (Villoro, 2016: 190).

Bajo este aspecto, dentro del ámbito jurídico, nuestro máximo tribunal se ha pronunciado acerca de lo que entendemos por derecho a la identidad, el cual postula que toda persona desde su nacimiento debe acceder a una identidad, la cual se entiende como el conjunto de rasgos propios de un individuo que lo caracterizan frente a los demás y que le dan consciencia de sí mismo; razón por la cual se relaciona con otros derechos fundamentales como el nombre, nacionalidad, la filiación o personalidad jurídica.

Hoy en día, con el uso de las tecnologías de la información y comunicación, queda clara la necesidad —creada y aceptada— de forjar una identidad digital,[1] pues en la mayoría de los casos no es suficiente contar con una identidad, sino que es menester crearla digitalmente. Nativos y migrantes digitales disponemos de una comunicación más ubicua, portátil e inmediata y podemos notar algo que no puede pasar desapercibido: la creación de nuestra identidad digital.

Podemos entender como identidad digital al conjunto de datos relacionados a una entidad. Dicha información representa a esa entidad frente a terceros, situación que

[1] Cabe destacar que en 2018 se llevó a cabo en México el denominado *Primer Seminario de Identidad Digital en México.* En mayo de 2019, *El Economista* presentó una nota de la cual se advierte —entre otras cosas— la idea de una asociación de identidad digital a partir del seminario en comento, además del fomento y la ayuda a la consolidación "de ecosistemas de identidad digital en México", así como la colaboración "con las autoridades en la formación y maduración de una normativa legal para el uso de la identidad digital en México". La nota completa se encuentra disponible en la siguiente liga: https://www.eleconomista.com.mx/tecnologia/Presentan-la-Asociacion-de-Identidad-Digital-de-Mexico-20190521-0094.html

nos permite identificarnos y diferenciarnos unos de otros con ayuda de la tecnología. Compuesta de un conjunto de características diversas que cumplen con estas propiedades, resulta entonces exponencialmente trascendente la información que decidimos aportar a través de las TIC; misma que se va almacenando a medida que la proporcionamos.

Søren Aabye Kierkegaard afirmó en su momento que *la vida se vive hacia delante, pero se entiende hacia atrás*, y así sucede con nuestra identidad digital, pues los vestigios que decidimos que se queden en la red y de los que vamos haciendo partícipes a terceros serán los que nos forjen dicha identidad. Puede decirse entonces que la identidad digital, tanto de personas físicas como morales, va siendo alimentada continuamente según las necesidades que se presenten; y si para una persona física es elemental un criterio adecuado sobre la creación de esta, cabe precisar que para personas morales resulta de suma importancia la elaboración de la misma, pues debe estar basada en la seguridad, sencillez y confianza que se genere al interactuar con ellas.

II. BIOMETRÍA

Teniendo como premisa lo referido en párrafos precedentes, podemos inferir que dentro de la identidad se encuentran los datos biométricos.

La biometría[2] consiste en el reconocimiento automático de las personas en función de sus características físicas únicas y de comportamiento, por lo que debe elegirse una característica lo suficientemente variable de un individuo a otro (la cara, la huella, la geometría de la mano, el iris, la voz, las venas, el pulso cardiaco, la radiografía dental, el ADN, la forma de escribir a mano,[3] etcétera). El funcionamiento de esta tecnología consta de una parte física que en la mayoría de las ocasiones son sensores que llevan a cabo las mediciones, y una parte lógica que ejecuta las comparaciones de los datos que han sido registrados previamente (Cortés, Medina y Muriel, 2010), valiéndose del reconocimiento de formas, inteligencia

[2] No pasa desapercibido que el término de *biometría*, dependiendo del autor, puede ser tomado como una ciencia o como las técnicas de uso. Al respecto, tenemos lo siguiente:

A) Richard Hopkins (1999) en su libro, *An Introduction to Biometrics and Large Scale Civilian Identification*, señala: "La definición estricta de la biometría es la ciencia que implica el análisis estadístico de las características biológicas".

B) Por otro lado, la acepción que se le da a la misma también puede referirse como la técnica a través de la cual la estadística auxilia a diferentes ciencias para resolver problemas (King y Stansfield, 2006).

