



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

**“SUPLANTACIÓN DE LA IDENTIDAD DIGITAL
CON FINES DE TRATA DE PERSONAS EN
FACEBOOK”**

PROPUESTA DE INTERVENCIÓN

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

Presenta:

Efraín Aguilar Barrera

Asesor:

Maestra Evelyn Téllez Carvajal

Ciudad de México, enero 2019.



Autorización de Impresión



C4

AUTORIZACIÓN DE IMPRESIÓN

Ciudad de México, 28 de enero de 2019

La Gerencia de Capital Humano/ Gerencia de Investigación hacen constar que el proyecto terminal titulado:

"Suplantación de la identidad digital con fines de trata de personas en Facebook"

Desarrollada por el alumno

Nombre: **Efraín**

Apellido paterno: **Aguilar**

Apellido materno: **Barrera**

Desarrollado bajo la asesoría del:

Mtra. Evelyn Téllez Carvajal

Ha sido revisado y aprobado por miembro del Núcleo Académico Básico (NAB).

Por lo cual, se expide la presente autorización para impresión del proyecto terminal al que se ha hecho mención.

Vo. Bo.

A handwritten signature in blue ink, appearing to read "Gabriela", is written over a horizontal line.

Mtra. Gabriela García Acosta
Encargada de la Gerencia de Evaluación de Proyectos

*Anexar a la presente autorización al inicio de la versión impresa del proyecto integrado que ampara la misma.

Agradecimientos

Agradecemos a Dios por bendecirnos la vida, por guiarnos a lo largo de nuestra existencia, ser el apoyo y fortaleza en aquellos momentos de dificultad y de debilidad.

Gracias a mi esposa e hijos: Claudia Flores Hernández, Ian Efraín Aguilar Flores e Iker Efraín Aguilar Flores, por ser mi compañía y mi aliento en momentos de dificultad, gracias por alentar mis sueños, gracias por compartir mi visión, por confiar y creer en el blanco perfecto.

Gracias a mis padres: Raúl Aguilar Calderón y Cruz Barrera Ceron, por ser los principales promotores de mis sueños, por ser mis maestros de la vida y creer en mis proyectos de vida, por los consejos, valores y principios que nos han inculcado.

Agradecemos a nuestros docentes de la escuela INFOTEC Centro de investigación e innovación en tecnologías de la información y comunicación, por haber compartido sus conocimientos a lo largo de la preparación de nuestra profesión, de manera especial, a la Maestra Evelyn Téllez Carvajal tutora de nuestro proyecto de investigación quien ha guiado con paciencia, y su rectitud como docente, también a la Doctora Anahiby Becerril como lectora de nuestro trabajo, por sus valiosos comentarios que sirvieron para mejorar la versión final, y CONACYT Consejo Nacional de Ciencia y Tecnología por su apoyo y la beca otorgada para concluir los estudios de posgrado.

Tabla de contenido

Introducción	1
Capítulo 1: Aspectos generales de la suplantación de la identidad digital con fines de trata de personas	6
1.1 La trata de personas y del uso de medios digitales para captar a víctimas de este ilícito	6
1.2 Conceptos básicos necesarios para comprender la suplantación de la identidad digital y prevenir su uso en la trata de personas	11
1.2.1 Conceptos de identidad e identidad digital	12
1.2.2 Identidad digital como un derecho humano.....	24
1.2.3 Usurpación, suplantación y robo de identidad	28
1.3 Suplantación de identidad con fines de trata de personas en Facebook	31
1.3.1 La trata de personas en México	31
1.3.2 Antecedentes para entender qué es y cómo funciona la red social Facebook.....	37
1.3.3 Seguridad en perfiles digitales en FB	40
1.3.4 Concepto de privacidad (privacidad en Internet) y privacidad en FB	41
1.3.5 Datos y datos personales. Conceptos básicos	47
1.3.6 Protección de datos personales en FB	49
1.3.7 Suplantación de identidad en FB	51
1.3.8 El uso de técnicas de ingeniería social en FB	53
1.4 Selección de perfiles por parte de los delincuentes con fines de trata	56
1.5 ¿Cómo identificar si se es víctima de un robo de identidad?	59
Capítulo 2: Marco jurídico en materia de suplantación de identidad digital y trata de personas	62
2.1 El fenómeno de la suplantación de identidad	62
2.2 Normatividad nacional e internacional en materia de suplantación de identidad	68
2.2.1 Ley FinTech	72
2.2.2 Legislación respecto a los delitos informáticos en materia penal	73
2.2.3 Contexto internacional en materia de suplantación de identidad	80
2.3 Ejemplos de suplantación de identidad	84
2.4 Normatividad nacional en materia de trata de personas	86
2.5 Normatividad internacional en materia de trata de personas	90
2.6 Anonimato tecnológico	95
2.7 Víctimas de trata contratadas por medios digitales	96
2.8 Procedimiento para denunciar la suplantación de identidad digital en México	98
2.9 Elementos para denunciar la trata de personas en México	99
Capítulo 3: Propuestas para evitar la usurpación de identidad y alertar sobre la trata de personas que se realiza haciendo uso de Facebook	101

3.1 Entender qué es y cómo funciona Facebook.....	101
3.2 Software malicioso en Facebook.....	106
3.3 SPAM en Facebook.....	107
3.4 Condiciones de uso de Facebook	109
3.5 Seguridad y protección de datos en Facebook.....	110
3.5.1 Seguridad y protección de los usuarios en FB.....	111
3.6 Derechos del usuario.....	112
3.7 Protección de los derechos de otras personas	114
3.8 Cómo denunciar la suplantación de identidad en Facebook.....	117
3.9 El ABC para prevenir la suplantación de la identidad y la trata en Facebook.....	122
<i>Conclusiones</i>	<i>125</i>
<i>Bibliografía</i>	<i>127</i>
Cibergrafía.....	128
Normatividad	135
Hemerografía	137
Videografía.....	140
<i>Anexo e Infografía.....</i>	<i>141</i>

Introducción

Actualmente con nuestras actividades diarias exponemos nuestra identidad y nuestros datos personales¹ en diversas ocasiones, por ejemplo cuando realizamos compras y utilizamos nuestra tarjeta de crédito, esta puede ser clonada para posteriormente hacer uso de nuestros recursos económicos de manera fraudulenta; al realizar un trámite bancario nos identificamos con algún documento oficial en donde dejamos expuesto no solo nuestro nombre y nuestra firma sino nuestra dirección, nuestra edad y hasta nuestro distrito electoral; también al realizar trámites escolares, por ejemplo; proporcionamos datos como son nuestra dirección, nuestro número de teléfono de oficina o personal; al sacar una copia de nuestra identificación oficial esta puede ser escaneada para posteriormente hacer uso de todos los datos que en ella se ostentan; y así, existen distintas acciones que ponen a los individuos en riesgo de usurpación, robo o suplantación de nuestra identidad conceptos que se esclarecerán más adelante en esta propuesta de intervención.²

¹ De acuerdo a la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, publicada el 5 de julio de 2010, es su artículo 3o. fracción V. los datos personales son “Cualquier información de una persona física identificada o identificable”.

Texto de la Ley disponible en <http://www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf>, consultada el 29 de octubre de 2018.

² Para este trabajo se entiende a una propuesta de intervención como un trabajo de investigación por medio del cual se comunican los antecedentes y datos sobre una problemática determinada así como las acciones que se deben realizar para mitigar o resolver determinada situación haciendo uso de los recursos disponibles y corriendo el menor riesgo de fracaso. Es la búsqueda de una solución para arrojar resultados esperados. Es la sistematización de una idea de cambio para lograr una mejora a una situación determinada.

Actualmente nuestros teléfonos celulares se han convertido en dispositivos que almacenan ya sea en su memoria interna³ o haciendo uso del almacenamiento en la nube,⁴ una cantidad enorme de información personal. Los distintos desarrolladores de programas solicitan nuestros datos para poder utilizar ciertas aplicaciones como son las bancarias, las de juegos y las de entretenimiento. Estas aplicaciones al instalarlas nos solicitan que aceptamos, e incluso, compartamos con terceros la información solicitada.

Los usuarios de estos dispositivos constantemente somos requeridos para actualizar ciertos programas; en ocasiones estas “actualizaciones”,⁵ son

Véase Calderón Betalleluz, Víctor Manuel, “La necesidad de toda organización de contar con Proyectos de Inversión, Universidad San Martín De Porres, Perú, *Revista del Centro de Derecho y Economía*, febrero 2012.

³ Memoria interna se refiere a la Memoria ROM por sus siglas en inglés *Read Only Memory*, en donde se almacena de manera permanente determinada información, en este caso nos referimos al almacenamiento que se hace en el teléfono celular.

⁴ A diferencia del almacenamiento en los dispositivos como las memorias internas, el almacenamiento en la nube o *cloud storage* en inglés es un servicio ofrecido por algún proveedor por medio del cual los usuarios “almacenan” su información en sitios remotos haciendo uso de servidores y de una red como Internet lo que permite que se puedan ofrecer básicamente tres tipos de almacenamiento, público, privado e híbrido.

⁵ Por actualización entendemos el obtener una versión más reciente del *software* o *hardware*, en general es una mejoría a un programa que se ha instalado con anterioridad y que supone permite eliminar versiones posteriores del mismo o bien eliminar vulnerabilidades a la seguridad, principalmente aunque no exclusivamente. Lo que no se difunde mucho es que algunas de estas actualizaciones se deben precisamente por “errores” que los programadores identifican y que son necesarios para evitar fallas en las versiones posteriores.

programadas y ya ni siquiera estamos conscientes de ellas, pero que sin estas, no podríamos continuar utilizando los programas lo que haría imposible seguir recibiendo pagos, mensajes, acceder a los juegos, hacer uso de aplicaciones como las bancarias, etcétera; y es muy riesgoso no hacerlas inmediatamente puesto esto ocasiona el aumento de la inseguridad en los dispositivos móviles y es más fácil que la información sea robada e incluso se nos intente extorsionar, por ejemplo al hacer uso de nuestras fotos privadas que fueron almacenadas y sustraídas sin nuestra autorización.

En ocasiones las personas desconocemos el nivel de seguridad o inseguridad que puede representar el que almacenemos y compartamos información desde nuestros teléfonos. Existen acciones que son sencillas de ejecutar para proteger nuestra información, y que muchos desconocemos. Precisamente la propuesta de intervención que se presenta es el resultado de la investigación que se realizó respecto al uso de perfiles en la red social conocida como Facebook para captar personas con miras a la trata. La propuesta culmina con la presentación de una infografía para que los usuarios de esta red social independientemente del país en el que se encuentren puedan conocer y prevenir la suplantación de su identidad o bien que por medio de esta actividad, algún delincuente pueda acceder a su perfil en Facebook y ocasionar que sean víctimas de la trata de personas.

No es necesario resaltar que la propuesta de intervención resulta práctica para cualquier usuario de Facebook independientemente del lugar en donde se encuentre ya que como se explica a lo largo de la investigación, no existe aún una uniformidad en torno a cómo se debería dar respuesta a la suplantación de identidad

Al no realizar las actualizaciones los usuarios pueden quedar vulnerables a malware, exploits o gusanos, todos estos programas que se esparcen para el robo de información o denegaciones de servicio principalmente.

Se sugiere consultar la página web de *internetpasoapaso.com*, de Granada en España, donde se encuentran guías y manuales gratis para aprender a usar Internet y navegar por la World Wide Web, disponible en <https://internetpasoapaso.com/que-es-una-actualizacion/>.

en medios digitales, ni tampoco existen campañas de concientización para evitar el fenómeno de la trata de personas haciendo uso de la suplantación de identidades en perfiles de Facebook.

A lo largo de la investigación se deja de manifiesto que es necesario asesorar a las personas sobre qué hacer en los casos en que sean víctimas de la suplantación de su identidad, pero principalmente es pertinente realizar acciones para concientizar a los individuos sobre la importancia de prevenirla. Por ello en la propuesta de intervención se decidió hacer una infografía que fuera fácil de exponer y a su vez fuera económica y de fácil distribución, por lo que se eligió que fuera un recurso digital lo que a su vez puede incrementar su difusión pero lo más importante de todo, que fuera útil para todos aquellos quienes tienen o piensan crear un perfil en la red social Facebook. Aunado a esto a lo largo de la investigación que se realizó para llegar a la propuesta de intervención se alerta específicamente, sobre la suplantación de identidad con fines de trata de personas, situación que se está dejando de lado pues los esfuerzos para combatir la suplantación de identidad en medios digitales se ha estado concentrando en la suplantación pero para fines de causar daños patrimoniales, lo que dificulta que existan en la actualidad datos precisos sobre la suplantación de identidad con fines de trata de personas.⁶

De esta manera haciendo uso de la investigación documental y el método inductivo-deductivo se ha logrado el objetivo de poder brindar a los lectores de esta investigación una serie de pasos a seguir para prevenir la suplantación de identidad y con ello evitar que las personas, no solo vean afectado su patrimonio, sino que

⁶ Boletín “División Científica de la Policía Federal Detecta Nuevas Amenazas Cibernéticas que Suplantán Identidades, Comisión Nacional de Seguridad”, Sala de Prensa de la Comisión Nacional de Seguridad, Secretaría de Gobernación, 8 de agosto de 2014, disponible en http://www.cns.gob.mx/portaWebApp/appmanager/porta/desk?_nfpb=true&_windowLabel=portlet_1_1&portlet_1_1_actionOverride=%2Fboletines%2FDetalleBoletin&portlet_1_1id=1348059, link consultado el 4 de mayo de 2017.

también se percaten de otros ilícitos que se derivan de la suplantación como es el caso de la trata de personas.

Con esta serie de consejos se busca brindar información útil para que la sociedad en general conozca una realidad que opera respecto a la trata de personas, y que en la actualidad las víctimas o posibles víctimas son contactadas por los delincuentes usando las redes sociales, específicamente Facebook.

Sabiendo así las limitantes de esta propuesta de intervención, se reconoce que son pocos los recursos y mucho el tiempo que se debe de invertir para lograr una sociedad consiente y preparada ante los retos que representa la suplantación de la identidad digital con fines de trata de personas. Sin embargo, esta investigación es nuestro granito de arena para intentar hacer frente al problema de la suplantación de identidad a través de perfiles de Facebook; consideramos que por medio de la información y concientización de las personas esta situación se puede prevenir por ello, en nuestra propuesta de intervención se realizó una infografía la cual se pretende mostrar los resultados de la presente investigación de manera sencilla y útil al señalar algunos consejos prácticos para los usuarios de Facebook que les ayude a conocer y prevenir la suplantación de identidad.



Capítulo 1

Aspectos generales de la suplantación de la identidad digital con fines de trata de personas



Capítulo 1: Aspectos generales de la suplantación de la identidad digital con fines de trata de personas

En el presente capítulo de esta propuesta de intervención se abordarán los conceptos base para un mejor entendimiento de la problemática de la trata de personas y de cómo la suplantación de la identidad digital, es factor clave para cometer ese ilícito.

Abordaremos conceptualmente tres aspectos fundamentales para la investigación que son: 1) el concepto propio de identidad, las distintas acepciones de identidad y la identidad como derecho humano por un lado; 2) se ahondará en el concepto de identidad digital y sobre la diferencia entre los conceptos de usurpación, suplantación y robo de identidad, a fin de establecer el concepto adecuado para esta investigación y finalmente 3) se planteará la suplantación de identidad digital en el fenómeno de la trata de personas a través de la red social Facebook que es donde se concentra la presente propuesta de intervención.

El objetivo particular de este capítulo es precisamente distinguir la suplantación de la identidad con fines de trata de personas utilizando una red social específica para así poder identificar la necesidad de incrementar la seguridad de los perfiles digitales de las personas específicamente en Facebook, señalando la necesidad de reconocer los principios básicos de la protección de datos y la privacidad de sus usuarios.

1.1 La trata de personas y del uso de medios digitales para captar a víctimas de este ilícito

La trata de personas tiene como antecedentes inmediatos la esclavitud. Uno de los primeros instrumentos a nivel internacional para hacer frente a este flagelo fue en 1921 la Convención Internacional para la Supresión de la Trata de Mujeres y Menores y desde entonces se han presentado una serie de informes,

principios, directrices, memorándums de entendimiento, protocolos y convenios para combatir este fenómeno.⁷

La trata de personas de acuerdo a la maestra Elma Trejo:

[C]onsiste en utilizar, en provecho propio y de un modo abusivo, las cualidades de una persona. Para que la explotación se haga efectiva los tratantes deben recurrir a la captación, el transporte, el traslado, la acogida o la recepción de personas. Los medios para llevar a cabo estas acciones son la amenaza o el uso de la fuerza u otras formas de coacción, el rapto, fraude, engaño, abuso de poder de una situación de vulnerabilidad. Además se considera trata de personas la concesión o recepción de pagos o beneficios para obtener el consentimiento de una persona que tenga autoridad sobre otra, con fines de explotación.⁸

⁷ Solo por mencionar algunos de estos instrumentos y documentos: Trata de Mujeres y Niñas. Informe del Secretario General, E/CN.4/2002/80 del año 2002; Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional; Convención de Palermo del año 2000; Protocolo para Prevenir, Reprimir y Sancionar la Trata de Personas, Especialmente Mujeres y Niños, que complementa la Convención de las Naciones Unidas contra la Delincuencia Organizada del año 2001; Principios y Directrices recomendados sobre los derechos humanos y la trata de personas; Informe del Alto Comisionado de las Naciones Unidas para los Derechos Humanos al Consejo Económico y Social, E/2002/68/Add.1 del año 2002.

Así como también el Acuerdo Internacional para la Supresión del Tráfico de Trata de Blancas, firmado en París el 18 de mayo de 1904, enmendado por el Protocolo firmado en Lake Success, Nueva York, el 4 de mayo de 1949, disponible en línea en <https://www.derecho.unam.mx/cultura-juridica/pdf/onu-1.pdf>, link consultado el 19 de diciembre de 2018.

⁸ Trejo García, Elma del Carmen, *et. al.*, *Compendio de Instrumentos Internacionales Relativos a la Trata de Personas*, Servicio de Investigación y Análisis, Subdirección de Política Exterior, Cámara de Diputados LXI Legislatura y Dirección General de Bibliotecas SIID, 2006, p. 1, disponible en línea en,

A lo largo del tiempo el concepto de trata de personas ha ido cambiando ya que en un principio se hacía referencia únicamente a mujeres y niños como las víctimas de este ilícito. Ejemplo de esto se observa en la Convención Internacional relativa a la Represión de la Trata de Mujeres Mayores de Edad de 1933. Esta Convención señalaba en su artículo primero que:

Deberá ser castigado quienquiera que, para satisfacer pasiones ajenas, haya conseguido, arrastrado o seducido, aun con su consentimiento, a una mujer o muchacha mayor de edad para ejercer la prostitución en otro país, aun cuando los diversos actos que sean los elementos constitutivos del delito se haya realizado en distintos países. El conato de delito, y dentro de los límites legales, los actos preparatorios, también serán punibles. Para los fines del presente artículo, el término "país" incluye a las colonias y protectorados de la alta parte contratante interesada, así como los territorios que estén bajo su soberanía y los territorios sobre el cual se haya otorgado un mandato.⁹

Hoy en día se utiliza el concepto "personas" para referirse a las víctimas de este crimen lo que indica que la trata ya no es un fenómeno que solo compete a las mujeres. Los instrumentos internacionales actuales consideran a la trata de personas que engloba tanto a hombres, como mujeres y menores de edad y lamentablemente también a infantes.¹⁰

<http://www.diputados.gob.mx/sedia/sia/spe/SPE-ISS-08-06.pdf>, link consultado el 30 de octubre de 2018.