[3] También conocido como "reconocimiento de escritor", mismo que consiste en identificar al autor de determinado texto manuscrito auxiliándose de un software de reconocimiento óptico de caracteres; lo anterior, bajo la premisa de que cada persona tiene una manera única de escribir, teniendo en consideración rasgos propios e inconfundibles para las letras. Situación que, indiscutiblemente, nos remite a los peritos en grafoscopía.

artificial, algoritmos matemáticos y aprendizaje de computadoras, entre otras cosas.

A. DATOS BIOMÉTRICOS

En razón de lo anterior, podemos identificar como dato biométrico a aquel que surge a través de un proceso de registro o codificación de las características de la persona física a la que corresponde el registro y la hace identificable entre los demás.

Los motivos para hacer uso de la biometría son variables y con frecuencia coinciden (Pato y Millett, 2010). Esto es, se piensa en un mejoramiento en la eficiencia de transacciones y acceso,[4] en reducir el fraude y la usurpación de identidad y, por supuesto, en una mejora en cuanto seguridad pública y privada, entre otras cosas. No obstante ello, habrá que cuestionarse la efectividad, el uso correcto y la manipulación de los mismos;[5] contextos variables que se ven reflejados en un impacto social y en consecuencias de privacidad por sus secuelas legales y políticas.

Como se ha planteado a lo largo de este artículo, la identidad se forja a partir de ciertas características y datos que son propios de cada persona física o moral, por lo que se estima necesario destacar que el buen uso de los datos biométricos parte de la trascendencia que estos tienen al ser considerados bajo ciertas circunstancias y para efectos legales, como datos personales. El Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales se ha pronunciado al respecto (INAI, 2018), haciendo hincapié en que un dato biométrico aislado que no esté registrado en un sistema biométrico y no pueda ligarse con una persona física particularmente o sea comparado con otras muestras no tiene el carácter de dato personal, ya que no puede identificar a su titular.

Caso similar sucede al darles el carácter de dato personal sensible, pues deberá cumplir con alguno de los supuestos contemplados por las leyes en materia de protección de datos, estos es: primero, la afectación de la esfera más íntima del titular;

[4] A manera de ejemplo, tenemos el caso del banco británico Barclays, que desde 2014 anunció el ofrecimiento para que, a partir de 2015, sus clientes contaran con la posibilidad de tener acceso a sus cuentas bancarias a través de un lector biométrico que detectaba las venas del dedo índice de cada cliente con el fin de dificultar el fraude por usurpación de datos personales.

[5] Uno de los casos más recientes es el de la aplicación FaceApp, que volvió a ser tendencia (después de 2017). Esta "novedad", alentaba a usuarios para que a través de dicha aplicación y por medio de su filtro "edad", compartieran fotografías en sus redes sociales (en su mayoría, aunque no limitativamente) con su rostro cambiado para simular un envejecimiento. Los términos y condiciones de la aplicación en comento no varían tanto respecto de otras, poniendo nuevamente de manifiesto cómo renunciamos a nuestra privacidad sin ser conscientes del alcance de ello; dejándonos, entre otras cosas, vulnerables a ser capturados digitalmente en usos de reconocimiento facial futuros.

segundo, que el uso indebido pueda dar origen a discriminación; y, tercero, que conlleve al titular a un riesgo grave.

Lo anteriormente abordado puede brindar un panorama general respecto a los casos en los que los datos biométricos son considerados como datos personales y datos personales sensibles; y, consecuentemente, proporcionar indiscriminadamente a terceros nuestros datos biométricos puede tener consecuencias desfavorables.

Actualmente, nos enfrentamos a la poca claridad referente a los datos biométricos y su adecuada protección en la legislación mexicana. Situación que se encuentra ligada a la falta de información por la cual se dan a conocer los mecanismos usados en la recolección, almacenamiento y análisis de los datos biométricos, así como del alcance de las políticas de los que tendrán la información en comento, o bien, si serán compartidos o transferidos entre distintos organismos públicos y privados y bajo qué circunstancias; por lo que la insuficiencia de una regulación apropiada al respecto no permite garantizar en su totalidad el tratamiento correcto de los datos biométricos, aun cuando los sujetos obligados tengan una serie de obligaciones. Esto, en razón de que los sistemas de identificación biométricos incrementan los riesgos de falsos positivos y de irrupciones a bases de datos que los contengan, en comparación a los riesgos de seguridad asociados a sistemas de identificación tradicionales.

Como hemos observado, dos de las características con las que cuentan estos datos es que son únicos e irremplazables, lo cual significa que se debe de tener especial cuidado para protegerlos de *robo*[6] o pérdida para que la identidad del titular no se vea comprometida, así como regular específicamente lo que pasaría bajo estos supuestos.

III. USURPACIÓN DE IDENTIDAD

La usurpación de identidad es una conducta ilícita que ha sido y sigue siendo una actuación que se encuentra presente prácticamente en cualquier ámbito de la sociedad.

Arreola González señala:

> El delito de usurpación de identidad, se tipifica como una conducta antijurídica, dolosa que emana de un individuo

[6] El director ejecutivo de la Red en Defensa de los Derechos Digitales, Luis Fernando García, hizo un señalamiento interesante en cuanto a datos biométricos: "El riesgo es mayor en comparación con otros datos, porque no se pueden cambiar. Por ejemplo, si te roban la contraseña, la puedes cambiar. Pero si se trata de las huellas digitales, no se puede. Y esos datos en manos equivocadas es muy peligroso". La nota completa está disponible en https://www.proceso.com.mx/464952/sistemas-biometricos-identificacion-los-ciber-riesgos. Consultado en línea el 04 de agosto de 2019.

> que dispone de la información personal de otro, sin su autorización con el ánimo de cometer una diversidad de delitos, manipulando diferentes fuentes para obtener la información íntima de una persona a través de un engaño hacia la víctima, y al mismo tiempo, maniobrando diversos medios convencionales y Tecnologías de la Información y Comunicación para realizar el delito, originándole un daño patrimonial o moral. (Arreola, 2017: 9)

En un ámbito penal, y por lo que hace a la legislación mexicana, el delito de usurpación de identidad se contempla únicamente en algunas leyes estatales,[7] encontrando la conducta en comento como usurpación de identidad o suplantación de identidad; lo que inevitablemente nos dirige a un tema de suma trascendencia, el cual se ha comentado: un Código Penal Nacional en México.

Al respecto, cabe precisar que el experto penalista, el doctor Alberto Enrique Nava Garcés, ha manifestado acertadamente en ocasiones previas la importancia de la realización de este proyecto, pues, tal como lo refirió, nos enfrentamos a la necesidad de:

> … contar con un sistema de justicia penal homologado, que tenga aplicación en todo el territorio y no permita que se formen nichos de impunidad derivados de los tantos códigos penales que regulan las conductas reprochables tanto en el ámbito federal como en las distintas entidades.[8]

Unificar criterios disímiles que prevalecen en las legislaciones locales implicaría emitir un criterio jurídico genuino a partir de casos concretos y subsanar el vacío jurídico que actualmente enfrentamos al respecto.

A. USURPACIÓN DE IDENTIDAD A TRAVÉS DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN

Dentro de la cadena de seguridad informática, el eslabón más débil es el factor humano; por ello, dentro de las técnicas que pueden ser útiles con el fin de cometer actos ilícitos, en este caso en particular la usurpación de identidad, podemos citar la ingeniería social.

[7] En el ámbito estatal, el delito de usurpación de identidad se encuentra contemplado en los códigos penales de: Durango, Colima, *Distrito Federal*, Hidalgo, Zacatecas, Nayarit, Baja California Sur, Tlaxcala, Guanajuato, Estado de México, Michoacán de Ocampo, Tamaulipas y Quintana Roo.

Por otro lado, una conducta delictiva similar tipificada como suplantación de identidad se contempla en los códigos penales de Campeche, Sinaloa, Chiapas, Nuevo León y Baja California.

[8] La entrevista realizada en mayo de 2018 al Dr. Enrique Alberto Nava Garcés puede ser consultada en su totalidad en la siguiente liga: https://elmundodelabogado.com/revista/posiciones/item/las-nuevas-tecnologias-y-el-codigo-penal-nacional. Consultado en línea al 30 de julio de 2019.

B. INGENIERÍA SOCIAL

La ingeniería social es la acción o conducta social destinada a conseguir información de las personas cercanas a un sistema con la finalidad de obtener datos de interés valiéndose de habilidades sociales. Dichas prácticas se encuentran relacionadas con la comunicación entre seres humanos (Borghello, 2019: 2).