⁹ Convención Internacional Relativa a la Represión de la Trata de Mujeres Mayores de Edad, 11 de octubre de 1933, disponible en línea en *http://www.oas.org/juridico/spanish/tratados/sp_cenve_inter_relat_repres_trat_muj_may_edad.pdf*, link consultado el 30 de octubre de 2018.

¹⁰ A pesar de que la Convención sobre los derechos del niño de 1989, que indica en su artículo 1 que se debe entender por niño "a todo ser humano menor de dieciocho años de edad, en virtud de la ley que le sea aplicable, haya alcanzado antes la mayoría de edad". Para otros fines como es el análisis psico-social y tratamiento con menores se hace diferencia entre infantes y niños, siendo en

Se ha dado una transformación en cuanto a los fines del ilícito ya que en sus inicios las mujeres eran raptadas con fines de esclavitud y también de explotación sexual como parte del botín de los conflictos bélicos. Actualmente las personas víctimas de trata son engañadas, manipuladas o amenazadas por ejemplo cuando buscan una oferta de trabajo o de estudio en un país distinto al suyo. Las personas son enroladas por medio de ofertas que a base de engaños, manipulación o amenazas logran capturar a las víctimas quienes son reclutadas con fines ya no solo de explotación sexual sino que también para la explotación laboral, para contraer matrimonio servil o relaciones filiales,¹¹ para la comisión

ocasiones los primeros aquellos en las edades de 1 a 6 años y en otras ocasiones considerados infantes a aquellos que se encuentran en las edades de 0 a 2 años.

Por ejemplo véase el sistema de indicadores sociales del Ecuador, que señala que los grupos de edad difieren según su dimensión analítica por ejemplo para casos de salud infante son considerados solo a los menores de un año. Véase como ejemplo “Conoce la realidad social y económica a través del nuevo SICES” disponible en línea en <http://www.siise.gob.ec/siiseweb/>, última fecha de consulta el 23 de diciembre de 2018.

¹¹ “Se desarrolla en la esfera doméstica y consiste en el aprovechamiento del vínculo filial para explotar a una persona. Se trata de relaciones matrimoniales de carácter servil que pueden presentar explotación sexual, reproductiva o doméstica. En ocasiones, las víctimas son captadas internacionalmente a través del Internet o de falsas agencias matrimoniales (OIM, 2007). En este caso la explotación sexual no es comercial pero la mujer se encuentra aún más esclavizada puesto que los lazos filiales generan incapacidad de salir del círculo de la violencia”.

Supliguicha, Verónica, Vásquez, Grace y Jácome, Paola, “Trata de personas: historias que invisibilizan verdades”, en Ciudad Segura, Programa Estudios de la Ciudad, FLACSO-Ecuador, núm. 36, 2009, p. 5, disponible en línea en

de ilícitos, la extracción de órganos y tejidos y para hacerlas partícipes en conflictos armados.¹²

Observemos que el concepto de trata se ha tenido que adaptar a la realidad pues los sujetos considerados víctimas se han ampliado así como las finalidades con las que se perpetra el ilícito. A esto se suma la transformación del modo comisivo del acto en sí. Nos referimos al empleo de las tecnologías para captar a las víctimas.

Existen diversos cálculos que indican que alrededor de 16,000 a 20,000 niños mexicanos y centroamericanos, han sido víctimas de la trata de personas con la finalidad de ser introducidos en los Estados Unidos de Norteamérica. Se estima que la unidad mexicana de crímenes cibernéticos desmanteló en el año 2004, doscientos sitios web dedicados a la pornografía infantil; sin embargo, las unidades ciberpoliciacas no se dan abasto [...].

En el año 2000, el Centro Nacional de Niños Desaparecidos y explotados de EUA, descubrió, a través de un estudio, que uno de cada cinco niños que usaban Internet había recibido alguna propuesta sexual a través de este medio [...]. Y es que para los acosadores sexuales, Internet representa un ambiente repleto de posibles víctimas fáciles de atacar, ya que los jóvenes no lo conciben como algo peligroso, lo que facilita que confíen totalmente, proporcionen datos personales, y digan cosas que jamás dirían a sus padres.¹³

http://www.flacso.org.ec/docs/ciudad_segura36.pdf, link consultado el 29 de octubre de 2018.

¹² Véase Alarcón García, Daniela, *Trata de personas: Uno de los delitos más lucrativos del mundo*, Monografía para optar por el título de Bachiller Académico, Gimnasio Josegina Castro de Escobar, Bogotá, D.C., 2013, pp. 22-23, disponible en <http://www.pensamientopenal.com.ar/system/files/2014/12/doctrina37867.pdf>, link consultado el 29 de octubre de 2018.

¹³ Trujano Ruiz, Patricia, Dorantes Segura, Jessica y Trovilla Quesada, Vania, "Violencia en Internet: nuevas víctimas, nuevos retos", *Liberabit*, vol. 15, núm. 1,

Es precisamente el uso de las tecnologías lo que ha facilitado el trabajo de los delincuentes ya que las personas como se mencionó en la introducción de este trabajo, muchas veces no tienen conocimiento del riesgo en el que se encuentran al navegar en Internet o tener su información personal expuesta en sus redes sociales.

A continuación nos referiremos a la importancia de la identidad de las personas. Analizaremos también el concepto de la identidad digital y la suplantación de la misma por parte de los delincuentes que utilizan esta situación para amenazar, intimidar, manipular o engañar a las víctimas para posteriormente explotarlas.

1.2 Conceptos básicos necesarios para comprender la suplantación de la identidad digital y prevenir su uso en la trata de personas

El uso de las tecnologías como el Internet arroja cada día informaciones relevantes sobre las personas, desde sus preferencias musicales, sus amigos en las redes sociales, los intereses que persiguen en sus búsquedas en Internet, hasta los últimos lugares en los que se encontraron gracias al uso de geolocalizadores. La minería de datos o *datamining* por su nombre en inglés es el conjunto de técnicas que permiten que los grandes cúmulos de datos se exploren de manera, ya sea automática o semiautomática, para detectar patrones o tendencias de comportamiento.

Este tipo de técnicas permiten utilizar los datos con fines estadísticos por ejemplo. Así al entrenar los algoritmos, los resultados que se pueden obtener son infinitos haciendo que los datos sin sentido, o en bruto, cobren relevancia. Por ello el procesamiento de datos es importante en el tema de la identidad digital pues gracias a esta minería de datos se puede permitir desarrollar estadísticas

Lima, enero-junio, 2009, disponible en línea en http://www.scielo.org.pe/scielo.php?script=sci_arttext&pid=S1729-48272009000100002, link consultado el 29 de octubre de 2018.

necesarias para ciertas investigaciones o para las empresas lo que representa una herramienta útil en beneficio del ahorro que puede causar el conocer a las personas y sus distintos hábitos de consumo y preferencias como se hacía antaño por medio de encuestas por ejemplo.

Se puede decir que esta tecnología permite acercar a las personas por medio de sus preferencias pero que también se puede influir de alguna manera en sus decisiones, es decir que puede influir en su identidad.

1.2.1 Conceptos de identidad e identidad digital

La identidad es definida en el diccionario de la Real Academia Española como “El conjunto de rasgos propios de un individuo o de una colectividad que los caracterizan frente a los demás, o la conciencia que una persona tiene de ser ella misma y distinta de los otros”.¹⁴

La identidad proviene del vocablo “latín *identitas*, que se refiere al grupo de rasgos y características que diferencia a un individuo o grupo de individuos, del resto”.¹⁵ Por medio de la identidad las personas logran distinguirse unas de otras y del resto dependiendo siempre de su propia historia y del contexto en el que se vive y se desarrolla.

La identidad depende del autoconocimiento: ¿Quiénes somos, qué somos, de dónde venimos? La identidad, con la información que proviene de la experiencia, es entonces, un proceso que dura toda la vida.

Aunque la identidad, como proceso se forma a partir del contexto o entorno desde el nacimiento, ésta evoluciona gracias a la experiencia y a los hechos que se presentan en distintos momentos de la vida. Es una constante tensión entre el entorno y el propio individuo. Puede definirse como un núcleo plástico, donde

¹⁴ Concepto de “Identidad” en el Diccionario de la Real Academia Española, en línea, disponible en <http://dle.rae.es/?id=KtmKMfe>, link consultado el 21 de enero de 2017.

¹⁵ Según el Wiktionary, proyecto de diccionario de la fundación Wikimedia, la identidad proviene del vocablo latín *identitas*, en línea disponible en <https://es.wiktionary.org/wiki/identitas> link consultado el 3 de mayo de 2017.

las características desarrolladas dependen de dicha tensión para adquirir un valor social, producto de la interacción, generando incluso la identidad de la sociedad.¹⁶

En los últimos años se ha estado estudiado el concepto de identidad encontrado algunas aportaciones como la de “Fredrik Barth considerado un pionero en la conceptualización de la identidad como manifestación relacional a partir de la interacción social”.¹⁷

Zygmunt Bauman, a partir de ciertas hipótesis básicas, edifica una rica y compleja obra intelectual llamada *Identidad*, afirmando que: “La relevancia de la identidad en el ámbito de las ciencias humanas y las disciplinas profesionales asociadas no sólo se evidencia en la irrupción de su tratamiento teórico en los últimos años, prolijo y casi inabarcable, también lo hace en la (re)ubicación alrededor de su órbita de los temas propios del análisis social, alineados ahora tras el eje de la identidad”.¹⁸

¹⁶ Fundación Telefónica, *Identidad digital: El nuevo usuario en el mundo digital en línea*, Madrid, Ariel-Fundación telefónica y Editorial Planeta, 2013, p. 11, disponible en http://www.educando.edu.do/files/9513/9281/6433/identidad_digital.pdf, link consultado el 3 de mayo de 2017.

¹⁷ Véase Marcús, Juliana, “Apuntes sobre el concepto de identidad”, *Revista sociológica de Pensamiento crítico*, vol. 5, núm. 1, 2011, p. 107, disponible en <http://intersticios.es>, link consultado el 4 de octubre de 2018.

Véase también Barth, Fredrik, *Los grupos étnicos y sus fronteras. La organización social de las diferencias culturales*, 1a. ed., en español, México, Fondo de Cultura Económica, 1976, disponible en línea en http://www.cedet.edu.ar/archivos/Bibliotecas_Archivos/id40/Barth-Los-grupos-etnicos-y-sus-fronteras.pdf, link consultado el 22 de octubre de 2018.

¹⁸ González, Noé, “Bauman, identidad y comunidad”, *Espiral*, vol. 14, núm. 40, Guadalajara, septiembre-diciembre 2007, disponible en

Bauman en su libro *Identidad* nos da las bases para poder ver el proceso relacional de la identidad cuando nos menciona que: “Los individuos desincrustados de sus estamentos premodernos estaban obligados a hacer uso de su nuevo estadio personal de autodeterminación alcanzado para formarse en el aprendizaje de los hábitos, actitudes y conductas que les permitieran incrustarse en la clase social de la sociedad industrial emergente”.¹⁹

En el ámbito de la filosofía, Darío Sztajnszrajber, en la conferencia dada en el Ministerio de Ciencia, Tecnología e Innovación Productiva en Argentina, sobre el tema de la identidad, sostiene que la identidad viene de la palabra *Ídem* que quiere decir idéntico. Sin embargo, afirma que nunca somos idénticos, siempre estamos cambiando, tanto que están muriendo 1,200,000 células por día, entonces no somos el mismo de ayer que hoy, no somos idénticos y al buscar quiénes somos, no debemos buscar desde la ciencia o metafísica, donde la identidad no existe o es un mito, la identidad se encontraría solamente desde el punto de vista del arte.²⁰

El historiador Ezequiel Adamovsky, por su parte menciona que la identidad es una imagen, cuando alguien nace no tiene consciencia de un yo, un bebé no sabe que la mano que ve es parte de él. No es sino hasta que reconoce cada parte de su cuerpo, que comienza a identificar que es un yo. La identidad es una narración de la continuidad o secuencia de lo mismo, en este caso del yo.

http://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S1665-05652007000100007, link consultado el 22 de octubre de 2018.

¹⁹ *Ídem*.

²⁰ Conferencia de identidad, ponentes el filósofo Darío Sztajnszrajber y el historiador Ezequiel Adamovsk, Ministerio de Ciencia Tecnología e Innovación Productiva en Argentina, disponible en <https://www.youtube.com/watch?v=ZP45ANGVST4>, link visitado el 22 de octubre de 2018.

También tenemos una identidad personal como colectiva porque somos parte de la historia de alguien más.²¹

Según Charles Taylor en su libro *Fuentes del yo*, la comprensión de la vida de las personas en las sociedades contemporáneas y a partir de la definición de la identidad como una forma de narración social, con base en el lenguaje, esta se fundamenta en dos aspectos: 1) en la tesis de que el sujeto no decide o no elige las fuentes de su identidad, sino que la construye a partir de la relación social en el marco de la comunidad con los otros significantes, y 2) que la identidad, a partir de la comunidad definidora asumida como una comunidad lingüística, se vuelve una narración de lo que somos y de quiénes somos.²²

Después de todas las aproximaciones arriba señaladas, es necesario identificar aquellos elementos que permiten entender el concepto de la identidad en diferentes áreas de estudio, específicamente nos interesa saber cuándo el concepto de identidad comienza a tener mayor influencia en la sociedad de la información, es decir el concepto identidad aplicado al contexto digital, o de las tecnologías de la información, que nos permita establecer un puente entre la definición de identidad según la psicología, según el derecho y según las tecnologías de la información.

Desde la perspectiva del derecho, la identidad es uno de los derechos fundamentales de todo ser humano que es necesaria para poder beneficiarse de los otros derechos fundamentales. La Declaración Universal de los Derechos Humanos señala específicamente que:

²¹ *Ídem.*

²² Taylor, Charles, *Fuentes del yo: La construcción de la identidad moderna*, Paidós Ibérica, Título original: *Sources of self, the making of the modern identity*. en Zárate Ortiz, José Francisco, “La identidad como construcción social desde la propuesta e Charles Taylor” en *Eidos*, núm. 23, Barranquilla, julio-diciembre de 2015, disponible en línea en http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S1692-88572015000200007, link consultado el 29 de octubre de 2018.

El derecho del niño a la **identidad**, desde el momento de su nacimiento, toda persona tiene derecho a obtener una **identidad**. La **identidad** incluye el nombre, el apellido, la fecha de nacimiento, el sexo y la nacionalidad. Es la prueba de la existencia de una persona como parte de una sociedad, como individuo que forma parte de un todo; es lo que la caracteriza y la diferencia de las demás. Todos los niños tienen derecho a poseer una identidad oficial, es decir, a tener un nombre, un apellido, una nacionalidad y a conocer la identidad de sus progenitores.²³ (Énfasis añadido).

Para el senador Benjamín Robles Montoya, la identidad:

[N]o es sólo uno más de los elementos que conforman la esencia del ser humano como tal, sino aquel que **representa la individualidad de cada uno y la potencialidad de desarrollarnos como personas y como parte de un grupo social, de aprovechar todas las capacidades y aptitudes naturales y adquiridas**, así como gozar y ejercer las libertades y los derechos que el orden jurídico nos reconoce u otorga. (Énfasis de la cita original).

El Estado, como organización política y jurídica de una sociedad, tiene como fines supremos realizar el bien común, y para ello, debe asegurar a su componente humano los medios necesarios para contar con una identidad particular y su constatación con carácter oficial, así como proveer los mecanismos institucionales y normativos que operen el servicio público de registro y certificación de la existencia de una persona, y las variaciones a su estado civil.²⁴

De conformidad con los criterios de la primera sala de la Suprema Corte de Justicia de la Nación:

²³ La Declaración Universal de Derechos Humanos, disponible en línea en <http://www.un.org/es/universal-declaration-human-rights/>, link consultado el 22 de octubre de 2018.

²⁴ Citando la obra *El derecho a la identidad como derecho humano*, enero de 2011, versión electrónica: disponible en línea en http://www.senado.gob.mx/64/gaceta_del_senado/documento/73846, link visitado el 22 de octubre de 2018.

Para el Derecho mexicano, la identidad “persigue proteger la conformación de la auto-percepción -como faceta identitaria” (Tesis: 1ª. XCVI/2018 (10ª). En esta tesitura, ha referido que “la identidad no se agota en lo biológico”, sino que “la construcción de la identidad se construye a través de múltiples factores psicológicos y sociales de la manera en la que el individuo se concibe y los rasgos definitorios de su personalidad se nutren sensiblemente de valores y principios que le transmiten las personas significativas para él en sus primeros años de vida” (Tesis 1º. LXXIII/2017 (10ª). En este sentido, el derecho a la identidad se construye no sólo a través del vínculo biológico, sino también del conocimiento de la realidad social del individuo.

Además de los factores biológicos y sociales, en términos de derechos, la imagen propia de la persona se encuentra determinada, en gran medida, “por el conocimiento de sus orígenes y su filiación, así como por la identificación que tiene en la sociedad a través de un nombre y una nacionalidad”. (Tesis 1º. CXVI/2011, Primera Sala).

De lo anterior se desprende que: la identidad se compone de varios factores: biológico, social, psicológico, así como por la “identificación que tienen en la sociedad a través de un nombre”, este último se traslada al plano digital. Recordando que los DDHH se encuentran reconocidos tanto en el mundo online como en el offline podemos considerar que, la identificación que una persona tenga dentro una red social (la cual constituye una sociedad virtual), es parte de su derecho a la identidad.

En el mundo físico, la identidad de una persona es el conjunto de rasgos que lo diferencia de los demás en sus distintas concepciones como ser humano: en el cuerpo, alma y espíritu. Por otro lado, en el mundo virtual la identidad digital es una extensión más de nuestra identidad real como se explica a continuación.

El término “identidad digital” surge en la década de 1990 con la introducción de las computadoras personales y el auge de Internet, así como el surgimiento de las redes sociales. Recordemos fechas relevantes y sus aportaciones:

1994: Se funda **GeoCities**, una de las primeras redes sociales de [I]nternet tal y como hoy las conocemos. La idea era que los usuarios crearan sus propias páginas web y que las alojaran en determinados barrios según su contenido (Hollywood, Wallstreet, etc[étera]).

1995: [Se crea] **TheGlobe.com** [... con la finalidad de que] sus usuarios [tuvieran] la posibilidad de personalizar sus propias experiencias online publicando su propio contenido e interactuando con otras personas con intereses similares.²⁵

1997: Se lanza **AOL Instant Messenger**.²⁶

1997: Se inaugura la web **Sixdegrees.com**, que permite la creación de perfiles personales y el listado de amigos.²⁷

2000: [El Internet es adoptado por la gran mayoría de los usuarios de computadoras].²⁸

2002: Se lanza el portal **Friendster**, pionero en la conexión online de “amigos reales”. Alcanza los 3 millones de usuarios en sólo tres meses.²⁹

²⁵ Véase la historia de theglobe.com puede ser consultada en su página oficial: theglobe.com, disponible en línea <http://www.theglobe.com/>, link consultado el 2 de mayo de 2017. Texto en idioma inglés.