Asimismo, podemos dividir la ingeniería social en dos factores principales: 1) técnicas que se valen de la interacción con máquinas; y 2) las basadas en la interacción humana (Xiangyu, Qiuyang y Chandel, 2017: 25-34); por consiguiente, la mayoría de los ataques aumentan sus posibilidades de éxito a partir de la combinación de ambos elementos.

Es importante puntualizar que la conducta delictiva podrá llevarse a cabo de forma directa o indirecta (Salahdine y Kaabouch, 2019). Para el caso de los ataques clasificados de forma directa, se usa el contacto directo entre el atacante y la víctima para realizarlo. En esta categoría podemos mencionar los que son realizados por contacto físico, visual o interacciones de voz. Cabe precisar que también pueden requerir la presencia del atacante en el área de trabajo de la víctima. A manera de ejemplificación, encontramos: acceso físico, *shoulder surfing*,[9] *dumpster diving*,[10] ingeniería social telefónica, suplantación en llamadas y robo de documentos importantes, entre otras.

Ahora bien, por lo que hace a los ataques llevados a cabo de forma indirecta, bastará precisar que estos no requieren la presencia del atacante para llevarse a cabo, es decir, el ataque se puede lanzar de forma remota a través de un *software* malicioso por archivos adjuntos de correo electrónico o mensajes. Ejemplos de estos ataques son: *phishing*,[11] *software* falso, ventanas emergentes, *ransomware*,[12] *smishing*[13] e ingeniería social inversa.[14]

[9] *Shoulder surfing*: es la técnica de observación directa al usuario para obtener datos.

[10] *Dumpster diving*: es la revisión de los papeles y documentos que se tiran a la basura y no son destruidos de manera segura.

[11] *Phishing*: técnica para intentar adquirir datos confidenciales, como números de cuenta bancaria, a través de una solicitud fraudulenta por correo electrónico o de un sitio web, en el que el atacante se hace pasar por una persona legítima.

[12] *Ransomware*: tipo de malware que intenta denegar a un usuario el acceso a sus datos, generalmente cifrándolos con una clave conocida por el atacante, hasta que se pague un *rescate*.

[13] *Smishing*: variante del *phishing*, es cuando alguien intenta engañar a un usuario para que proporcione información privada a través de un texto o un mensaje SMS.

[14] Ingeniería social inversa: podemos resumirla en tres pasos: sabotaje, publicidad y asistencia. En el primer paso, un atacante encuentra una manera de sabotear una red, desde lanzar un ataque contra el sitio web del objetivo o simplemente enviando un correo desde una dirección fraudulenta, haciendo creer a las víctimas la existencia de un problema. Posteriormente, el atacante da a conocer una "solución" a la problemática suscitada. Finalmente, la víctima (habiendo sido engañada) contacta al atacante y le brinda accesos, por lo que, habiendo

Sin duda, quien lleve a cabo la suplantación se vale de técnicas y habilidades en cuanto al lenguaje, pues se presupone una interacción con la víctima, por lo que el atacante depende en gran medida de su capacidad para desarrollar una relación de confianza con el objetivo y hacer una primera impresión positiva para ganarse la confianza de la víctima.[15]

Una vez abordado el panorama que precede, se estima conveniente hacer notar la diferencia que existe entre identidad digital y reputación digital, ya que, si bien la primera es la que cada persona física o moral se forja en línea respecto de sí misma, la variante radica en que la segunda dependerá de los juicios que terceros emitan al respecto,[16] de modo que la reputación es una consecuencia de la identidad.

Un atributo característico de la identidad que vamos formando en la red es la libertad que tenemos para compartir datos personales de manera voluntaria, expresar opiniones y el acceso a una gran cantidad de información. Según Lichtenberg *no hay que juzgar a los hombres por sus ideas, sino por aquello en lo que sus ideas los convierten*; e invariablemente nos damos a esa tarea ayudados de la tecnología, ya sea creando opiniones respecto de nuestra persona o la de terceros, dando pie a una ilusión de convivencia perfectamente trabajada, aunque no siempre en el mejor sentido. Nuestro derecho a una libre expresión lleva consigo la obligación de un buen criterio y respeto.

IV. LIBERTAD DE EXPRESIÓN

Es de gran trascendencia e impacto el buen criterio que debe de imperar al forjar y seguir alimentando nuestra identidad digital, lo que inevitablemente nos remite a otro derecho: la libertad de expresión.

La Suprema Corte de Justicia de la Nación se ha pronunciado respecto a la libertad de expresión y

obtenido el acceso, se podrán implementar *loggers*, robar datos confidenciales, etcétera.

[15] Aun cuando las diversas instituciones bancarias han advertido a sus clientes que no se revelen datos sensibles respecto de sus cuentas por teléfono —o cualquier otro medio—, los atacantes siguen valiéndose de llamadas telefónicas para obtener dicha información y llevar a cabo diversas conductas delictivas.

La Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros hace referencia a que México ocupa el octavo lugar a nivel mundial en el delito de robo de identidad; asimismo, indica que el 67% es por pérdida de documentos, 63% por robo de cartera y portafolio y el 53% por información tomada de una tarjeta bancaria. La nota completa se encuentra disponible en https://www.condusef.gob.mx/Revista/index.php/usuario-inteligente/consejos-de-seguridad/563-robo-de-identidad, y las estadísticas en https://www.condusef.gob.mx/gbmx/?p=estadisticas. Sitios consultados el 01 de agosto de 2019.

[16] En concordancia con lo referido por Carlos Pinzón al hacer hincapié en que la identidad digital es pilar de la reputación *on-line*, se estima que una no puede subsistir sin la otra. http://www.inveniopro.es/diferencia-entre-identidad-digital-y-reputacion-on-line/. Consultado en línea al 30 de julio de 2019.

sus diversas vertientes. Caso concreto podemos remitirnos a la resolución de 20 de junio de 2013 relativa a la acción de inconstitucionalidad 29/2011,[17] en la cual nuestro máximo tribunal esclarece lo siguiente:

> … la libertad de expresión constituye un derecho preferente, ya que sirve de garantía para la realización de otros derechos y libertades.[18] En efecto, tener plena libertad para expresar, recolectar, difundir y publicar informaciones e ideas es imprescindible, no solamente como instancia esencial de auto-expresión y auto-creación, sino también como premisa para poder ejercer plenamente otros derechos humanos –el de asociarse y reunirse pacíficamente con cualquier objeto lícito, el derecho de petición o el derecho a votar y ser votado– y como elemento funcional que determina la calidad de la vida democrática de un país.

En México tenemos derecho a gozar de un ámbito de proyección de existencia que quede reservado de la invasión y la mirada de los demás y que a su vez provea de las condiciones necesarias para el despliegue de nuestra identidad, compartiendo de manera consciente la información que estimemos adecuada y/o necesaria para un fin en particular. Por lo que, en un sentido más amplio, la protección de nuestra información también dependerá en gran medida del buen criterio que cada persona tenga al brindar de alguna manera ciertos datos.

Hoy en día, las TIC representan un medio esencial para la creación de nuestra identidad digital. Compartir lo que pudieran ser elaboradas peroratas no siempre resulta lo más conveniente, ya que, ocasionalmente, un error se disfruta como virtud. En el mundo digital actual podemos excusarnos en interpretaciones y sentidos dirigidos a ideas concretas, creamos continuamente la ilusión de un idioma privado compartido en forma íntima únicamente con aquellos que no difieren con nuestro pensar.

La libertad de expresión da pauta a que de manera simultánea nos equivoquemos u ofendamos al manifestar nuestro derecho de pensar y expresarnos; sin embargo, el respeto es un valor moral que las leyes no pueden imponer —independientemente de los indicios que haya al respecto—, situación que nos ha llevado a conformarnos con un instrumento más modesto: la tolerancia.

En varios casos, nuestro derecho a la libertad de expresión ha sido usado, no solamente para una confrontación de opiniones, sino también para proliferar inexactitudes

[17] Disponible en: http://www2.scjn.gob.mx/ConsultaTematica/PaginasPub/DetallePub.aspx?AsuntoID=132774. Consultado el 30 de julio de 2019.