²⁶ Véase la historia de AOL Instant Messenger, se encuentra disponible en Wikipedia, disponible en línea en https://es.wikipedia.org/wiki/AOL_Instant_Messenger, link consultado el 2 de mayo de 2017.

²⁷ Véase la historia de Sixdegrees.com, puede consultarse en su página oficial en Sixdegrees.com, disponible en línea en <http://sixdegrees.com/>, link consultado el 2 de mayo de 2017.

²⁸ Véase Castells, Manuel, *La galaxia Internet: Reflexiones sobre Internet, empresa y sociedad*, Barcelona, Plaza & Janés, 2001.

²⁹ Véase la historia del portal Friendster, disponible en línea en <http://timerime.com/es/evento/2530833/Se+lanza+el+portal+Friendster/>, link consultado el 2 de mayo de 2017.

2003: Se inaugura la web **MySpace**, concebida en un principio como un “clon” de Friendster. Creada por una empresa de marketing online, su primera versión fue codificada en apenas 10 días.³⁰

2004: Se lanza **Facebook**, concebida originalmente como una plataforma para conectar a estudiantes universitarios. Su [lanzamiento] tuvo lugar en la Universidad de Harvard y más de la mitad de sus 19.500 estudiantes se suscribieron a ella durante su primer mes de funcionamiento.³¹

2006: Se inaugura la red de microblogging **Twitter**.³²

2008: Facebook adelanta a MySpace como **red social líder**,³³ respecto a visitantes únicos mensuales.³⁴ (Énfasis de la cita original)

Si bien, con el paso del tiempo, las redes sociales han traído el tema de la identidad digital aún no se ha encontrado una definición acabada de este concepto. Por ello plasmaremos algunas definiciones de la identidad digital en diferentes áreas de estudio como es el derecho y las tecnologías de la información, a fin de entender este concepto en relación con estas áreas de estudio.

³⁰ Véase la historia de MySpace, disponible en línea en http://www.laccei.org/LACCEI2010-Peru/published/TTL146_SanMartin.pdf, link consultado el 2 de mayo de 2017.

³¹ Véase la historia de Facebook, disponible en línea en la página oficial de Facebook en <https://newsroom.fb.com/company-info/>, link consultado el 2 de mayo de 2017.

³² Véase la historia de Twitter, disponible en línea en http://www.cad.com.mx/historia_de_twitter.htm, link consultado el 2 de mayo de 2017.

³³ Véase la historia de Facebook adelanta a MySpace como red social líder, disponible en línea en <https://www.ecured.cu/Myspace>, link consultado el 2 de mayo de 2017.

³⁴ Blog normol, Redes sociales, “Historia de las redes sociales”, disponible en línea en <http://histinf.blogs.upv.es/2011/12/20/redes-sociales/>, link visitado el 22 de octubre de 2018.

Por su parte y solo por mencionar el tema, y sin que se aborde a cabalidad en este trabajo, debe entenderse que en el contexto de las redes sociales es importante no confundir entre identidad y reputación. Julio Alonso explica que:

La identidad es lo que permite distinguir entre miembros de una misma especie. Es un concepto relativo al individuo, pero a su vez sólo tiene sentido en cuanto esté forma parte de un grupo social. En cierta medida la identidad es lo que yo soy, o pretendo ser, o creo que soy. La reputación, mientras, es la opinión que otros tienen de mí. Se forma en base a lo que yo hago y lo que yo digo, pero también a lo que otros perciben de mis actos o palabras, a cómo lo interpretan y a cómo lo transmiten a terceros.³⁵

Es innegable que hoy por hoy, mucho de lo que es la identidad de las personas en los medios digitales y fuera de ellos también tiene que ver con la reputación que se crea alrededor de uno mismo,

en un pequeño pueblo, por ejemplo, todos se conocen; saben cómo se llama cada uno de ellos, quiénes son sus padres, dónde viven, a qué se dedican, incluso que han hecho durante el fin de semana. La información circula de forma muy rápida y eficaz, lo que haces o dice[s] se sabe y permite construir tu identidad. A ello contribuyes tu con tus actos, pero también lo [... que dicen tus vecinos y las personas que te conocen]. En ese contexto, la construcción de la identidad personal y de la reputación es fácil y casi inconsciente.³⁶

³⁵ Alonso, Julio, *Identidad digital y reputación on line*, Madrid, Evoca Comunicación e imagen, 2011, p. 6, disponible en línea en <http://www.evocaimagen.com/cuadernos/cuadernos5.pdf>, link consultado el 22 de octubre de 2018.

“Julio Alonso es fundador y Director General de Weblogs SL, la principal empresa española de contenidos especializados en Internet. Fundada en 2005, Weblogs SL ofrece más de 40 publicaciones online sobre temáticas que van de la tecnología a la moda, pasando por el motor o la economía. También asesora a grandes empresas sobre sus estrategias en medios sociales”, p. 5.

³⁶ *Ídem*.

Según F. Georges, “la **identidad digital** está constituida por diferentes tipos de datos según el usuario tenga o no la intención de revelarlos, lo que da lugar a una identidad declarada, compuesta por aquella información que revela expresamente la persona, otra identidad actuante, según las acciones que esta lleva a cabo, y otra calculada o inferida, según el análisis de las acciones que realiza la persona”.³⁷ (Énfasis añadido).

Toda esta información puede ser utilizada para configurar una idea de quién es y qué le gusta a una persona determinada. En concreto, el tipo de datos que ayudan a configurar esta identidad pueden catalogarse como:

- Datos de identidad individual: se trata de identificadores como el nombre, el número de la Seguridad Social o el DNI, el número del permiso de conducción, el número de la tarjeta de crédito, la fecha de nacimiento, los identificadores sociales de los sitios web a los que accede, etc[étera].
- Datos de comportamiento: sobre transacciones, historial de navegación, datos de localización, transcripciones del call-center, historial de compra, accesos, etc[étera].
- Datos derivados o calculados: son atributos modelados de manera analítica que sirven para hacer un perfilado de las personas, por ejemplo, para valorar el riesgo de un cliente a la hora de darle un crédito, entender la propensión a hacer algo, valorar su influencia en un ámbito determinado, etc[étera].
- Datos que va creando el propio usuario para identificarse: como opiniones sobre productos, redes profesionales a las que pertenece, ‘me gusta’ en redes sociales, intenciones de compra, valoraciones y revisiones de productos, respuestas en foros, etc[étera].

El concepto de identidad digital tiene, además, diferentes representaciones de acuerdo al entorno, es decir, las personas cuentan con varios perfiles según el contexto en el que se desenvuelven, creando perfiles que incluyen distinta información.³⁸

³⁷ Fundación Telefónica, “Identidad digital: el nuevo usuario en el mundo digital en línea”, *op. cit.*, nota 16, p. 11.

³⁸ *Ídem.*

Así, es posible que en el mundo digital, inclusive la gente que no conocemos, tenga acceso a diferentes tipos de nuestros datos. En ocasiones los empleadores buscan perfiles de los candidatos a los puestos ofertados en redes sociales, esto es lo primero que se muestra de uno o es lo primero que se conocerá de nosotros. La construcción de la identidad y la reputación se forman a partir de una imagen.

El propósito principal de la identidad digital o la llamada identidad 2.0 fue para la identificación de una persona que se accionaba conectada en línea para distintos fines. Por ejemplo, había sistemas informáticos con los que se necesitaba relacionar a una persona física determinada de acuerdo con su identidad digital para reconocer que la persona en el mundo físico era la misma persona en el mundo virtual. Según Roberto Aparici y Sara Osuna en su artículo “La cultura de la participación” la, “**Identidad 2.0 o identidad digital** es todo lo que manifestamos en el ciberespacio e incluye tanto nuestras actuaciones como la forma en la que nos perciben los demás en la red”.³⁹

Después con el surgimiento de los dispositivos móviles se han generado más interconexiones sociales. A su vez, la digitalización de la información está haciendo que el desarrollo de aplicaciones se base en crear perfiles de consumo, haciendo atractivo para las empresas el seguir contribuyendo en la evolución de la identidad digital de las personas, con el fin de poder visualizar su reputación y privacidad en redes sociales y en aplicaciones de Internet. Convirtiéndose esto en elementos que debemos saber para llegar a entender y a gestionar nuestra identidad digital.

Algunas organizaciones como la Organización Internacional de Telecomunicaciones el Banco Mundial o el Foro Económico Mundial han

³⁹ Aparici, Roberto y Osuna Acedo, Sara, “La cultura de la participación”. *Revista Mediterránea de Comunicación*, vol. 2, no. 2, 2013, p. 144. Texto disponible en línea en https://rua.ua.es/dspace/bitstream/10045/34243/5/ReMedCom_04_02_07.pdf, link consultado el 19 de diciembre de 2018.

aportado sus propias definiciones de identidad digital como aquellos atributos de la identidad que son capturados y almacenados de manera electrónica para ser utilizados en transacciones electrónicas con el propósito de mejorar la funcionalidad de los usuarios en un mundo digital.⁴⁰

En resumen se puede asegurar que la identidad digital,

Es el rastro que cada usuario de Internet deja en la red como resultado de su interrelación con otros usuarios o con la generación de contenidos. Es decir la identidad digital es consecuencia de la comunicación 2.0 [y su relación con otros usuarios].

Todos, alguna vez hemos buscado nuestro nombre en Google o en otros buscadores [... y c]omo resultado hemos obtenido información sobre nosotros que en algún momento hemos publicado, [o que otros han subido]. Comentarios en un blog, imágenes, videos, menciones en una noticia, la publicación de una sanción [...], los resultados de una [demanda], un trabajo [realizado o demás, es el tipo de información que se encuentra en internet y que quizá prefiriésemos] no estuviera para evitar una situación [incómoda o perjudicial].⁴¹

Con el desarrollo de las tecnologías se ha modificado radicalmente el concepto de identidad ya que actualmente contempla diferentes planos sociales del individuo como son: la familia, el trabajo y los amigos. La identidad digital se

⁴⁰ Véase el White Paper, del World Economic Forum “Digital Identity on the Threshold of a Digital Identity Revolution”, Davos-Klosters, Suiza, 23-26 de enero de 2018, pp. 6 y 7 disponible en línea en http://www3.weforum.org/docs/White_Paper_Digital_Identity_Threshold_Digital_Identity_Revolution_report_2018.pdf, link consultado el 19 de diciembre de 2018.

⁴¹ Carbellido Monzó, Carlos, “Identidad digital, reputación on line, el derecho al olvido y cómo borrar contenido de Internet”, en *community manager*, consutor de marketing digital, 23 de enero de 2018, disponible en línea en <https://www.uncommunitymanager.es/identidad-digital/>, link consultado el 22 de octubre de 2018.

construye ya no sólo a partir de lo que somos, sino también de lo qué hacemos y de cómo nos relacionamos con otros.

1.2.2 Identidad digital como un derecho humano

Si bien los antecedentes de los derechos humanos se dan desde los movimientos sociales de la Revolución Francesa y la Independencia de las trece colonias de Inglaterra, pasando posteriormente en 1945 con el fin de la Segunda Guerra Mundial y los juicios de Núremberg, la realidad demuestra que el tema tecnológico se comenzó a introducir en los tratados en materia de Derechos Humanos hasta que las tecnologías se encontraron disponibles para un mayor número de personas.

Únicamente la Convención sobre los derechos de las personas con discapacidad, celebrada en 2006 y con inicio de vigencia hasta 2008, hace mención a las tecnologías en 17 ocasiones por ejemplo en su artículo 4 señala como obligación de los Estados parte de este instrumento vinculante:

g) Empezar o promover la investigación y el desarrollo, y promover la disponibilidad y el **uso de nuevas tecnologías, incluidas las tecnologías de la información y las comunicaciones, ayudas para la movilidad, dispositivos técnicos y tecnologías de apoyo adecuadas para las personas con discapacidad, dando prioridad a las de precio asequible;**

h) Proporcionar información que sea accesible para las personas con discapacidad sobre ayudas a la movilidad, **dispositivos técnicos y tecnologías de apoyo, incluidas nuevas tecnologías**, así como otras formas de asistencia y servicios e instalaciones de apoyo;⁴² (énfasis añadido).

⁴² El texto completo de la Convención está disponible en el siguiente link <https://www.un.org/esa/socdev/enable/documents/tccconvs.pdf>, consultado por última ocasión el 18 de noviembre de 2018.

No obviamos mencionar que existen otros documentos internacionales sobre el tema pero que no son vinculantes como puede ser la “Proclamación de Teherán” de 1968, adoptada en la Conferencia Internacional de Derechos Humanos, en

El artículo 9 de la misma Convención también establece sobre la accesibilidad que:

A fin de que las personas con discapacidad puedan vivir en forma independiente y participar plenamente en todos los aspectos de la vida, los Estados Partes adoptarán medidas pertinentes para asegurar el acceso de las personas con discapacidad, en igualdad de condiciones con las demás, al entorno físico, el transporte, **la información y las comunicaciones**, incluidos los sistemas y las **tecnologías de la información y las comunicaciones**, y a otros servicios e instalaciones abiertos al público o de uso público, tanto en zonas urbanas como rurales. Estas medidas, que incluirán la identificación y eliminación de obstáculos y barreras de acceso, se aplicarán, entre otras cosas, a:

b) Los servicios de información, comunicaciones y de otro tipo, incluidos los servicios electrónicos y de emergencia.

su punto 18, que hace referencia a los riesgos en torno a los derechos y las libertades de los individuos que traen consigo los descubrimientos científicos y adelantos tecnológicos. Disponible en línea en <http://www.ordenjuridico.gob.mx/TratInt/Derechos%20Humanos/OTROS%2016.pdf>, link consultado el 19 de diciembre de 2018, y también la Resolución 3384 de 10 de noviembre de 1975, “Declaración sobre la Utilización del Progreso Científico y Tecnológico en Interés de la Paz y en Beneficio de la Humanidad”, adoptada por la Asamblea General de la ONU, disponible en línea en: <http://www.ordenjuridico.gob.mx/TratInt/Derechos%20Humanos/INST%2024.pdf>, link consultado el 19 de diciembre de 2018.

Así como las resoluciones 55/63 y 56/121 de la Asamblea General de las Naciones Unidas sobre la lucha contra la utilización de la tecnología de la información con fines delictivos, la resolución 57/239 relativa a la creación de una cultura mundial de seguridad cibernética y la resolución 58/199 sobre creación de una cultura mundial de seguridad cibernética y protección de las infraestructuras de información esenciales.

g) Promover el acceso de las personas con discapacidad a los nuevos **sistemas y tecnologías de la información y las comunicaciones, incluida Internet;**

h) Promover el diseño, el desarrollo, la producción y la distribución de sistemas y **tecnologías de la información y las comunicaciones accesibles en una etapa temprana, a fin de que estos sistemas y tecnologías sean accesibles al menor costo.**⁴³

Solo hasta hace diez años se incluyó el tema de las tecnologías en las convenciones de derechos humanos y en lo que respecta a la identidad digital como un derecho humano es hasta el marco de la Segunda Cumbre Anual de ID2020 de 2017 con sede en la Organización de las Naciones Unidas (en adelante ONU) que se presentaron diversos esfuerzos para lograr el reconocimiento de la identidad digital como derecho humano.⁴⁴

ID2020, es una asociación promotora de la Agenda 2030 de la ONU para el Desarrollo Sostenible, que presentó un prototipo para proporcionar la identidad digital para todos en el mundo conforme lo indica el objetivo 16.9 de los Objetivos para el Desarrollo Sostenible.⁴⁵

Haciendo referencia a lo mencionado por Rosana Mazza, socia de PwC Argentina, en dicha cumbre, la ausencia de una identidad es equivalente a ser invisible o carecer de un derecho básico. Según Mazza, tanto las empresas como los gobiernos necesitan conocer las identidades de la población real para evitar inconvenientes financieros o legales.⁴⁶

Durante la mencionada Segunda Cumbre ID2020 se presentó un Manifiesto en el que se mencionan algunos principios sobre identidad digital en donde en

⁴³ *Idem.*

⁴⁴ Blog de Estrada Villegas, Carina, "ONU: Identidad digital como derecho humano básico", 7 de agosto de 2017, disponible en línea en <https://carinaestradasite.wordpress.com/2017/08/07/onu-identidad-digital-como-derecho-humano-basico/>, link consultado el 22 de octubre de 2017.

⁴⁵ *Ídem.*

⁴⁶ *Ídem.*

su primer y segundo principios se establece que poder comprobar la identidad de alguien es tanto un derecho fundamental como un derecho humano y que esta comprobación debe ser verificable y comprobable tanto en el mundo físico como en el digital.⁴⁷

Maja Vujinovic, directora general de información de General Electric Digital, presentó su proyecto para crear un identificador digital de todas las personas del mundo en colaboración con el sector privado como Microsoft y Accenture, así como el sector público con el Programa Mundial de Alimentos y la Agencia para Refugiados de la ONU.⁴⁸

Vujinovic mencionó que el objetivo es integrar toda la información de la identidad digital básica del mundo como puede ser huellas, fecha de nacimiento, registros médicos, educación, viajes y cuentas de banco.⁴⁹

Finalmente en este evento y en el Manifiesto no se deja de lado que la identidad digital también conlleva riesgos que no deben desestimarse principalmente cuando existe una base de datos centralizados.⁵⁰

⁴⁷ En el manifiesto se lee: “1. The ability to prove one’s identity is a fundamental and universal human right

2. We live in a digital era. Individuals need a trusted, verifiable way to prove who they are, both in the phisycal world and online”.

El Manifiesto completo se puede leer directamente del link <https://id2020.org/manifesto/>, consultado por última vez el 19 de noviembre de 2018.

⁴⁸ Blog de Estrada Villegas, Carina, “ONU: *op. cit.*, nota 43.

⁴⁹ *Ídem.*

⁵⁰ En el principio 6 se puede leer “Digital identity carries significant risk if not thoughtfully designed and carefully implemented. We do not underestimate the risks of data misuse and abuse, particularly when digital identity systems are designed as large, centralized databases”. Manifiesto *op. cit.* nota 46.

1.2.3 Usurpación, suplantación y robo de identidad

La usurpación, suplantación y robo de identidad son conceptos que al momento de referirnos a la identidad digital suelen usarse de manera indistinta.

La usurpación se puede definir de la forma siguiente: “Del latín *usurpatio-ōnis*, 1. Acción y efecto de usurpar; 2. Cosa usurpada, especialmente el terreno usurpado; 3. Delito que se comete apoderándose con violencia o intimidación de inmueble o derecho real ajeno”.⁵¹ Sin embargo como un concepto en materia de derecho civil, encontramos otra concepción de usurpación, entendida como el “Delito que comete quien utiliza de forma estable el estado civil, nombre y apellidos de otra persona, suplantando su personalidad”.⁵² No olvidemos la definición del latín sobre la acción de usurpar o *Usurpāre* se define como: “1. Apoderarse de una propiedad o de un derecho que legítimamente pertenece a otro, por lo general con violencia; 2. Arrogarse la dignidad, empleo u oficio de otro, y usarlos como si fueran propios”.⁵³

Por otro lado como concepto la suplantación de la identidad es entendida en general: “... como la actividad maliciosa en la que un atacante se hace pasar por otra persona por motivos como: cometer fraudes, ciberacosar, sextorsión, etcétera. Un caso típico de suplantación de identidad es, en las redes sociales,

⁵¹ Definición de usurpación disponible en el diccionario de la Real Academia Española del vocablo latín *identitas*, disponible en línea <http://dle.rae.es/srv/fetch/fetch?id=bC17km6>, link consultado el 3 de mayo de 2017.

⁵² *Ídem*.

⁵³ Definición de usurpar disponible en el diccionario de la Real Academia Española del vocablo latín *identitas*, disponible en línea en <http://dle.rae.es/srv/search?m=30&w=usurpar>, disponible en línea link consultado el 3 de mayo de 2017.

crear un perfil de otra persona e interactuar con otros usuarios haciéndose pasar por ella”.⁵⁴

La suplantación de identidad se asocia al uso público de un nombre y apellidos de un tercero ficticio, que puede existir o ser imaginario. Por ejemplo: aquella persona que abre una cuenta en una red social creando un perfil falso con la finalidad de enmascarar su identidad y con la intención de hacerse pasar por otro. Este tipo de actos de acuerdo a la jurisprudencia penal española considera que **“no comete delito el que se limita a una ficción esporádica**, ni quién se hace pasar por otro en un momento determinado y para un acto concreto con **la finalidad de disfrazar su propia identidad**. (Énfasis de la cita original).⁵⁵

Otro concepto que también suele utilizarse para referirse a la apropiación de la identidad de otra persona para aparentar ser ella y asumir su identidad frente a terceros con fines de obtener ganancias económicas o cualquier otro tipo de beneficio es denominado como robo de identidad. El robo de identidad es definido como “la apropiación de la identidad de una persona para hacerse

⁵⁴ Definición de suplantación de identidad, Oficina de Seguridad del Internauta, Blog, “Cómo puedo denunciar una suplantación de identidad en Internet”, publicado el 14 de mayo de 2014, disponible en línea en <https://www.osi.es/es/actualidad/blog/2014/05/14/como-denunciar-una-suplantacion-de-identidad-en-internet>, link consultado el 3 de mayo de 2017.

⁵⁵ De Roselló Moreno, Rocio, “Usurpación vs suplantación de la identidad”, *Info Security News*, año 12, núm. 10, octubre 2016, disponible en línea en http://www.infosecurityvip.com/newsletter/leyes_oct16.html, link visitado el 22 de octubre de 2018.

Por doctrina jurisprudencial se refiere a la jurisprudencia 23.654 Usurpación del estado civil del 23 de mayo de 1986. Disponible en Ruiz Gutierrez, Urbano, *Diccionario de Jurisprudencia penal 1983-1988*, Ministerio de Justicia, Tomo VII, Secretaría General Técnica. Centro de Publicaciones, Madrid, 1991, p. 1247.

pasar por ella, asumir su identidad frente a terceros públicos o privados a fin de obtener ciertos recursos o beneficios a su nombre”.⁵⁶

La CONDUSEF señala que el robo de identidad surge “Cuando una persona obtiene, transfiere, posee o utiliza de manera no autorizada datos personales de alguien más, con la intención de asumir de manera apócrifa su identidad y realizar compras, obtener créditos, documentos o cualquier otro beneficio financiero en detrimento de sus finanzas”.⁵⁷

Por lo anterior expuesto es que se observa que es común que los conceptos de robo, usurpación y suplantación de identidad se utilicen como sinónimos generalmente en los medios de comunicación.

Debido a que no es el tema de esta investigación ni de la propuesta de intervención dar una respuesta sobre cuál de los conceptos es el correcto o ahondar en las diferencias o semejanzas entre ellos simplemente sirva hasta lo aquí expuesto para que el lector comprenda que en la literatura se encuentran el uso de esos conceptos de manera indistinta. Y que para efectos legales es necesario conocer el marco jurídico de cada país ya que las normas jurídicas se establecen de conformidad a cada sistema al cual pertenecen por lo que el concepto utilizado puede variar.

En nuestra propuesta seguiremos utilizando el concepto de suplantación que es el que nos parece el adecuado para los efectos de nuestra propuesta de intervención, sin embargo, cuando hagamos referencia a los textos e ideas de

⁵⁶ Robo de identidad de acuerdo a la Guía para prevenir el robo de identidad del INAI, S/a, *Guía para prevenir el robo de identidad*, México, INAI, p. 5, disponible en http://inicio.ifai.org.mx/DocumentosdeInteres/Gu%C3%ADa_Prevenir_RI.pdf, link visitado el 9 de septiembre de 2017.

⁵⁷ CONDUSEF, “Robo de identidad”, disponible en <https://www.condusef.gob.mx/Revista/index.php/usuario-inteligente/consejos-de-seguridad/563-robo-de-identidad>, consultado el 4 de noviembre de 2018.

otras personas respetaremos el concepto que se utiliza en las fuentes y por los autores de las mismas.

1.3 Suplantación de identidad con fines de trata de personas en Facebook

La trata de personas es un fenómeno que se va propagando y actualizando también con la evolución de la tecnología siendo cada vez más complejo. Es con el uso de las tecnologías y las identidades digitales que quedan expuestas en sitios como las redes sociales, que la suplantación es un ilícito que ha proliferado, en particular el uso de los perfiles de Facebook que facilita la captura de víctimas con fines de trata.

A continuación se ahondará en la problemática específica del uso de perfiles en Facebook con la finalidad de captar personas y someterlas a la trata en nuestro país.

1.3.1 La trata de personas en México

Según la Ley para Prevenir y Sancionar la Trata de Personas en su artículo 5, la trata de personas es considerada un delito y define quién es la persona que lo realiza:

Comete el delito de trata de personas quien promueva, solicite, ofrezca, facilite, consiga, traslade, entregue o reciba, para sí o para un tercero, a una persona, por medio de la violencia física o moral, engaño o el abuso de poder para someterla a explotación sexual, trabajos o servicios forzados, esclavitud o prácticas análogas a la esclavitud, servidumbre, o a la extirpación de un órgano, tejido o sus componentes.⁵⁸

Sin embargo, la información que se puede obtener sobre el número de personas víctimas de la trata de personas, los medios que se utilizan para

⁵⁸ Ley para Prevenir y Sancionar la Trata de Personas en su Artículo 5, disponible en https://docs.mexico.justia.com/federales/ley_para_prevenir_y_sancionar_la_trata_de_personas.pdf, link consultado el 22 de octubre de 2018.

contactarlas, y las medidas que se realizan para enfrentar el ilícito no es tan detallada, pues faltan estadísticas y datos que expliquen este fenómeno. Aunado a esto la corrupción y los enormes montos que recauda la explotación de las personas, hace que este ilícito sea atractivo para muchos mercados y, en lo social a causa de la ignorancia, apatía y menosprecio, al abordar el tema hace el caldo de cultivo perfecto para que las personas sean presas fáciles de la trata, y sobre todo cuando en la sociedad en general nos damos cuenta de que algo anda mal y preferimos ignorar el problema.

La Organización de las Naciones Unidas, específicamente el Comité de Derechos para los Trabajadores Migrantes y sus Familias, ha identificado la incapacidad de México respecto al tema de trata y tráfico de personas para perseguir y procesar a los responsables sin que se avance en el combate de este delito.⁵⁹

Las víctimas de trata son explotadas incluso en lugares abiertos principalmente y tienen contacto con la sociedad, pero tienen sus respectivos motivos por el cual no escapan, ya que son sometidas a constantes amenazas, estas podrían ser las más comunes según el escrito *Trata de Personas. Aspectos Básicos*:

Uso de la violencia o amenaza de violencia física, psicológica y/o sexual.

Muchas veces, niños, niñas y mujeres jóvenes son golpeadas o violadas por sus explotadores como forma de mantenerlas sometidas [...].

Amenaza de ser enviadas a prisión o ser deportadas cuando son extranjeras en situación irregular, [...].

Muchas veces los tratantes investigan mínimos detalles de la vida familiar de la víctima, por lo que amenazan con lastimar a sus familiares en sus comunidades de origen.

Se utiliza presión o chantaje por deudas o supuestas deudas contraídas como otro de los factores importantes para crear miedo, dependencia y vencer barreras psicológicas.

⁵⁹ Véase la obra de Orozco, Rosi, *Trata de personas*, México, Instituto Nacional de Ciencias Penales, 2011.

Aislamiento social y lingüístico cuando se trata de extranjeras que no conocen el país o la localidad donde se encuentran [...].

Exposición y estigmatización. [...] infringida por el entorno social, al dificultar la reintegración, a menudo se considera la principal causa de la reincidencia entre las víctimas de la trata. [...].⁶⁰

El problema de la trata de personas está presente en la mayoría de los países, ya que el tratante lo ve como un negocio redondo, en pocas palabras al tratante sólo le interesa su propio bienestar sin importarle prácticamente nada, puesto que en ocasiones la trata pasa desapercibida para las autoridades y siguen operando, en ocasiones, a plena luz del día.

La trata de personas es sin duda una grave violación de los derechos humanos y la dignidad de las personas. Es también una actividad criminal altamente lucrativa, en la que frecuentemente están involucradas redes del crimen asociadas a menudo con otras actividades delictivas como el tráfico de migrantes, el narcotráfico, lavado de dinero y tráfico de armas. La trata de personas se convierte así en un tema importante de seguridad nacional e internacional inclusive de salud pública.

El impacto de la trata en sus víctimas, especialmente en las mujeres y las niñas es devastador.⁶¹

México es un país en el que se captan personas con fines de trata, también somos un país por el cual transitan personas que son víctimas de trata,

⁶⁰ Ezeta, Fernanda, *Trata De Personas: Aspectos Básicos*, México, Comisión Interamericana de Mujeres de la Organización de Estados Americanos, Organización Internacional para las Migraciones, Instituto Nacional de Migración e Instituto Nacional de las Mujeres, 2006, p. 26, disponible en línea en <https://www.oas.org/atip/reports/trata.aspectos.basicos.pdf>, link visitado el 13 de septiembre de 2017.

⁶¹ Página de la Policía Federal, Acciones y Programas, “Trata de personas en el marco de operaciones encubiertas”, disponible en línea en <https://www.gob.mx/policiafederal/acciones-y-programas/trata-de-personas-en-el-marco-de-operaciones-encubiertas>, link visitado el 23 de octubre de 2017.

principalmente migrantes tanto del territorio mexicano como de Centroamérica y Sudamérica que muchas ocasiones fueron contactados por medio de la ingeniería social que se describe.⁶²

La trata de personas es definida por el Protocolo para prevenir, reprimir y sancionar la trata de personas, especialmente mujeres y niños que complementa la Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional, el su artículo 3 como:

“la captación, el transporte, el traslado, la acogida o la recepción de personas, recurriendo a la amenaza o al uso de la fuerza u otras formas de coacción, al rapto, al fraude, al engaño, al abuso de poder o de una situación de vulnerabilidad o a la concesión o recepción de pagos o beneficios para obtener el consentimiento de una persona que tenga autoridad sobre otra, con fines de explotación. Esa explotación incluirá, como mínimo, la explotación de la prostitución ajena u otras formas de explotación sexual, los trabajos o servicios forzados, la esclavitud o las prácticas análogas a la esclavitud, la servidumbre o la extracción de órganos”⁶³

En el ámbito nacional se define en la Ley General para Prevenir, Sancionar y Erradicar los Delitos en Materia de Trata de Personas y para la Protección y Asistencia las Víctimas de estos Delitos en el Capítulo II De los Delitos en Materia de Trata de Personas artículo 10 como: “Toda acción u omisión dolosa de una o varias personas para captar, enganchar, transportar, transferir, retener, entregar, recibir o alojar a una varias personas con fines de explotación...”⁶⁴

⁶² Ezeta, Fernanda, *op. cit.*, nota 60, p. 3.

⁶³ Naciones Unidas Oficina contra la Droga y el Delito, “Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional y su Protocolos”, disponible en línea en <http://www.unodc.org/documents/treaties/UNTOC/Publications/TOC%20Convention/TOCebook-s.pdf>, link consultado el 19 de diciembre de 2018.

⁶⁴ Ley General para Prevenir, Sancionar y Erradicar los Delitos en Materia de Trata de Personas y para la Protección y Asistencia a las Víctimas de estos delitos, disponible en línea en

La trata de personas, usualmente se suele relacionar con espacios específicos. “Los sitios más comunes en donde se detecta este delito son en zonas en donde se ejerce la prostitución, bares o clubes nudistas, lugares de producción de pornografía, agencias de acompañantes, fincas agrícolas, zonas de construcción, industrias informales, fábricas, hoteles y similares, circos, servicio doméstico”.⁶⁵

Algunas informaciones a los que se puede acceder dan cuenta de que en el país, el número de víctimas de trata de personas no se conoce con exactitud, se estima en 500,000 casos, de los cuales alrededor de 70,000 son menores de edad sujetos a explotación sexual. Gran parte de la proliferación de este ilícito se debe a que en México existen aproximadamente 47 grupos de delincuencia organizada involucrados en la trata de personas para fines sexuales y laborales, de acuerdo con una investigación para el Instituto Belisario Domínguez del Senado de la República.⁶⁶

Esta información la corroboran Rubén Torres y Jorge Monroy al señalar que México es un país de origen, tránsito y destino de víctimas de trata de personas

https://www.gob.mx/cms/uploads/attachment/file/310904/LEY_GPSEDM_TRAT_A_19-01-2018.pdf, link consultado el 19 de diciembre de 2018.

⁶⁵ Global Media, “¿Cómo identificar a una víctima de trata de personas?”, 4 de septiembre de 2017, disponible en línea <https://globalmedia.mx/articles/-C%C3%B3mo-identificar-a-una-v%C3%ADctima-de-trata-de-personas-> link visitado el 13 de septiembre de 2017.

⁶⁶ Ponce Sernicharo, Gabriela y Kánter Coronel, Irma del Rosario, *Al día las cifras hablan núm. 70. Día mundial contra la trata de personas*, México, Instituto Belisario Domínguez del Senado de la República, pp. 4-6. disponible en línea en <http://www.bibliodigitalibd.senado.gob.mx/bitstream/handle/123456789/3560/A-D-70.pdf?sequence=1&isAllowed=y>, link visitado el 23 de octubre de 2018.

y de acuerdo a información de la Procuraduría General de la República, órgano encargado de perseguir los delitos federales, en México.⁶⁷

Aunado a lo anterior tenemos que señalar que la inclusión de las Tecnologías de la Información y la Comunicación han permitido que las comunicaciones sean más ágiles y que por medio del uso de mensajes de texto, video, voz, fotografías se compartan e intercambien informaciones a una velocidad que antes no era posible.

Tal es el caso del Internet, que se utiliza de manera impune especialmente en aquellos países en los que aún no existe reglamentación. [...], es el medio con menor censura en nuestros días.

Lo anterior favorece la existencia de múltiples actividades ilegales en la red. En palabras de Gutiérrez [...], algunos delitos como los fraudes cibernéticos, el phishing, el pharming, la trata de personas y la pornografía, se encuentran tipificados en México a nivel Federal, Estatal y Municipal; sin embargo, la formación de ciberpolicias es insuficiente en este ámbito, ya que cuando se desmantela o niega el permiso a un dominio web, surgen 20 más del mismo contenido.

A pesar de ello, grupos interesados en la seguridad y la gobernabilidad de medios como el Internet, comienzan a dar frutos. Es así que en el año 2006, Atenas abrió el Foro Internacional de "Gobernanza de Internet". Este contemplaba la intención de legislarlo para todos los continentes; sin embargo es complicado, pues tratar de implementar una ley que rija al ciberespacio puede traducirse también como censura y atentado a la libertad de expresión [...]⁶⁸

⁶⁷ Torres, Rubén y Monroy, Jorge, "México, sin cifras precisas sobre trata", *El economista*, México, disponible en línea en <https://www.eleconomista.com.mx/politica/Mexico-sin-cifras-precisas-sobre-trata-20170730-0073.html>. Link visitado el 23 de octubre de 2017.

⁶⁸ Trujano Ruiz, Patricia, Dorantes Segura, Jessica y Trovilla Quesada, Vania, "Violencia en Internet: nuevas víctimas, nuevos retos", *et. al., op. cit.*, nota 13. Algunas citas del original fueron eliminadas.

Sin embargo los enganchadores suelen hacer uso de plataformas y redes sociales que utilizan los jóvenes e incluso niños para comunicarse como lo es Facebook y en ocasiones estos perfiles se crean sin precaución o supervisión de adultos en el caso de menores o con el conocimiento de los riesgos en jóvenes inexpertos lo que provoca que sean presas fáciles de los engaños de los delincuentes.

1.3.2 Antecedentes para entender qué es y cómo funciona la red social Facebook

Facebook es una empresa por medio de la cual se gestiona una red social denominada Facebook (en adelante FB) que es alimentada por los millones de usuarios alrededor del mundo que acceden desde la página oficial de Facebook y crean, a iniciativa propia, una cuenta denominada “perfil de usuario”.

A pesar de que Facebook no es la única red social es una de las más utilizadas a nivel mundial⁶⁹ junto con MySpace, Twitter, WhatsApp y LinkedIn. Todas estas comunidades requieren que las personas creen un perfil proporcionando cierta información que generalmente son datos personales a fin de que una vez creada la cuenta de usuario o perfil de usuario, se pueda interactuar con otras personas que también hayan creado un perfil de usuario en la misma red social.

En México según datos de la Asociación Mexicana de Internet el 98 por ciento de las personas que utilizan Internet tienen al menos una cuenta de Facebook. Esta red social es la más popular en nuestro país seguida por

⁶⁹ Por ejemplo hay catorce millones de usuarios estimados en España en 2015. En Chamorro Luser, Andrés, *et al.*, “Gestión de la privacidad de los perfiles de Facebook de adolescentes”, en *Revista de Medios de Educación*, núm. 48, enero 2016, p. 198, disponible en línea en <https://idus.us.es/xmlui/bitstream/handle/11441/39199/Gestion%20de%20la%20Oprivacidad%20de%20los%20perfiles%20de%20facebook.pdf?sequence=1&isAllowed=y>, 29 de octubre de 2018.

WhatsApp, YouTube, Instagram y Twitter.⁷⁰ La red social de Facebook en sus inicios fue pensada como apoyo en formato digital para que los estudiantes universitarios en Harvard se conocieran ya que era común en esta institución universitaria que se hicieran libros con las fotografías de los estudiantes al iniciar el ciclo escolar con esta finalidad.

Facebook permite a sus usuarios no solo comunicarse, sino también compartir fotos, juegos en línea y hasta revelar información personal, como el correo electrónico, la fecha de nacimiento, creencias religiosas o políticas, la ocupación laboral y el estado civil. Es, por tanto, un espacio con multiplicidad de aplicaciones, que inicialmente estaban centradas en la comunicación y el entretenimiento, pero que recientemente se ha convertido en un espacio interesante para la política o la economía, puesto que es fuente de información para los negocios y el marketing.⁷¹

La popularidad de Facebook hizo que en poco tiempo un gran número de estudiantes de otras universidades que tuviera un perfil en la red social pudieran entrar en contacto.