[18] Por ejemplo, la Primera Sala ha desarrollado su doctrina sobre este tema, principalmente, en el amparo directo en revisión 2044/2008, sentencia de 17 de junio de 2009, en el amparo directo 28/2010, sentencia de 23 de noviembre de 2011 y en el amparo directo 8/2012, sentencia del 4 de julio de 2012.

y calumnias, creando noticias falsas para ser propagadas. Es evidente que la falsedad en las noticias tiene mejor desenlace, pero no siempre se puede ser capaz de sostener un repertorio de engaños. La desventaja radica en las consecuencias generadas a partir de la desinformación y, por supuesto, el engaño del que se hace partícipes a los usuarios.

A. NOTICIAS FALSAS

Las noticias falsas son también conocidas como *fake news,* término usado para conceptualizar la divulgación de noticias falsas que generan un círculo de desinformación. Las redes sociales permiten y facilitan que los usuarios sean productores y consumidores de diversos contenidos a la vez, y favorecen la difusión de información engañosa, falsa o fabricada (FIP, 2018).

Bajo ciertas circunstancias pareciera que el inventar noticias falsas cumple con una necesidad social y no necesariamente dotada de sentido común, pues la desinformación en internet es de los principales peligros a los que se puede enfrentar una sociedad democrática. A través de varios heterónimos, y a veces sin valerse de estos, se crean noticias falsas cuyo objetivo puede ser directamente una afectación económica, o bien, un objetivo ideológico de cualquier índole.

Valerse de la tecnología para acceder a la información ha dado lugar a que la autenticidad de las notas esté aún más cuestionada, o por lo menos así debería de ser bajo determinadas circunstancias. Otorgar inmediatamente el carácter de auténtico a la información que se comparte por medios sociales ha dejado de resultar la mejor forma de estar adecuadamente informado, pues la popularidad de una noticia, el grado en que esta genere indignación, los sesgos de confirmación y el nivel de implicación de las personas con los contenidos son elementos esenciales para impulsar su propagación, y, conjugados estos, los contenidos se vuelven virales a gran velocidad y escala, con independencia de la veracidad que los inviste (Bradshaw y Howard, 2018).

La gran mayoría hemos sido espectadores —por lo menos— de la enorme influencia que ejercen las redes sociales en la propagación de información, de ahí que derive la trascendencia política al valerse de estas plataformas; movimientos sociales siguen apoyándose de estas para asegurar y generar un gran impacto en distintos ámbitos.

En México, nuestro Código Penal Federal contempla sanciones para la propalación dolosa de noticias falsas por lo que hace a la economía

pública y las jornadas electorales (CPF, arts. 254, fr. III; 405, fr. XI y 406, fr. V). En esta misma línea, en algunos estados existen normativas estatales que contemplan conductas como el *ciberacoso,* abordando vagamente la idea del uso de las TIC como instrumento de hostigamiento o amenaza; sin embargo, uno de los grandes retos es encontrado en el desafío de diseñar e implementar soluciones que regulen a las redes sociales de forma tal que se evite una interferencia política autoritaria sin reprimir la libertad de expresión, pues existe una delgada línea entre nuestro derecho fundamental y la supresión de contenido perjudicial para la sociedad, sobre todo dentro de un ámbito político. En ese sentido, las mejores estrategias serán las decisiones tomadas a partir del buen criterio de los usuarios, razón por la cual es tan importante fomentar una cultura que valore y promueva la verdad, así como que reconozca la diferencia entre especulación y verdad.

V. CONCLUSIONES

Sin duda, nuestras condiciones de vida se ven mejoradas con las TIC y aun con ellas seguimos dando un valor a nuestra necesidad de existencia, lo que se traslada al ámbito digital. La interacción con personas nos permite experimentar el sentimiento de ocupar un lugar en el vínculo social, dando pie al disfrute de una autonomía y suficiencia personal para formar nuestra identidad.