Desde el punto de vista del uso, en Facebook la mayoría de amigos se conocen y luego son invitados a convertirse en miembros del grupo de amigos en línea [...] que se puede fácilmente alcanzar una magnitud entre 200 a 250 amigos.

Los riesgos más habituales que se han desarrollado con la expansión del uso de Internet entre menores y adolescentes son: a) Adicción a las nuevas tecnologías; b) Ciberacoso sexual; c) Acceso a contenido poco fiable; d) Ciberbullying; e) Malinterpretación de la información social; f) Compartir información de otras personas; g) Publicar contenidos

⁷⁰ “14 Estudio sobre los hábitos de los usuarios de Internet en México 2018”, *Asociación de Internet. Mx*, disponible en línea en <https://www.asociaciondeinternet.mx/es/component/remository/Habitos-de-Internet/14-Estudio-sobre-los-Habitos-de-los-usuarios-de-Internet-en-Mexico-2018/lang,es-es/?Itemid=>, link consultado el 30 de octubre de 2018.

⁷¹ Chamorro Luser, Andrés, *et al.*, “Gestión de la privacidad de los perfiles de Facebook de adolescentes”, *op. cit.*, nota 69, pp. 197.

inadecuados; h) Pérdida de la anonimidad, etc. [...]. Estos riesgos son especialmente importantes entre los adolescentes si consideramos que éstos se caracterizan por priorizar la gratificación inmediata y el vivir el presente, creerse invulnerables al peligro, sentir curiosidad por nuevas vivencias estimulantes y arriesgadas, tener dificultad en el control de los impulsos y ser influenciados por los medios de comunicación y la publicidad, lo que los hace más susceptibles a las conductas de riesgo [...] consideran que un riesgo esperable entre los jóvenes usuarios de Facebook es sentirse incómodo o lamentar la divulgación de información privada y experimentar conflictos con los padres. En este contexto, los adolescentes constituyen un grupo de alto riesgo al ser los más familiarizados con Internet y a las redes sociales [...]. Es por ello que la privacidad juega un papel clave en la protección de los adolescentes respecto a estos riesgos.⁷²

Los países con mayor número de usuarios de Facebook son la India con 270 millones de usuarios, seguido por los Estados Unidos con 240 millones, Indonesia con 140 millones, Brasil le sigue con 130 millones y México ocupa el quinto sitio con 85 millones de usuarios, es por esto que el tema resulta relevante para nuestro país pues alertar que esta red social está siendo utilizada con fines de trata de personas permite dimensionar lo atractivo que resulta para los delincuentes hacer uso de esta herramienta para captar a sus víctimas, especialmente si son niños y adolescentes inexpertos y confiados en lo que respecta al manejo de la privacidad y la protección de sus datos.⁷³

⁷² *Ibidem*, pp. 198- 199. Algunas citas del original fueron omitidas en esta transcripción.

⁷³ Véase el “Ranking mundial de los 10 países con más usuarios de Facebook a fecha de abril de 2018”, *Statista.com*, portal de estadísticas, disponible en línea en <https://es.statista.com/estadisticas/518638/ranking-de-los-paises-con-mas-usuarios-de-facebook-a-nivel-mundial/>, link consultado el 30 de octubre de 2018.

1.3.3 Seguridad en perfiles digitales en FB

No se trata de causar una alarma o promover el cierre de perfiles en la red social señalando que es una red social insegura. De hecho los perfiles de Facebook dependiendo del país en el que se abra la cuenta, tienen determinadas normas de privacidad. Reconociendo que la seguridad de la información no puede existir al cien por ciento ni siquiera en el mundo físico ni en el digital, consideramos que la prevención en la manera en que se utiliza la información dentro de las cuentas de esta red social puede ayudar a disminuir los riesgos, detectar y disminuir las amenazas sobre el tema de suplantación de identidad y trata.

Es menester recalcar que si bien las cuentas de Facebook no cuentan con las mismas herramientas de privacidad en todos los países a causa de la diferencia de cada régimen jurídico de los países en donde se crean las cuentas de usuarios, sí podemos encontrar en algunos casos mayor certidumbre en el manejo de la información siempre y cuando el usuario conozca los medios para mantener privada su cuenta y no compartir su información personal y además de conocerlo tome el tiempo necesario para constantemente revisar la privacidad del perfil de usuario y de su biografía.

Principalmente los usuarios tienen la opción de controlar con quienes ponerse en contacto en el apartado de "Privacidad"; al entrar se brindan las opciones de "configuración y herramientas de seguridad"; estas tienen dos opciones, primero la relativa a los controles de "Tu actividad" y la otra sobre "Como pueden contactarte y ponerse en contacto contigo las personas" a partir de ahí el usuario puede controlar qué personas pueden ver el contenido del perfil y la biografía, controlar las publicaciones que otras personas hagan dentro de la biografía del usuario así como impedir que otras personas vean las publicaciones anteriores que se van almacenando en la biografía.

Es también relevante revisar el aspecto que tiene el perfil para otras personas ya que los delincuentes que buscan enganchar a sus víctimas preferirán perfiles de menores solos, o de mujeres solas, es importante saber que existen herramientas para controlar la revisión de la biografía porque así se puede evitar que personas desconocidas puedan tener acceso a lo que se

publica en los perfiles, en este espacio se controla cuando otras personas hacen etiquetas a nombre del usuario y con este control se puede tener control de las publicaciones que otros hagan lo que evita que por medio de publicaciones de terceros se ventilen datos de una persona y puedan quedar expuestos ante un público distinto al originalmente destinatario.

En esta parte de privacidad también se puede controlar evitar que otras personas vean la lista de amigos, o lo que se publique en la biografía.

1.3.4 Concepto de privacidad (privacidad en Internet) y privacidad en FB

Cuando hacemos referencia a la identidad digital, es casi imposible no referirnos al concepto de privacidad e intimidad de los individuos. Ambos conceptos no son sinónimos aunque tampoco se aseguran definiciones únicas o acuñadas como absolutas, ya que para algunos países el concepto se denomina vida privada, esfera privada, esfera íntima, derecho a estar solo, lo que ha dificultado su interpretación.

Por un lado se considera a la privacidad como aquel “ámbito de la vida privada que se tiene derecho a proteger de cualquier intromisión.”⁷⁴

Tomada del mismo Diccionario la intimidad se define como: “zona espiritual íntima y reservada de una persona o de un grupo, especialmente de una familia.”⁷⁵

Este derecho puede definirse como aquel que los individuos poseen para separar aspectos de su vida íntima del escrutinio público, por lo que, sin distinción, todos tenemos derecho a ella.

⁷⁴ Definición de “Privacidad”, tomada del Diccionario de la lengua española de la Real Academia Española, disponible en línea <http://dle.rae.es/?id=UD4g0KW> link visitado el 9 de septiembre de 2017.

⁷⁵ Definición de “Intimidad” tomado del Diccionario de la Real Academia Española, disponible en línea en <http://dle.rae.es/?id=LyCn6I9>, link visitado el 9 de septiembre de 2017.

Como lo plantea Diego García Ricci en su documento “Artículo 16 Constitucional. Derecho a la privacidad”, las primeras acepciones de este derecho fueron acuñadas en Estados Unidos a finales del siglo XIX, debido a la aparición de las fotografías instantáneas. Con la tecnología de aquellos años, se atentaba contra la “vida doméstica”, desde el momento en el que las imágenes podían ser difundidas de forma masiva. En aquéllos años se definió como el derecho a **no ser molestado**.

Posteriormente, el concepto de privacidad incluyó otros elementos destacables como la facultad que toda persona posee para determinar la manera, el momento y la información personal que podía ser comunicada con otras personas. En otras palabras, esta idea ofrecía la posibilidad y el **derecho a controlar la información propia**, incluso luego de que fuese compartida.

Como en aquellos años, el derecho a la privacidad continúa vigente y es cada vez más relevante, como una forma de procurar nuestras actividades íntimas y del mismo modo, la preocupación se mantiene debido a los nuevos desarrollos tecnológicos. En la actualidad estamos inmersos en un sinnúmero de nuevas herramientas digitales que exponen nuestras actividades cada vez más, incluso con nuestro consentimiento, o también, a partir de nuestro desconocimiento.⁷⁶ (Énfasis del original).

⁷⁶ Mendoza, Miguel Ángel, “El derecho a la privacidad en la era digital”, *welivesecurity by eset*, 2 de marzo de 2017, disponible en línea en <https://www.welivesecurity.com/la-es/2017/03/02/derecho-a-la-privacidad-era-digital/>, link consultado el 23 de octubre de 2017.

Véase también García Ricci, Diego, “Artículo 16 constitucional. Derecho a la privacidad”, en Ferrer Mac-Gregor Poisot, Eduardo *et al.*, (coords.), *Derechos Humanos en la Constitución. Comentarios de Jurisprudencia Constitucional e Interamericana*, México, Suprema Corte de Justicia de la Nación, UNAM y Konrad Adenauer Stiftung, Programa Estado de Derecho para Latinoamérica, 2013.

Es precisamente que el avance tecnológico ha traído como consecuencia que los individuos pierdan el control sobre los datos y la información que sobre ellos mismos se tiene disponible.

De acuerdo a la Organización Argentina Segura “La privacidad en Internet podía entenderse como el control que ejerce un usuario sobre su información para limitar la cantidad de personas autorizadas a obtenerla”.⁷⁷

Coincidimos con los autores Piñar Mañas y Recio Gallo cuando sostienen que:

El derecho a la privacidad en Internet implica que deba considerarse la aplicación de la normatividad relativa a la protección de datos personales, pero, más allá de ésta, también la relativa a los derechos de los usuarios de servicios de telecomunicaciones, el secreto de las comunicaciones, así como la interrelación entre el derecho a la privacidad y otros derechos humanos, como la libertad de expresión, libertad de asociación u otros...⁷⁸

Las personas deben de conocer cómo proteger su privacidad e intimidad en los medios digitales, principalmente hay que reconocer que la vida personal que se expone en medios digitales como son las redes sociales una vez que se hacen públicas, difícilmente, si no es que imposiblemente, vuelven a ser privadas.

⁷⁷ Argentina Cibersegura, “¿Qué es la privacidad en Internet?”, disponible en línea en https://www.argentinacibersegura.org/admin/resources/files/consejos/33/Gu%C3%ADa_sobre_Privacidad.pdf, última fecha de consulta el 23 de diciembre de 2018.

⁷⁸ Piñar Mañas, José Luis y Recio Gayo, Miguel, “La privacidad en Internet”, en Recio Gayo, Miguel, *Temas selectos de derecho digital mexicano*, México, Suprema Corte de Justicia de la Nación, Centro de Estudios Constitucionales, 2016, pp. 73 – 74, disponible en línea en <https://www.sitios.scjn.gob.mx/cec/node/190>, link visitado el 23 de diciembre de 2017.

Miguel Ángel Mendoza en su artículo “El derecho a la privacidad en la era digital” da algunas opciones para cuidar nuestra privacidad como: navegar en sitios confiables, no compartir información sensible con desconocidos, configurar las opciones de privacidad de las redes sociales, evitar el uso de redes abiertas para operaciones sensibles, cerrar todas las sesiones iniciadas en Internet así como borrar el caché que permite acceder fácilmente a las cuentas recordando los nombres de usuario y las contraseñas.⁷⁹

Debido a que el tema de Privacidad e Internet es un tema vasto y que no es el tema central de esta investigación baste hasta aquí con lo expuesto para continuar con el tema de protección de la privacidad en Internet y permítasenos continuar con algunas recomendaciones sobre cómo proteger la privacidad de las personas en el internet de acuerdo a diversos órganos especializados.

Por ejemplo la Agencia Española de Protección de Datos en su “Guía de Privacidad y Seguridad en Internet”, menciona: la importancia del uso de contraseñas, la necesidad de reconocer páginas apócrifas, el derecho de las personas a negarse a proporcionar sus datos, la importancia del borrado de datos de los navegadores.⁸⁰

Otra herramienta de gran utilidad es la Guía de Privacidad en Internet de la ESET (Enjoy Safer Technology), que señala revisar la privacidad del perfil a través de los accesos directos de privacidad, hacer una comprobación rápida de privacidad para decidir qué público puede tener acceso a la información que se publica, tomar decisiones informadas sobre las aplicaciones que tienen acceso a nuestro perfil, en la medida de lo posible eliminar y no compartir en el perfil los datos personales como teléfono, correos electrónicos, fechas de cumpleaños y ciudad de origen ya que a mayor número de datos que se comparten se está en

⁷⁹ *Idem.*

⁸⁰ Véase Privacidad y Seguridad en Internet, por la Agencia Española de Protección de Datos disponible en línea en <https://www.aepd.es/media/guias/guia-privacidad-y-seguridad-en-internet.pdf>, última fecha de consulta el 23 de diciembre de 2018.

un mayor riesgo de sufrir algún tipo de ataque por medio de por ejemplo ingeniería social,⁸¹ como los que se explicarán en capítulos más adelante.

La página Argentina Cibersegura menciona también algunas medias para proteger la privacidad en Internet como es, configurar los perfiles de las redes sociales, concientizar a los menores sobre los peligros y alcances del Internet, e instalar un antivirus.⁸²

Existen además otros sitios como el portal Universia de España presenta 5 consejos útiles para proteger nuestra identidad digital en Internet.

1. Somos lo que publicamos

Cuida tus publicaciones y tus datos. Todo dato o información que brindes a la red no podrá borrarse y estará en algún rincón. Asegúrate de pensar bien qué decir, qué ubicación dar y cuáles fotos o videos compartir.

2. Búscate en Google

Aunque parezca de película, es necesario que conozcas tu presencia en la web. Al buscarte en Google sabrás qué información tuya es pública y cuánto se sabe de ti. Así podrás saber cómo actuar y cuánto más ocultar.

3. Configura la privacidad de tus redes

No dejes todo al libre albedrío. Cuidar tus redes también implica configurar de la mejor manera posible tu privacidad, aquello que publicas e incluso tus datos. De esta forma te asegurarás de que nadie pueda robarte tu identidad.

4. Evita el WiFi público

Todos nos alegramos cuando entramos a un lugar con WiFi, sin embargo, es una red poco segura en la cual quedamos expuestos al robo de cualquier información. Asegúrate de no realizar transacciones bancarias con WiFi público o brindar datos importantes.

5. Conoce tus derechos

⁸¹ ESET, Guía de Privacidad en Internet, disponible en línea en <https://www.welivesecurity.com/wp-content/uploads/2015/09/eset-guia-privacidad-internet.pdf>, última fecha de consulta el 23 de diciembre de 2018.

⁸² Argentina Cibersegura, *op. cit.*, nota 77.

Ten en cuenta la Ley de Protección de Datos Personales en Posesión de Particulares, la cual obliga a las empresas a proteger tus datos. Incluso puedes recurrir al derecho a desindexar si consideras que tu persona está siendo perjudicada, para ello debes denunciarlo en Google.⁸³

Otro sitio es la enciclopedia digital Wikipedia que brindan algunos consejos de cómo se puede proteger la privacidad en Internet:

- Utiliza[r] un seudónimo y no tú nombre real en Internet, excepto que sea estrictamente necesario.
- Instalar un cortafuego [...para evitar] que un sujeto pueda entrar a nuestra computadora o bien que usen un troyano y quizá pueda robar información valiosa como tarjetas de crédito o claves, etc[étera].
- [Instalar u]n antivirus que en lo posible también detecte spyware servirá mucho para evitar que nos manden troyanos o spyware que envíe información confidencial, aunque si tenemos un firewall es probable que este bloquee el troyano/spyware al tratar de conectarse.
- [Instalar u]n antispymware que ayuda a eliminar el spyware que entró a través de distintas páginas.
- Usar un navegador web [alternativo a Internet Explorer, o bien mantenerlo] actualizado.
- Mantener actualizado nuestro sistema operativo [es importante para evitar que a través de un fallo del mismo alguien se pueda apoderar de nuestra computadora y posteriormente de algo valioso].
- No entrar en páginas web sospechosas de robar contraseñas o de mandar virus/spyware al PC.
- [...]
- No realizar transacciones comerciales en páginas web no seguras, las seguras tienen una "s" después del http

⁸³ Universia España, "5 consejos para cuidar tu identidad digital en Internet", 14 de julio de 2016, disponible en línea en <http://noticias.universia.es/ciencia-tecnologia/noticia/2016/07/14/1141808/5-consejos-cuidar-identidad-digital-internet.html>, link visitado el 10 de septiembre de 2017.

- Estudiando.⁸⁴

Al respecto de los sitios con https se recomienda cautela ya que la “s” solo significa que el sitio cuenta con un certificado para poder dar un cifrado en los datos que se generan pero, los delincuentes ahora diseñan páginas con estos certificados haciendo páginas apócrifas con el candado de “seguro” lo que hace que los usuarios no desconfíen y sea más sencillo robar sus datos.⁸⁵

De esta manera la privacidad en Internet y la privacidad en los perfiles de los usuarios de Facebook no pueden estar garantizadas al cien por ciento pero sí puede existir un mínimo de seguridad siempre y cuando los usuarios sepan cómo proteger su información y manejar correctamente los perfiles de sus cuentas.

1.3.5 Datos y datos personales. Conceptos básicos

Los datos personales como se anotó con anterioridad son todos aquellos datos que permiten identificar o hacer identificable a una persona. Estos datos revelan, el nombre de las personas, su nacionalidad, su domicilio, teléfono, correo electrónico, su firma, etcétera.

En nuestro país se cuenta con un marco regulatorio que protege y garantiza la protección de estos datos. Desde el año 2002 se publicó la Ley de Transparencia y Acceso a la Información Pública Gubernamental,⁸⁶ en la cual se

⁸⁴ Información obtenida de la búsqueda Privacidad en Internet en Wikipedia, disponible en https://es.wikipedia.org/wiki/Privacidad_en_Internet, link consultado por última vez el 19 de septiembre de 2018.

⁸⁵ “El protocolo HTTPS no garantiza la seguridad”, *Kaspersky*, 17 de enero de 2018, disponible en línea en el link <https://latam.kaspersky.com/blog/https-does-not-mean-safe/12331/>, consultado por última ocasión el 19 de noviembre de 2018.

⁸⁶ Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, publicada en el Diario Oficial de la Federación el 11 de junio de

incluyó la temática de protección de datos personales en el ámbito público a nivel federal y también se realizó la reforma al artículo sexto constitucional en el que se incluyó la protección de los datos personales y al artículo 16 constitucional que ponía como límite al derecho de acceso a la información justamente a los datos personales.

En año 2010 se publicó la Ley Federal de Protección de Datos Personales en Posesión de los Particulares y finalmente en el año 2017 se ha publicado la Ley General de Protección de Datos Personales en posesión de los Sujetos Obligados.⁸⁷

A nivel internacional existen varios documentos en la materia de protección de datos personales como en la Unión Europea con el Convenio para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal que fuera firmado en 1981 por Alemania, Francia, Dinamarca, Australia y Luxemburgo y conocido como el “Convenio 108”. Al cual México se ha adherido y a su protocolo el 12 de junio y 28 de septiembre de 2018 respectivamente, según consta en los Diarios Oficiales.