Los datos biométricos forman parte de nuestra identidad. Aun cuando los sistemas de reconocimiento humano son falibles,[19] la posibilidad de error es mínima, por lo que se resalta la importancia en el robustecimiento de los sistemas biométricos, particularmente a medida en que estos vayan cobrando importancia, considerando que lo óptimo es que el diseño y la evaluación de estos sea bajo contextos específicos y no genéricos, pues su efectividad dependerá en gran medida del entorno social y del fortalecimiento de la tecnología y

[19] Las características biológicas de cada persona están sujetas a cambios, por lo que se estima que la biometría no es, en consecuencia, una ciencia exacta, debiendo de tener en consideración la gran variante de mecanismos que existen para la interpretación de datos, así como también las diferentes condiciones ambientales que imperaron al momento de que los datos en comento fueron capturados. A manera de ejemplo podemos citar las huellas digitales, que pueden ser marcadas o mutiladas deliberadamente de manera temporal, dañadas por factores externos o distorsionadas al momento de colocar el dedo; situaciones que hacen que la biométrica de una huella digital se torne variable, lo que puede generar que la confiabilidad del proceso de identificación se complique.

Lo mencionado en el párrafo precedente compete a una calidad biométrica que se enfoca a una calidad de muestra, sin embargo, se destaca la importancia que tienen los metadatos en los sistemas operativos, pues "las bases de datos necesitan estar al tanto de las relaciones erróneas entre los elementos de los datos, los cuales generalmente se generan por causas administrativas más que por causas biométricamente específicas". (Moses, s.f.)

seguridad que impliquen. El uso de la tecnología conjuntado con la biometría da resultados altamente eficientes para acelerar el proceso de identificación, haciéndolo práctico, rentable y preciso; empero, representa todavía un gran desafío tanto en un ámbito de funcionamiento eficiente y fiable como en la legislación al respecto.

En la usurpación de identidad, los ataques serán tan variados como la capacidad de quien los diseñe lo permita. Nos enfrentamos a una conducta delictiva que repercute en diversos ámbitos, ya sea con entidades bancarias o en las propias redes sociales al ser víctimas de la creación de perfiles falsos, por mencionar algo. Es por ello que es de gran trascendencia la mesura y el buen criterio que los usuarios debemos tener al compartir nuestros datos, pues en una era donde las diversas plataformas son parte de nuestro entorno, valorar nuestros datos personales ayudaría a mitigar la problemática que representa la usurpación, ya que un atávico sentido de prudencia podría evitar consecuencias adversas. Cabe precisar que no se pretende llegar a extremos de posturas como solución, sino que el buen uso de nuestra información dependerá de la colaboración de quien la brinde, quien la obtenga y su adecuada regulación.

Finalmente, se debe de considerar al hacer frente a los vacíos legales que, aun cuando la interpretación de diversas disposiciones en cuanto a la seguridad que se brinda a la identidad de una persona destaca que las personas pueden expresar libremente su identidad (en relaciones con la sociedad o en lo individual), vale la pena enfatizar su vinculación con otros derechos, por lo que las afirmaciones contenidas en las regulaciones deben ser útiles en la medida en que no sean tomadas de forma descontextualizada y surja su correcta interpretación a partir de un análisis minucioso entre los diferentes escenarios jurídicos en los que se encuentren en riesgo los derechos de las personas.

VI. FUENTES DE CONSULTA

Arreola González, J. (2017). *Delito de usurpación de identidad. La homogeneización del sistema jurídico*. México: Flores.

Borghello, C. (abril de 2009). "El arma infalible: la Ingeniería Social", en *Technical & Educational Manager de eset para Latinoamérica*, p. 2. Disponible en http://www.eset-la.com/pdf/prensa/informe/arma_infalible_ingenieria_social.pdf. Consultado el 31 de agosto de 2019.

Cooke, K. (31 de octubre de 2017). "'Fake news' reinforces trust in mainstream new brands". En Kantar UK. Disponible en https://uk.kantar.com/business/brands/2017/trust-in-news/

Cortés Osorio, J., Medina Aguirre, F. y Muriel Escobar, J. (diciembre de 2010). "Sistemas de seguridad basados en biometría". En *Scientia et Technica*, XVII, (46), Colombia: Universidad Tecnológica de Pereira. Disponible en https://www.redalyc.org/pdf/849/84920977016.pdf. Consultado el 02 de agosto de 2019.

Department of Homeland Security (24 de Agosto de 2017). *The future of ransomware and social engineering*. Disponible en https://www.dni.gov/files/PE/Documents/6---2017-AEP_The-Future-of-Ransomware-and-Social-Engineering.pdf

Díaz Limón, J. (2019). *Abogado digital, estudios sobre derecho cibernético, informático y digital*. México: Vlex.