Estos documentos han servido como guía para que nuestro país incluya ciertos estándares y normatividad en la materia. Por no ser objeto de este trabajo profundizar en un análisis comparativo del tema sirva solamente mencionar que:

En el mundo existen dos vertientes principales entorno a la protección de los datos personales: El modelo europeo busca proteger la información y la propiedad de la misma, en aras de conservar la honorabilidad de la

2002, disponible en línea en <http://inicio.ifai.org.mx/LFTAIPG/LFTAIPG.pdf>, última fecha de consulta el 23 de diciembre de 2018.

⁸⁷ La Ley se puede consultar en el siguiente link <http://www.diputados.gob.mx/LeyesBiblio/pdf/LGPDPPSO.pdf>, última fecha de consulta el 19 de noviembre de 2018.

Para profundizar en el tema se sugiere dar lectura al documento elaborado por el INFOEM, *El abc de los datos personales*, disponible en https://www.infoem.org.mx/doc/publicaciones/ABC_Datos.pdf, link consultado el 30 de octubre de 2018.

persona aun cuando ésta hubiese fallecido, la motivación de este modelo tiene base en los derechos humanos de los individuos. El modelo estadounidense pretende proteger la información de las personas con el concepto de derecho a la privacidad, el cual puede extinguirse con la muerte del sujeto, el modelo surge derivado de motivos comerciales ya que las empresas utilizaban de manera indiscriminada esa información.⁸⁸

Es precisamente por la diferencia que hacen los Estados en sus normas que en materia de protección de los datos personales actualmente no hay una uniformidad al respecto. Existen algunos estándares pero no existe una forma única de cuál debe ser el tratamiento adecuado para los datos en el ciberespacio, por esto aún es mucha la responsabilidad que se deja en manos de los propios individuos.

1.3.6 Protección de datos personales en FB

En Facebook, la privacidad de los usuarios tiene como base la protección que se hace a la protección de los datos personales y es una parte importante para el cuidado de la identidad digital sin embargo también el hacer minería de los datos es una actividad cotidiana que se realiza a través de esta y otras redes sociales.

La identidad digital como se anotó con anterioridad es:

La información asociada a las actividades que los usuarios llevamos a cabo en el ciberespacio, como resultado de la interacción con otros usuarios, organizaciones o servicios en Internet, donde generalmente se trata [n...] datos personales que suelen ser concedidos a terceros.

[Gran parte del problema con la privacidad es que e]stos últimos suelen procesar, almacenar o transmitir los datos de los usuarios, incluso hasta el grado de lucrar con esa información. En la actualidad, muchos servicios de

⁸⁸ Sánchez Pérez, Gabriel y Rojas González, Isai, “Leyes de protección de datos personales en el mundo y la protección de datos biométricos. Parte I”, en *Revista .Seguridad* de la Dirección General de Tecnologías de Información y Comunicación de la Universidad Nacional Autónoma de México, núm. 13, pp. 5 y 6.

Internet conocen gran parte de las actividades de los usuarios, gustos, preferencias, así como sus datos personales, mismos que se utilizan con fines comerciales. Por lo tanto, la protección de esta información contribuye a preservar nuestra intimidad.⁸⁹

Como hemos comentado no en todos los países se regula la protección de datos de la misma manera, incluso, es común observar como algunos sitios en internet como YouTube o mismo Facebook tienen políticas distintas entre un país y otro, esto ocasiona que temas como la suplantación de identidad de perfiles digitales como los creados en Facebook sean tratados de manera poco uniforme.

Sin embargo es importante no solo que existan normas en torno a la privacidad y la protección de los datos personales de los usuarios sino que también los usuarios de esta red social que es Facebook estemos conscientes de los riesgos que pueden existir por un mal uso de la plataforma.

Hasta el día de hoy las políticas de privacidad de Facebook no son del todo conocidas por sus usuarios. Después del problema de Cambridge Analytica,⁹⁰ su espacio se modificó y hoy se explica de manera más sencilla en nueve pasos, qué tipo de información se recopila, cómo se usa la información, cómo se comparte la información, cómo trabajan en conjunto con Facebook otras empresas, cómo los usuarios pueden administrar y eliminar su información. También hay un espacio sobre solicitudes legales y evitar engaños, sobre las notificaciones en cambios a sus políticas de privacidad y de cómo hacer llegar dudas al respecto, en general se ha simplificado la información para que los

⁸⁹ Mendoza, Miguel Ángel, “El derecho a la privacidad en la era digital”, *op. cit.*, nota 76.

⁹⁰ BBC Mundo, “5 claves para entender el escándalo de Cambridge Analytica que hizo que Facebook perdiera US\$37.000 millones en un día”, disponible en <https://www.bbc.com/mundo/noticias-43472797>, última fecha de consulta el 19 de noviembre de 2018.

usuarios de la red social tengan información más clara al respecto de temas de privacidad y la protección de sus datos.⁹¹

1.3.7 Suplantación de identidad en FB

La suplantación de identidad en la red social conocida como Facebook es una actividad que se ha ido incrementando con el paso del tiempo.

Las personas que crean cuentas de usuarios requieren de un registro en el que determinan la información que proporcionan para así socializar dentro de la red. En 2017 se reportaban más de dos mil millones de usuarios.⁹² Sin embargo no existe información sobre cuántos de esos millones de usuarios utilizan seudónimos, o crean perfiles falsos.

Como se anotaba arriba, el crear un perfil señalando un nombre distinto o indicando ser otra persona no representa en si una acción ilegal. Sí lo es en cambio, el hacerse pasar por una persona distinta que sí existe y no somos esa persona, es decir cuando se está suplantando la identidad de alguien. Esta actividad ilícita es cada vez más común, por ejemplo, de acuerdo a las estadísticas sobre el robo de identidad del programa de seguridad Panda que señala que aproximadamente 60 millones de ciudadanos americanos han sido afectados por el robo de identidad en el año 2017.⁹³

⁹¹ La información está disponible en <https://www.facebook.com/privacy/explanation>, última fecha de consulta el 19 de noviembre de 2018. En el sitio inclusive se puede acceder a una liga en Internet para consulta y una dirección postal en Melano Park California.

⁹² APF, "Facebook alcanza los 2,000 millones de usuarios", El economista, disponible en línea en <https://www.eleconomista.com.mx/tecnologia/Facebook-alcanza-los-2000-millones-de-usuarios-20170627-0013.html>, última fecha de consulta el 23 de diciembre de 2018.

⁹³ Véase el reporte de Estadísticas de robo de identidad proporcionadas por la página oficial de Panda, disponible en <https://www.pandasecurity.com/mediacenter/news/identity-theft-statistics/>, consultado el 3 de noviembre de 2018.

Dentro de las redes sociales que sufren mayores ataques se encuentran justamente Facebook, Instagram y Snapchat, con un 46 por ciento de porcentaje de riesgo de que las cuentas sean suplantadas.⁹⁴

La difusión sobre el tema de robo de identidad y las medidas que deben de seguirse para combatirla debería de ser una obligación para todos los usuarios de computadoras, tabletas, teléfonos celulares y extenderlo a los usuarios de las redes sociales como Facebook pues debido a la propia naturaleza de estas formas de comunicación, las personas son animadas a compartir información personal y de sus contactos por lo que un número cada vez mayor de usuarios se convierten en víctimas del robo de identidad.

Los usuarios de Facebook debemos de estar conscientes de que los ladrones de identidad están constantemente intentando nuevas estrategias para robar la información personal y muchas veces somos los mismos usuarios los que proporcionamos los datos que nos solicitan.⁹⁵

No podemos olvidar que como hemos mencionado anteriormente Facebook tuvo un gran problema respecto al caso Cambridge Analytica que afectó a 87 millones de usuarios de Facebook alrededor del mundo; la mayoría

⁹⁴ *Idem.*

⁹⁵ Tomado de “Identity Theft Prevention Tips for Facebook Users”, Kaspersky Lab, el original en inglés dice: Identity theft protection is a must for all computer users, and that extends to social media such as Facebook. Because of the very nature of social networking sites — where people are encouraged to share personal information — users are automatically at risk of becoming victims of identity theft.

Facebook users should be aware that identity thieves are constantly coming up with new scams aimed at stealing personal data. And oftentimes, that data is publicly accessible and within easy reach.

Traducción libre.

de ellos en los Estados Unidos⁹⁶ lo que dejó al descubierto la facilidad con la que los datos de los usuarios pueden ser compartidos sin que los dueños de los mismos sepan en realidad cuándo y con qué fin se pueden compartir estos datos o en el peor de los casos sean los delincuentes quienes sustraigan información de las cuentas particulares de los usuarios.

1.3.8 El uso de técnicas de ingeniería social en FB

De conformidad con el glosario de términos publicado en la web de la European Union Agency for Network and Information Security (ENISA) “la ingeniería social se refiere a todas las técnicas dirigidas a hablar con un objetivo para que revele información específica o realice una acción específica por razones ilegítimas”.⁹⁷ Se destaca que las técnicas de ingeniería social explotan las vulnerabilidades humanas, más que tecnológicas.

Las técnicas de ingeniería social pueden presentarse de diversas maneras, las más reconocidas son el phishing, el pharming y el uso de malware. La ingeniería social del phishing y el pharming permite que por medio del engaño los delincuentes dirijan a los usuarios a páginas de Internet parecidas a las oficiales pero que en realidad son falsas y una vez que son conducidos a estos espacios le son solicitados sus datos, sobre todo bancarios y financieros, para posteriormente tener acceso a estas cuentas y disponer de los recursos de las víctimas.

⁹⁶ Badshah, Nadeem, “Facebook to contact 87 million users affected by data breach”, *The Guardian*, 8 de abril de 2018, disponible en <https://www.theguardian.com/technology/2018/apr/08/facebook-to-contact-the-87-million-users-affected-by-data-breach>, consultado el 2 de noviembre de 2018.

⁹⁷ Véase: European Union Agency for Network and Information Security, “What is ‘Social Engineering’?”, disponible en línea en <https://www.enisa.europa.eu/topics/csirts-in-europe/glossary/what-is-social-engineering>, última fecha de consulta el 23 de diciembre de 2018.

Sin embargo, también existe la técnica de la sextorsión en la que los delincuentes se hacen pasar como posibles relaciones casuales y trabajan para que las personas les envíen fotografías o videos comprometedores para posteriormente chantajearlos y extorsionarlos. De la mano con este tipo de actividad se ha difundido la actividad de crear afinidad expandida, esta se trata de relacionarse con las posibles víctimas a través de sus intereses manifiestos como puede ser activismo social, acudir a conciertos, espectáculos, compartir la misma afición por algún deporte. Una vez que se logra tener los datos suficientes los delincuentes tienen facilidad de aproximarse a las víctimas, esta es una de las maneras más socorridas por los tratantes de personas.

Existen muchas otras técnicas de ingeniería social que se utilizan para captar a víctimas de trata como son: ofertar vacantes de empleo falsas, ofrecer viajes con grandes descuentos a lugares desconocidos, prometer cursos o capacitaciones que prometen cambiar vidas, entre muchos otros listados algunos a continuación.

Pretexting: es una variación de la ingeniería social, con la diferencia de que, para realizarla, el atacante debe tener un estudio previo de la información de la víctima potencial, para así, crear y utilizar un escenario favorable con el objetivo de persuadir a una víctima y obtener información. El atacante puede acoplarse a una víctima específica de manera que aumenta la posibilidad de conseguir información o que la víctima realice acciones específicas a su voluntad.

[...]

Shoulder surfing o espionaje por encima del hombro: es una técnica derivada de la observación, la particularidad que tiene es que el espionaje a los usuarios se realiza de cerca, para obtener información confidencial. Sólo basta con permanecer observando sigilosamente por la espalda de la víctima las teclas que digita, el monitor o cualquier otro soporte de información que pueda ser de interés para obtener información. Esta técnica se utiliza comúnmente para obtener contraseñas, números PIN, códigos de seguridad y datos similares.

[...]

Dumpster diving: es una técnica que se centra en buscar información valiosa en la basura. Tirar cualquier tipo de documentos sin un debido proceso de destrucción es una práctica que puede resultar riesgosa, pues se pueden rescatar de la basura datos importantes contenidos en documentos desechados sin ser destruidos previamente.

Asalto al buzón de correo: es un delito centrado en el robo de la correspondencia que se encuentra en los buzones de correo sin seguro, de los cuales se pueden sustraer documentos con información valiosa (estados de cuenta bancarios o de tarjetas de crédito, o cualquier otro documento).⁹⁸

La suplantación de la identidad digital en Facebook permite que a través de la ingeniería social los usuarios sean manipulados y de esta manera puedan ser una víctima de la trata de personas.

Se recomienda evitar conectarse a las redes WiFi públicas porque son utilizadas muchas veces por los hackers ya que como su nombre lo indica, “Wifi gratis” es atractivo para cualquier usuario en apuros, ya sea que se le hayan acabado sus datos, o tenga una emergencia, encontrar una red abierta es un respiro para este mundo donde necesitamos estar conectados. Al ser de libre acceso hace a la red vulnerable ya que cualquiera puede tomar nuestros datos y hacer mal uso de ellos, así como también podrían llegar a instalar software espía en nuestro equipo portátil sin que nos demos cuenta del suceso.

Por ejemplo, supongamos que queremos enviar un mensaje a alguno de nuestros contactos a través de una red pública. Si el mensaje no va cifrado, un atacante puede leer ese mensaje, y modificarlo como quiera para que nuestro contacto reciba algo diferente como si fuera nuestro. Esto también se puede aplicar a nosotros, porque el atacante puede enviarnos una respuesta falsa de nuestro contacto para hacernos pensar que todo va bien.⁹⁹

⁹⁸ Guía para prevenir el robo de identidad, *op. cit.*, nota 56, p. 6.

⁹⁹ Omicrono, “Cuales (sic) son los peligros reales de utilizar redes WiFi públicas y cómo prevenirlos” 14 de mayo de 2015, disponible en línea en

Si llegáramos a usar una red pública hay que evitar ingresar contraseñas, correos electrónicos, hacer transacciones bancarias, verificar que a la páginas en las que naveguemos tengan el HTTPS activado, y de ser posible utilizar una red privada virtual que sirve para proteger y cifrar nuestra conexión.¹⁰⁰ En todo caso hay que “mitigar los riesgos a través de una combinación de protección personal y conciencia sobre el uso de Internet”.¹⁰¹

Es necesario entender las nuevas modalidades de ingeniería social que son utilizadas para captar víctimas de ilícitos como puede ser el robo de información, la suplantación de la identidad y hasta la trata de personas y poder prevenirlo.

1.4 Selección de perfiles por parte de los delincuentes con fines de trata

Los perfiles de Facebook que son preferidos por los delincuentes principalmente son aquellos que no tienen ningún filtro de privacidad, es decir en el que pueden mirar la información de los contactos, las fotos, las publicaciones, la información personal, entre más datos se puedan obtener mucho mejor.

Dentro de la información que es más atractiva se encuentran las fechas de cumpleaños, los números de teléfonos, las personas que tienen muchos contactos ya que muchos de esos contactos seguramente no son en realidad relaciones de amistad y es fácil aceptar a desconocidos como parte de los “amigos” y así tener mayor posibilidad de acceder a datos sobre la persona.

Las fotografías y las indicaciones sobre lugares que se frecuentan y los horarios en que se frecuentan también son datos de utilidad para los

<http://omicronno.elespanol.com/2015/05/peligros-de-utilizar-redes-wifi-publicas/>,

link visitado el 10 de septiembre de 2017.

¹⁰⁰ Como se mencionó también líneas anteriores el que una página tenga un certificado HTTPS no puede tenerse por sentado que es un lugar seguro.

¹⁰¹ Kaspersky Lab, “¿qué es el pharming y cómo evitarlo?”, disponible en <https://latam.kaspersky.com/resource-center/definitions/pharming>, última fecha de consulta el 19 de noviembre de 2018.

delincuentes por lo que un perfil que provea estas informaciones serán seleccionados sobre los que manejan algún tipo de protección a la información.

Los tratantes estarán buscando perfiles con información de menores, hombres y mujeres que tengan comentarios o alusiones a sus colegios, centros de trabajo, y en general lugares que frecuenten habitualmente.

Es por esto que constantemente es preciso revisar la privacidad que se maneja en los perfiles de usuarios de la red social ya que con algunas actualizaciones se debe de volver a activar la privacidad de las publicaciones, fotografías, y en general los datos que se tienen en la cuenta de usuario.

Algunos perfiles que buscan los delincuentes son de adolescentes, niños y niñas, que son los más vulnerables a ser víctima de trata por la incomprensión del uso y alcance de esta red social, para algunos internautas¹⁰² que creen que solo sirven para chatear y subir fotos sin control ni medidas, todos esos errores que son aprovechados por traficantes para comenzar la búsqueda y contacto con los menores y toda potencial víctima. Es verdad que los menores de 13 no deberían contar con perfiles de Facebook pues esto va en contra de sus perfiles de uso, pero esto en la práctica no se ha podido evitar.

Estos tratantes prometen en ocasiones empleo fácil y seguro con un alto y desorbitado sueldo por labores demasiado sencillas, sin tomar en cuenta la edad ni experiencia alguna, a esto se le suma las declaraciones de amor falsas solo para enganchar, a través de la palabra prometen viajes, dinero, amor y felicidad y a través de falsas agencias de modelos solicitan fotos de jóvenes, aprovechando su ilusión.¹⁰³

¹⁰² Definición del diccionario Oxford en español, “Internauta”: Persona que utiliza los servicios de Internet u otra red informática” disponible en línea en <https://es.oxforddictionaries.com/definicion/internauta>, link visitado el 13 de septiembre de 2017.

¹⁰³ Facebook Notes, Fundación María de los Ángeles, “Trata de personas, métodos de reclutamiento”, en línea <https://www.facebook.com/notes/fundaci%C3%B3n-mar%C3%ADa-de-los->

Esto orilla a que la víctima busque escapar de casa por la ilusión que le provoca tener una oportunidad como esas, el tratante aprovecha esta situación y procede a la captura y privación a la libertad para proceder a labores de explotación laboral, sexual entre otras, de las cuales es casi imposible salir.

La falta de comunicación hacia los padres es un factor importante para conocer un motivo para que los adolescentes se refugien en las redes sociales, principalmente se da porque el hijo siente que no se le respeta su privacidad, siente que no se le comprende, tiene vergüenza de contar las cosas tal y como son, o el simple hecho de no causarle preocupación a los padres. Esto lleva a que el adolescente oculte y guarde las cosas que le pasan cada día.