Doctor, K. (26 de septiembre de 2017). "Newsonomics: Our Peggy Lee moment: Is that all there is to reader revenue?". En *NiemanLab*. Disponible en https://www.niemanlab.org/2017/09/newsonomics-our-peggy-lee-moment-is-that-all-there-is-to-reader-revenue/

FIP (2018). *¿Qué son las fake news? Guía para combatir la desinformación en la era de la posverdad*. Documento disponible en https://www.ifj.org/fileadmin/user_upload/Fake_News_-_FIP_AmLat.pdf. Consultado en línea el 06 de agosto de 2019.

Grevtsova, I. (9 de mayo de 2015). "¿Qué es el patrimonio digital?". En Digital Heritage & Culture. Disponible en https://irinagrevtsova.com/que-es-patrimonio-digital/

Google (febrero de 2019). *How Google Fights Disinformation*. Disponible en https://storage.googleapis.com/gweb-uniblog-publish-prod/documents/How_Google_Fights_Disinformation.pdf

Herrán Aguirre, A. (2019). *Libertad de expresión y el internet*. México: Tirant lo Blanch.

Hopkins, R. (1999). "An introduction to biometrics and large scale civilian identification". En *International Review of Law, Computers & Technology*, 13(3), Yarm, UK, pp. 337-363.

IFAI (2018). *Guía para el tratamiento de datos biométricos*. Documento disponible en http://inicio.ifai.org.mx/DocumentosdeInteres/GuiaDatosBiometricos_Web_Links.pdf. Consultado en línea el 04 de agosto de 2019.

King, R. y Stansfield, W. (2006). *A Dictionary of Genetics*. Nueva York: Oxford University Press.

Lira Arteaga, O. (2018). *Cibercriminalidad. Fundamentos de investigación en México*. México: Ubijus.

Nava Garcés, A. (Coord). (2019). *Ciberdelitos*. México: Tirant lo Blanch.

Moses, K. (s.f.). *Sistema Automatizado de Identificación de Huellas Dactilares (afis)*, Documento disponible en https://www.ncjrs.gov/pdffiles1/nij/250979.pdf. Consultado el 04 de agosto de 2019.

OEA. Declaraciones conjuntas. Disponible en http://www.oas.org/es/cidh/expresion/documentos_basicos/declaraciones.asp

Salahdine, F. y Kaabouch, N. (2 de abril de 2019). "Social Engineering Attacks: A Survey". En *Future Internet*, 11(89), USA: School of Electrical Engineering and Computer Science, University of North Dakota.

Pato, J., y Millet, L. (2010). *Biometric Recognition: Challenges and Opportunities*. Washington: National Academy of Sciences. Disponible en https://dataprivacylab.org/TIP/2011sept/Biometric.pdf. Consultado en línea al 03 de agosto de 2019.

Redacción (26 de diciembre de 2018). "Code of Practice on Disinformation". En Digital Single Market. Disponible en https://ec.europa.eu/digital-single-market/en/news/code-practice-disinformation

Redacción (13 de septiembre de 2019). "Tackling online disinformation". En Digital Single Market. Disponible en https://ec.europa.eu/digital-single-market/en/tackling-online-disinformation

Toler, A. (19 de febrero de 2019). "Using the New Russian Facial Recognition Site SearchFace". En Bellingcat. Disponible en https://www.bellingcat.com/resources/how-tos/2019/02/19/using-the-new-russian-facial-recognition-site-searchface-ru/

UNESCO (2018). *Journalism, fake news & disinformation*. París, France: United Nations Educational, Scientific and Cultural Organization. Disponible en https://en.unesco.org/sites/default/files/journalism_fake_news_disinformation_print_friendly_0.pdf

UNESCO (s.f.). "El patrimonio digital". Disponible en https://es.unesco.org/themes/information-preservation/digital-heritage

Villoro, L. (2016). *La significación del silencio y otros ensayos*. México: Fondo de Cultura Económica.

Xiangyu, L., Qiuyang, L. y Chandel, S. (12-14 de octubre de 2017). "Social Engineering and Insider Threats". En *Proceedings*

of the International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery. Nanjing, China, pp. 25-34.

ISSN 0187-0416