Existen sin embargo otros factores que hacen vulnerables a las posibles víctimas, mismos que pueden verse reflejados en la información que publican en sus perfiles en la red social como puede ser: “la pobreza, la marginación, el desempleo, la falta de escolaridad, la desintegración o la disfunción familiar, la violencia doméstica, las desigualdades, la baja tasa de matriculación escolar, así como la condición de migrante, la preferencia étnica y otros factores culturales”.¹⁰⁴

El uso de herramientas de privacidad incluidas en Facebook, como los controles de quiénes pueden contactar o ver las publicaciones es vital para restringir el acceso de personas no deseadas en los perfiles, es necesario ajustar todas estas medidas con mucho cuidado, de igual manera evitar aceptar a desconocidos, ser muy precavidos en el uso de la red social y ser muy observadores con actividad inusual.

http://www.senado.gob.mx/comisiones/trata_personas/docs/Diagnostico_Trata.pdf, link visitado 13 de septiembre de 2017.

¹⁰⁴ Cfr. Senado de la República, *Diagnóstico sobre la situación de la Trata de Personas en México*, p. 23, http://www.senado.gob.mx/comisiones/trata_personas/docs/Diagnostico_Trata.pdf, última fecha de consulta 23 de diciembre de 2018.

Podemos sacar varias conclusiones, por ejemplo, la falta de comunicación con los padres, esto es un problema grande ya que es un factor importante en la problemática de actitud con los más jóvenes pero también como se ha mencionado a las desigualdades, la pobreza, la ignorancia la baja escolaridad entre muchos otros.

1.5 ¿Cómo identificar si se es víctima de un robo de identidad?

Finalmente es preciso indicar qué es lo que se debe de hacer en caso de estar ante un caso de suplantación de la identidad, recordemos que por lo general la suplantación de la identidad se realiza para obtener los datos bancarios y patrimoniales para poder obtener acceso a estos recursos, sin embargo; la suplantación de identidad aunque se ha estudiado menos en este aspecto, también se suele utilizar para contactar a posibles víctimas de trata de personas.

Es muy común que las personas no se den cuenta de que su identidad ha sido suplantada sino hasta después de que se cometen desfalcos o los recursos han sido dispuestos por los delincuentes.

Las señales que indican que se ha sido víctima de un robo de identidad pueden ser:

- Llamadas de despachos de cobranza con respecto a deudas que no hayas adquirido.
- Si recibes tarjetas de crédito que no hayas solicitado.
- Si te niegan solicitudes de crédito de forma inesperada.
- Si no recibes correspondencia que esperabas o se reduce la cantidad de esta.
- Si observas cargos o retiros en tu crédito o tarjeta de débito que no hayas realizado.
- Tus tarjetas son denegadas.
- Encuentras en tu reporte de crédito cuentas o cargos no reconocidos.
- Recibes la notificación de vulneración de una empresa que tiene en posesión tus datos personales.
- Si ves inicios de sesión en tu red social sospechosos o de ubicaciones erróneas.

- Comienzas a ver interacciones o me gusta a páginas que no hayas visitado.¹⁰⁵

Si la información fue usada para objetivos maliciosos será mejor cambiar la contraseña de manera inmediata. De ser posible cambiar también tu nombre de usuario. De igual forma cambiar las contraseñas que sean iguales a la que fue vulnerada y usar diferentes contraseñas para cada red social.

También se sugiere estar atentos a otros tipos de extorsión que existen como por vía telefónica que suelen solicitarnos datos como dirección, o algún número de tarjeta, de la misma manera en Internet evita rellenar formularios con datos personales, jamás proporcionar contraseñas en páginas de dudosa reputación.

Las contraseñas pueden ser almacenadas mentalmente o también se puede utilizar un gestor de contraseñas donde se almacene toda información en la nube, podemos mencionar algunos gestores de contraseñas como Lastpass, 1Password y KeePass.

Es esencial protegernos con un software antivirus spyware en nuestros equipos de cómputo ya que pueden llegar a ser intervenidos de manera remota para intentar extorsionarnos vía redes sociales. También en ocasiones se ha llegado a ver como algunas personas colocan un pedazo de cinta no transparente, o un post it en la parte frontal de sus equipos de cómputo, justo en la parte de la cámara web y de la misma manera en la parte del micrófono. Incluso se ha visto por la web que el creador de Facebook hace uso de este último método¹⁰⁶ el cual no es infalible.

¹⁰⁵ S/a, *Guía para prevenir el robo de identidad*, México, INAI, *op. cit.*, nota 56, p. 13.

¹⁰⁶ RT, ¿Por qué Zuckerberg tapa la cámara y el micrófono de su ordenador?, 27 de junio de 2016, disponible en línea en <https://actualidad.rt.com/actualidad/211460-zuckerberg-tapar-camara-microfono-laptop>, link visitado el 9 de septiembre de 2017.

Entramos en la parte de las publicaciones en redes sociales, en Facebook los usuarios suelen subir publicaciones sin control, colocan donde están, con quien, y que es lo que hacen, así se están exponiendo en gran manera a los extorsionadores y tratantes de personas.

La publicación sin control en Facebook les ahorra tiempo a los tratantes, ya que pueden realizar un seguimiento de la persona sin necesidad de hacer mucho esfuerzo, ya que prácticamente les está contando su vida diaria y pueden llegar a contactar a más personas conocidas de la primera víctima, como lo son sus padres, puede obtener sus nombres, dirección o fotos para intentar describir a la víctima lo mejor posible.

En cuanto a compras por Internet hay que revisar que la página sea confiable, de buena reputación y muy importante verificar que el protocolo sea HTTPS. “El protocolo de Transferencia de Hiper-Texto (HTTPS) es la versión segura del http (Hyper Text Transfer Protocol) que todos conocemos y utilizamos habitualmente. La diferencia es que, con HTTP podemos desarrollar actividades ecommerce, ya que permite realizar transacciones de forma segura”.¹⁰⁷

Sirva hasta aquí sobre algunas medidas para poder protegernos sobre algunas actividades en línea para apropiarse de datos e informaciones que pudieran posteriormente utilizarse para cometer actos ilícitos en nuestra contra. En estos temas la información, concientización y la propia conducta respecto al manejo de nuestra información en Internet son fundamentales.

¹⁰⁷ S/a, “¿Qué significa el protocolo HTTPS y cómo funciona?”, *Internet Lab* disponible en línea 29/ de enero de 2010 disponible en línea en <https://www.internetlab.es/post/888/que-significa-el-protocolo-https-y-como-funciona/>, link visitado el 9 de septiembre de 20117.



Capítulo 2

Marco jurídico en materia de suplantación de identidad digital y trata de personas



Capítulo 2: Marco jurídico en materia de suplantación de identidad digital y trata de personas

En este capítulo se abordarán las normas jurídicas que se refieren a la suplantación de la identidad digital en el contexto nacional e internacional.

Se explicarán las distintas normas que hacen frente al fenómeno de suplantación de identidad y robo de datos; se planteará la situación detectada respecto a que en materia de suplantación de identidad, cuando la doctrina y la autoridad la refieren, lo hacen más para el estudio y persecución del uso de redes sociales que se utilizan para realizar delitos financieros y económicos que afectan a las personas en sus patrimonios más que a la posibilidad de que la suplantación de identidad y robo de datos presenta para la trata de personas.

2.1 El fenómeno de la suplantación de identidad

Los ilícitos cometidos a través de medios electrónicos han ido en aumento. “De acuerdo con el Reporte cibercrimen de Norton Symantec, a escala mundial se registraron 378 millones de afectados en el 2013, por algún delito cibernético, es decir, más de un millón de víctimas por día. Esto es, 12 personas por segundo padecen este tipo de ilícitos, entre ellos la usurpación de personalidad”.¹⁰⁸

Infortunadamente este ilícito ha afectado ya a millones de usuarios alrededor del mundo ya que crear perfiles falsos no es complicado como se explicó en el capítulo anterior.

Para crear una cuenta en Facebook no se requiere de mucho esfuerzo. Millones de usuarios ingresan día a día como si fuera pan caliente. Lo alarmante de esta situación es el hecho de que la red social no está previendo, ni velando por el bienestar de los integrantes de Facebook, pues en lugar de implementar parámetros más firmes para la accesibilidad, se está promoviendo

¹⁰⁸ Avilés, Karina, “México, tercer lugar mundial en número de afectados pro cibercriminales, revela estudio”, *La Jornada*, Política, 29 de enero de 2014, disponible en <http://www.jornada.com.mx/2014/01/29/politica/015n1pol>, link visitado el 24 de octubre de 2018.

un caos social que deriva de perfiles falsos, extorsiones, robo de identidad, fraudes, o acosos.¹⁰⁹

Dentro de los países latinoamericanos con mayor índice de robo de identidades se encuentran México y Colombia: “Según El portal Globometer.com clasificó en febrero pasado a los 11 países con mayor número de personas que fueron víctimas de alguna de las variantes de robo de identidad y la lista la encabeza Estados Unidos, seguida de China, Rusia, Corea del Sur, Taiwán, Alemania, Francia, Ucrania, Suecia, Colombia y México”.¹¹⁰

Para evitar ser víctimas de la suplantación de identidad tanto en Facebook como en cualquier otro sitio, hay que fijarnos que naveguemos en páginas seguras SSL y que no descarguemos nada que parezca sospechoso. Existen dos palabras que encierran esta idea, y es, tener sentido común; ya que “Cifras de agencias de seguridad en delitos informáticos revelan que al menos 10 millones de personas al año son víctimas de alguna de las variantes de robo de identidad [tan solo] en Estados Unidos”.¹¹¹

Según el reporte, la escala de afectados es muy alta, por lo que consideramos que se deberían implementar medidas de seguridad, desde la capacitación o entrega de manuales a los usuarios de la red, así como para aquellos usuarios que realicen transacciones en línea.

Según el portal de seguridad de ESET el robo de identidad se ha incrementado a nivel mundial:

¹⁰⁹ Avendaño, Susana, “Una Extraña estadística en Facebook”, *Unocero*, 29 de marzo de 2017, disponible en línea en <https://www.unocero.com/noticias/redes-sociales/una-extrana-estadistica-de-facebook/>, link visitado el 9 de septiembre de 2017.

¹¹⁰ Camarillo Cortés, Mario D., “Robo de identidad, delito al alza y sin estadísticas en el mundo”, *Cronica.com.mx*, 29 de enero de 2014, disponible en línea en <http://www.cronica.com.mx/notas/2015/889903.html>, link consultado el 24 de octubre de 2018.

¹¹¹ *Idem*.

Estadísticas internacionales indican que entre el 2006 y el 2009, la cantidad de casos reportados en Estados Unidos se incrementó de 8.4 a 11.1 millones de personas. Según una infografía sobre el robo de identidad, con datos de CreditRepair.org, el fraude ocasionado por este delito asciende a 54 mil millones de dólares.¹¹² El documento señala que 41 por ciento de los adultos conectados a internet (sic) en el mundo sufrieron ataques como virus, piratería, estafas, fraudes y robo, al no contar con medidas adecuadas de seguridad y por no tener un manejo responsable de sus cuentas en internet (sic).¹¹³

Como se puede observar, prácticamente cualquier usuario de la red puede ser vulnerable a un ataque y robo de identidad, desde los jóvenes, los adultos y hasta los más versados.¹¹⁴ Algunas acciones ilícitas que se realizan para delinquir en la red se encuentran la piratería, los fraudes, el uso ilegítimo de marcas y nombres de dominio, las estafas, el pharming y el phishing. Este último es el principal causante del robo de datos como activos de la información en general. “Los ataques de phishing son aquellos que se valen de la ingeniería social (redes sociales, chats, correo electrónico), con el propósito de sustraer datos personales y credenciales de cuentas bancarias de las personas”,¹¹⁵ como se anotó en el capítulo anterior.

¹¹² Labarca Castro, Raphael, “El robo de identidad y sus cifras en América Latina, *welivesecurity by eset*, 8 de abril de 2011, disponible en línea en <https://www.welivesecurity.com/la-es/2011/04/08/robo-identidad-cifras-america-latina/>, link consultado el 23 de octubre de 2017.

¹¹³ Camarillo Cortés, Mario D., “Robo de identidad, delito al alza y sin estadísticas en el mundo”, *Cronica.com.mx*, *cit*, nota 86.

¹¹⁴ Alcántara, Beatriz, “Adolescente que hackeó a la CIA y al FBI tendrá que pagarlo muy caro”, *Urban Tecno*, Tecnología, 22 de abril de 2018, disponible en <https://urbantecno.com/tecnologia/sentencia-adolescente-hacker-cia-fbi>, consultado el 3 de noviembre de 2018.

¹¹⁵ Nava Garcés, Alberto Enrique, *La prueba electrónica en materia penal. Nuevas tecnologías de la información, redes sociales, telefonía celular, dispositivos*

El *phishing*, es la actividad por medio de la cual los atacantes usan correos apócrifos con la finalidad de llevar a las personas a un dominio parecido al original pero que es un sitio falso creado *ex professo* para que aprovechando el engaño a las víctimas, éstas proporcionen los datos de sus números de cuenta, códigos de seguridad, números de tarjeta de crédito o débito y contraseñas para que una vez obtenidos estos datos se proceda a utilizar los datos financieros para hacer transferencias bancarias o compras en línea por ejemplo.

El medio informativo El Economista público en 2016, que México es el octavo país con mayor robo de identidad y menciona que, “[l]a [entonces] comisionada presidenta del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI), Ximena Puente de la Mora, urgió la consolidación del marco normativo en materia de protección de datos personales, a fin de proteger la privacidad de los ciudadanos. “[...]Al inaugurar la conmemoración del Día Internacional de Protección de Datos Personales, reveló que, de acuerdo con datos de la Condusef, en el primer semestre del 2015 se registró un aumento de 40% del robo de identidad”.¹¹⁶

Los datos de la CONDUSEF para el segundo trimestre de 2018, respecto a los R[obos de] I[dentidad] cibernético disminuyeron 60% respecto del mismo periodo del 2017 y representaron el 3.6% de los Robos de Identidad.

	2013	2014	2015	2016	2017	2018	VAR. (2018 VS 2017)
Totales	29,881	38,460	50,911	32,719	39,775	33,136	
Cibernéticos	369	1,163	982	768	2,960	1,180	60%
	2.3%	3.2%	1.9%	2.4%	7.5%	3.6%	-
Tradicionales	28,642	35,443	49,811	31,786	36,395	31,956	-12%
	98.7%	96.8%	98.1%	97.6%	92.5%	96.4%	-

electrónicos, geolocalización, cadena de custodia, prueba ilícita, casos, México, Porrúa, 2015, p. 59.

¹¹⁶ Hernández, Leopoldo, “México, octavo país con mayor robo de identidad”, *El Economista*, 29 de enero de 2016, disponible en línea en <https://www.eleconomista.com.mx/politica/Mexico-octavo-pais-con-mayor-robo-de-identidad-20160129-0091.html>, link consultado 3 de marzo de 2018.

Por definir	870	1,854	118	165	420	-	-
-------------	-----	-------	-----	-----	-----	---	---

Tabla tomada de la página de la CONDUSEF.¹¹⁷

México también se ve afectado al no denunciar estos actos a las dependencias ya que no conocen donde se debe presentar una denuncia. En nuestra opinión hace falta la cultura de la denuncia para que las dependencias puedan hacer un mejor trabajo es necesario que se les informe de los sucesos.

En lo que respecta a la suplantación de identidad con fines de trata la Asociación Mexicana de Internet (AMIPCI), en México señala que hay más de 40 millones de usuarios de redes sociales, de los cuales, dos de cada tres personas tienen entre 12 y 34 años de edad.¹¹⁸

Coincidentemente los más jóvenes, en el Estado de México, son el sector en donde las autoridades locales han identificado más víctimas de trata de personas, convencidas por el enamoramiento a través del contacto en redes sociales como Facebook y Twitter.¹¹⁹

Actualmente los métodos que utilizan los traficantes de personas son más discretos, puesto que ya existe un poco más de divulgación de estos métodos que usan, pero aun así con un solo like podemos abrir las puertas y ser víctima de estos traficantes.

Principalmente esto se da mediante el contacto a adolescentes en Facebook vía perfiles falsos, estos son la forma más fácil de llevar a cabo sus actividades maliciosas, como por ejemplo tienen un nivel de anonimato un poco alto y es muy fácil crear un perfil como ya lo hemos explicado, en ocasiones las medidas de seguridad se quedan un poco cortas en los registros de algunas redes sociales,

¹¹⁷ CONDUSEF, “Robos de identidad”, disponible en <https://www.condusef.gob.mx/gbmx/?p=estadisticas>, consultado el 4 de noviembre de 2018.

¹¹⁸ Fuentes, Mario Luis, “Trata de personas: jóvenes en riesgo”, *Excélsior en línea*, disponible en línea en <http://www.excelsior.com.mx/nacional/2013/09/24/920068>, link consultado el 16 de mayo de 2017.

¹¹⁹ *Idem*.

solo se debe ingresar un correo electrónico, verificar edad por medio de una pregunta y proporcionar un nombre no necesariamente real.

La suplantación de la identidad se define como “[...] aquella acción por la que una persona se hace pasar por otra para llevar a cabo actividades de carácter ilegal, como pueden ser pedir un crédito o préstamo hipotecario, contratar nuevas líneas telefónicas o realizar ataques contra terceras personas”, como ya avanzábamos en el capítulo anterior.¹²⁰

Este tipo de actividad “se perfecciona con la realización de la actividad usurpadora y cesa cuando concluye la implantación. La conducta del agente exige una cierta permanencia y es ínsito al propósito de usurpación plena de la personalidad global del afectado”.¹²¹

El tema de usurpación ha cobrado tal relevancia que inclusive el Tribunal Superior de la Provincia de Cadiz, en España retomó el tema de la personalidad digital usurpada de una persona al fallecer: “la Sentencia de 15 de mayo de 2009 que en el caso particular se juzgaba la usurpación de identidad de una persona fallecida considerando la Sala que el delito se comete tanto si se sustituye a una persona viva, como fallecida”. En tal sentido se dice que “[...] la acción consiste en simular una identidad o una filiación distinta de la que corresponde al sujeto, pero, la persona sustituida ha de ser real, siendo indiferente que haya o no fallecido”,¹²² situación que al no ser tema de esta propuesta solo sirva como mención.

¹²⁰ Legálitas, “Suplantación de Identidad”, 3 de marzo de 2016, disponible en línea en <https://www.legalitas.com/actualidad/suplantacion-de-identidad>, link visitado el 9 de septiembre de 2017.

¹²¹ Legálitas, “La usurpación de identidad”, 1 de julio de 2015, disponible en línea en <https://www.legalitas.com/pymes-autonomos/actualidad/articulos-juridicos/contenidos/La-usurpacion-de-identidad>, link visitado el 25 de octubre de 2018.

¹²² *Idem*.

2.2 Normatividad nacional e internacional en materia de suplantación de identidad

Dentro de las normas mexicanas no se encuentra aún tipificado el delito de suplantación de identidad digital. Sin embargo, poco a poco se ha avanzado en materia de protección de datos¹²³ y el derecho a la privacidad¹²⁴ aunque es de reconocerse que aún falta trabajo legislativo al respecto.

Como se anotaba ya en el capítulo anterior, no existe uniformidad a nivel internacional sobre la manera en que los países regulan la privacidad o la protección de datos. Han existido algunos intentos por incorporar a los tipos penales, ya existentes, alguna referencia para que aplique el contexto digital pero a la fecha no se ha conseguido concretar unificar las conductas ilícitas en el ciberespacio. Algunos temas pendientes que son señalados por la Coordinación de Seguridad de la UNAM, de la Dirección General de Tecnologías de la Información y Comunicación son que:

En el Código Penal Federal, seis artículos (del 386 al 389 bis) contemplan el delito de fraude, previendo penas y multas de acuerdo con el monto y valor de lo defraudado; sin embargo, ninguno de dichos artículos contempla el fraude cometido a través del uso de medios electrónicos o de Internet.

Desde el año 2000, se han desarrollado en la Cámara de Diputados algunos esfuerzos e iniciativas para reformar el Código Penal Federal y su legislación, con el objeto de prever y castigar algunos delitos informáticos y financieros que se cometen a través de Internet. Desafortunadamente ninguna de las iniciativas

¹²³ Véase la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, en que se contempla el tratamiento indebido de los datos personales en posesión de particulares y se advierte la obligación de hacer del conocimiento del dueño de los datos sobre el uso que se hará de los mismos a través de un aviso de privacidad.

También véase la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

¹²⁴ Reconocido en el artículo 16 Constitucional.

presentadas ha fructificado debido a la poca información que manejan los legisladores acerca de estos temas.

El Instituto Federal de Acceso a la Información y Protección de Datos (IFAI) está facultado para imponer infracciones y sanciones a quienes hagan mal uso de los datos personales. Aquellas entidades que manejan datos personales deberán prever medidas de seguridad y establecer mecanismos para que los usuarios puedan Acceder, Rectificar, Cancelar u Oponerse al manejo de su información personal.

La [...] Ley Federal de Protección de Datos Personales protege la información personal que pueda encontrarse en las bases de datos de cualquier persona física, o empresa como, aseguradoras, bancos, tiendas departamentales, telefónicas, hospitales, laboratorios, universidades, etc. Esta ley regula la forma y condiciones en que las empresas deben utilizar los datos personales de sus clientes.¹²⁵

Algunos proyectos legislativos para regular los ilícitos cometidos por medios digitales se pueden vislumbrar desde el año 2009 con la LXI Legislatura: “a) Iniciativa con Proyecto de Decreto que reforma el artículo 387 del Código Penal Federal, relativa al robo de identidad con fines defraudatorios, presentada el 3 de diciembre de 2009 [...]; b) Iniciativa de Proyecto de Decreto que reforma y adiciona diversas disposiciones de los Códigos Penal Federal y Federal de Procedimientos Penales en materia de robo de identidad, presentada el 17 de marzo de 2011 [...]”.¹²⁶

¹²⁵ UNAM-CERT, “Robo de Identidad y Consecuencias Sociales”, 25 de octubre de 2010, disponible en línea en <https://www.cert.org.mx/historico/documento/index.html-id=16> link visitado el 9 de septiembre de 2017.

¹²⁶ Zamora Jiménez, Arturo, “Por un marco legal para los delitos contra la identidad de las personas en México”, *Revista del Instituto Belisario Domínguez*, vol. 6, núm. 28, 2016, pp. 129-130, disponible en <http://revista.ibd.senado.gob.mx/index.php/PluralidadyConsenso/article/view/332/338>, consultado el 4 de noviembre de 2018.

La Legislatura LXII del Congreso de la Unión en funciones de 2012 a 2015 también presentó una serie de iniciativas al respecto:

a) Iniciativa con Proyecto de Decreto que adiciona el Capítulo III al Título decimoctavo (sic) y el artículo 287 Bis al Código Penal Federal, para adicionar el tipo penal de *robo de identidad*, [...]; b) Iniciativa con Proyecto de Decreto que adiciona el artículo 287 Bis del (sic) Código Penal Federal, para tipificar el delito de *suplantación de identidad*, [...]; c) Iniciativa con Proyecto de Decreto que adiciona un capítulo III- *Robo de identidad*- al título décimo octavo y el artículo 287 Bis al Código Penal Federal [...].¹²⁷

Finalmente la recién concluida Legislatura LXIII, apenas en agosto del año en curso también presentó algunas iniciativas como las siguientes:

a) Iniciativa con Proyecto de Decreto que adiciona el capítulo VII al título vigésimo segundo del libro segundo y el artículo 399 Ter al Código Penal Federal, presentada el 15 de diciembre, [...]; b) Iniciativa con Proyecto de Decreto que adiciona el Capítulo III intitulado “Suplantación de Identidad”, al Título Décimo Octavo del artículo 287 al Código Penal Federal, [...]; c) Iniciativa con Proyecto de Decreto que reforma y adiciona diversas disposiciones del Código Federal, en materia de usurpación o robo de identidad [...]; d) Iniciativa con Proyecto de Decreto por la que se reforman y adicionan diversas disposiciones del Código Penal Federal, la Ley del Sistema de Pagos, la Ley del Banco de México y de la Ley de Instituciones de Crédito [...]; f) Iniciativa con Proyecto de Decreto por el que se crea el capítulo III denominado “Usurpación de Identidad” en el Título Decimonoveno denominado “Delitos contra la Paz y Seguridad de las Personas” del Código Penal Federal y se adiciona el artículo 287 BIS para tipificar a nivel nacional el delito de usurpación de identidad, [...].¹²⁸

Una de las iniciativas que nos gustaría resaltar es la del 29 de noviembre de 2016 por la que la Cámara de Diputados de manera expresa hace referencia a los delitos contra la identidad de las personas identificándolo como usurpación:

¹²⁷ *Ibidem*, p. 130. El énfasis fue añadido.

¹²⁸ *Ibidem*, pp. 130-131.

La Cámara de Diputados aprobó, con 414 votos a favor, el dictamen que adiciona un artículo 430 al Código Penal Federal, para sancionar la usurpación de identidad con una pena de uno a seis años de prisión y 400 a 600 días de multa y, en su caso, la reparación del daño que se hubiere causado.

El dictamen, enviado al Senado de la República para sus efectos constitucionales, destaca que comete el delito de usurpación de identidad quien por sí o por interpósita persona, usando cualquier medio lícito o ilícito, se apodere, apropie, transfiera, utilice o disponga de datos personales sin autorización de su titular o, bien, suplante la identidad de una persona, con la finalidad de cometer un ilícito o favorecer su comisión.

Las penas aumentarán hasta en una mitad cuando el ilícito sea cometido por un servidor público que, aprovechándose de sus funciones, tenga acceso a bases de datos que contengan este tipo de información, así como a los particulares responsables del tratamiento de datos personales sensibles, en términos de la ley en la materia.

Al fundamentar el dictamen que adiciona el Título Vigésimo Séptimo “Delitos contra la identidad de las personas. Capítulo Único. Usurpación de identidad”, el presidente de la Comisión de Justicia, diputado Álvaro Ibarra Hinojosa (PRI), señaló que la identidad es un derecho humano y, de acuerdo con el Fondo de las Naciones Unidas para la Infancia, esta garantía consiste en el reconocimiento jurídico y social de una persona como sujeto de derechos y responsabilidades.

En México, dijo, la usurpación de identidad va en aumento. Según datos del Banco de México, el país ocupa el octavo lugar a nivel mundial en la comisión de este delito. “Hoy hacemos eco a las demandas ciudadanas que existen y exigen una protección más eficaz a sus derechos de identidad”.¹²⁹

¹²⁹ *Boletín núm. 2661*, “Delito de usurpación de identidad será castigado con uno a seis años de prisión”, 29 de noviembre de 2016, Cámara de Diputados del H. Congreso de la Unión, disponible en línea en <http://www5.diputados.gob.mx/index.php/esl/Comunicacion/Boletines/2016/Noviembre/29/2661-Delito-de-usurpacion-de-identidad-sera-castigado-con-uno-a-seis-anos-de-prision>, link visitado el 23 de octubre de 2018.

Lamentablemente aún podemos ver que no existe un consenso ni si quiera de cómo debe de ser referida la actividad ilícita de apropiarse de la identidad de otro, en algunas ocasiones se refiere como robo de identidad, usurpación de identidad, suplantación de identidad e incluso se refiere a ella como falsificación de identidad.

2.2.1 Ley FinTech¹³⁰

Una ley que ha considerado el tema de suplantación de identidad es, “[I]a nueva Ley para Regular las Instituciones de Tecnología Financiera, también conocida como “Ley FinTech”, pone a México a la vanguardia a nivel internacional en el desarrollo de servicios financieros con la finalidad de incrementar el nivel de inclusión financiera y mejorar las condiciones de competencia en el sistema financiero mexicano”.¹³¹

Es la primera vez que existe el término en una ley en México donde se mencione suplantación de identidad:

Artículo 131.- Se sancionará con prisión de tres a nueve años y multa de 5,000 a 150,000 UMA, a quien valiéndose de cualquier medio físico, documental, electrónico, óptico, magnético, sonoro, audiovisual, informático o de cualquier otra clase de tecnología, suplante la identidad, representación o personalidad de cualquiera de las Autoridades Financieras o de alguna de sus unidades administrativas o áreas o de un servidor público, de las ITF o sociedades autorizadas para operar con Modelos Novedosos o de alguno de sus

¹³⁰ Iniciativa de la Ley FinTech, disponible en línea en http://www.senado.gob.mx/sgsp/gaceta/63/3/2017-10-12-1/assets/documentos/Iniciativa_Ejecutivo_Federal.pdf, link consultado el 11 de octubre de 2017.

¹³¹ Comunicado 017 de la Secretaría de Hacienda y Crédito Público, del 1º de marzo 2018, “El Congreso de la Unión aprueba la “Ley FinTech”, disponible en línea en https://www.gob.mx/cms/uploads/attachment/file/304841/Comunicado_SHCP_Ley_Fintech_1_de_marzo_2018.pdf, link consultado el 2 de marzo de 2018.

directivos, consejeros, empleados, funcionarios, dependientes o representantes legales.¹³²

2.2.2 Legislación respecto a los delitos informáticos en materia penal

Los delitos informáticos se entiende que son aquellas conductas consideradas como ilícitas de conformidad con las leyes en materia penal que se cometen en contra o con la ayuda de sistemas informáticos.¹³³

Dentro de esta composición de ordenamientos, son pocos los estados que consideran a los cibercrimes dentro de su catálogo penal, menos los que hacen una división de tal categoría, e incluso, existen algunos estados en los que ni siquiera se ha considerado que la computación pueda ser el medio comisivo en la realización de este tipo de ilícitos.¹³⁴ En México el primer estado de la República en legislar sobre los delitos informáticos fue Sinaloa en el año 1992:

¹³² Artículo 131.- Se sancionará con prisión de tres a nueve años y multa de 5,000 a 150,000 UMA, a quien utilice, realice u obtenga, por sí o a través de interpósita persona, cualquier servicio, Operación o producto proporcionado por alguna de las ITF o sociedad o Entidad Financiera u otro sujeto supervisado por alguna Comisión Supervisora o por el Banco de México, autorizado para operar con Modelos Novedosos previstas en esta Ley bajo una identidad falsa o suplantada.

¹³³ Véase Calderón Martínez, Alfredo, "Delito informático: reto para los sistemas penales del mundo", Nava, Garcés, Alberto Enrique, La prueba electrónica..., *op. cit.*, nota 115, p. 3.

¹³⁴ Los estados que tratan los delitos informáticos en su Código penal son Aguascalientes, Baja California, Chiapas, Colima, Distrito Federal, Morelos, Oaxaca, Puebla, Sinaloa, Querétaro, Tabasco, Tamaulipas, Zacatecas y en el federal. Y los cuales donde no se hace referencia alguna a los mismos en sus códigos estatales son; Baja California Sur, Campeche, Chihuahua, Coahuila, Durango, Estado de México, Guanajuato, Guerrero, Hidalgo, Jalisco, Michoacán, Nayarit, Nuevo León, Quintana Roo, San Luis Potosí, Sonora, Tlaxcala, Veracruz Llave, Yucatán.

donde se estableció en el Código Penal artículo 217 que: “Intercepte, interfiera, reciba, use, altere, dañe o destruya un soporte lógico o comete delito informático, la persona que dolosamente y sin derecho: I. Use o entre a una base de datos, sistemas de computadores o red de computadoras o a cualquier parte de la misma, con el propósito de diseñar; ejecutar o alterar un esquema o artificio con el fin de defraudar; obtener dinero, bienes o información; o programa de computadora o los datos contenidos en la misma, en la base, sistema o red”.

[...]

Ya en 1999, se incorpora al Código Penal Federal un capítulo denominado “Acceso ilícito a sistemas y equipos de informática”, en el cual se agregan una serie de artículos –del 211 bis 1 al 211 bis 7- que tratan sobre el delito de sabotaje informático, consistente en la modificación, destrucción o provocación de pérdida, o la copia o acceso ilegítimo, “sin autorización, de información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad. [...].

Otro de los ordenamientos importantes donde se protegen ciertos bienes jurídicos frente a la informática es la Ley Federal contra la Delincuencia Organizada (LFDO), en la cual se establece la existencia de una unidad especializada de la Procuraduría General de la República para la investigación y persecución de delitos que se organizan a través de la red.

Consecuentemente, [...] se ha creado la “Coordinación Interinstitucional de combate a Delitos Cibernéticos” institución que se encarga de controlar el uso y contenidos ilícitos en Internet, y la organización de delitos en la red, todo a

Cita del original en Ferrada Bubniak, Nicole Eden e Iniescar Medina, Fernanda Jesús, “Usurpación de identidad en las redes sociales: Facebook y Twitter. Tratamiento legal y jurisprudencia en Chile”, Memoria para optar por el grado de licenciado en Ciencias Jurídicas y Sociales, Facultad de Derecho, Departament de Derecho Procesal, Universidad de Chile, 2015, p. 211, disponible en línea en <http://repositorio.uchile.cl/bitstream/handle/2250/135613/Usurpaci%C3%B3n-de-identidad-en-las-redes-sociales.pdf?sequence=1&isAllowed=y>, link consultado el 25 de octubre de 2018.

través del monitoreo de una Base de Datos Nacional en la que se observarán patrones, preferencias y modus operandi de las causas reportadas.¹³⁵

Esta Coordinación Interinstitucional de combate a Delitos Cibernéticos, está formada por; la Presidencia de la República, la Procuraduría General de la República, la Procuraduría General de Justicia del Distrito Federal, la Policía Penal Preventiva, el Centro de Investigación y Seguridad Nacional, la Secretaría de la Defensa Nacional, la Secretaría de Marina, la Secretaría de Seguridad Pública, entre otros.

Vistas las medidas legales e institucionales tomadas por México para contrarrestar la comisión de delitos que se auxilien de las nuevas tecnologías, debemos comentar que sería necesario el despliegue de una política común respecto a los ciberdelitos, ya que el caos que se genera con la variedad de leyes que permite el régimen federal y la falta de uniformidad en el tratamiento de los e-crimes a nivel local permite que en la actualidad se aprovechen estas lagunas legislativas para incrementar la impunidad en el contexto de la delincuencia informática.¹³⁶

Las normas penales debido a la incidencia de las tecnologías han tenido que considerar a las mismas en sus textos. En el Código Penal Federal en su capítulo 2, artículo 202, señala que comete delito de pornografía infantil a personas menores de dieciocho años de edad,¹³⁷ esta ley es de relevancia a gran cantidad de adolescentes y jóvenes que hoy están siendo expuestos en diferentes plataformas ya sea por suplantación de identidad o uso indebido de imágenes, sin embargo no tiene claro el uso en medios digitales o que sean tratados con sistemas informáticos y mucho menos la suplantación de la identidad digital, solo existe muy ambiguamente la usurpación de funciones o profesiones y nos especifica que sea o no a través de los medios digitales.

¹³⁵ *Idem.*

¹³⁶ *Ibidem*, pp. 210-214.

¹³⁷ Código Penal Federal, disponible en línea en <http://www.delitosinformaticos.mx/codigos-penales/codigo-penal-federal/>, link consultado el 1 de diciembre de 2017.

De las diversas reformas propuestas al Código Penal Federal en materia de delitos informáticos, propuesta por el Decreto que reforma y adiciona diversas disposiciones al Código Penal Federal, en materia de delitos en contra de medios o sistemas informáticos, en marzo del año 2012, se puede resaltar aquella que agrava hasta con el doble las sanciones relacionadas con pornografía infantil, en el caso de que la persona se “valga del uso o empleo de medios informáticos para generar relación de confianza o amistad con la víctima”.¹³⁸

Por otra parte Peña Libien en su artículo sobre los Delitos informáticos previstos y sancionados en el Ordenamiento Jurídico Mexicano, señala que:

Los Códigos Penales de las Entidades Federativas también han hecho lo propio por ejemplo en el artículo 336 del Nuevo Código Penal del Distrito Federal, relativo a la Producción, Impresión, Enajenación, Distribución, Alteración o Falsificación de Títulos al Portador, Documentos de Crédito Públicos o Vales de Canje, dispone que se impondrán de tres a nueve años de prisión y de cien a cinco mil días multa al que, sin consentimiento de quien esté facultado para ello, altere los medios de identificación electrónica de tarjetas, títulos o documentos para el pago de bienes y servicios (fracción IV); acceda a los equipos electromagnéticos de las instituciones emisoras de tarjetas, títulos o documentos para el pago de bienes y servicios o para disposición de efectivo (fracción V); adquiera, utilice o posea equipos electromagnéticos o electrónicos para sustraer la información contenida en la cinta o banda magnética de tarjetas, títulos o documentos, para el pago de bienes o servicios o para disposición de efectivo, así como a quien posea o utilice la información sustraída, de esta forma (fracción VI); y a quien utilice indebidamente información confidencial o reservada de la institución o persona que legalmente esté facultada para emitir tarjetas, títulos o documentos utilizados para el pago de bienes y servicios, o de los titulares de dichos instrumentos o documentos. (Fracción VII), de igual forma solo

¹³⁸ Dictámenes aprobados en la LXI legislatura relativos a leyes o decretos, disponible en línea en http://sitl.diputados.gob.mx/LXI_leg/dictameneslxi_ld.php?tipot=&pert=0&init=3208, link consultado el 12 de mayo de 2017.

existe usurpación de funciones o profesiones pero no de suplantación de identidad y mucho menos de identidad digital.

Por otra parte, en el Código Penal Federal se encuentran previstos entre otros, los delitos de Revelación de Secretos, Acceso ilícito a equipos y sistemas de informática y los Delitos contra los Derechos de Autor.

En este tenor, el delito de revelación de secretos se tipifica cuando en perjuicio de alguien, sin justa causa y sin consentimiento, se revele, divulgue o utilice algún secreto, comunicación, información o imágenes, que hayan sido conocidas o recibidas con motivo de un empleo, cargo o puesto, por la prestación de un servicio profesional o técnico, por ser funcionario o empleado público; cuando dicho secreto sea de carácter industrial, o bien, se hubiese obtenido de una intervención de comunicación privada.¹³⁹

Como se mencionó con anterioridad en la Ley Federal contra la Delincuencia Organizada (LFDO);¹⁴⁰ se establece la existencia de una unidad especializada de la Procuraduría General de la República para la investigación y persecución de delitos cometidos por miembros de la delincuencia organizada.

Como sabemos la delincuencia organizada en trata de personas es de la más graves y redituables a nivel mundial, dicha unidad especializada, puede intervenir las comunicaciones privadas que se realicen de forma oral, escrita, por signos, señales o mediante el empleo de aparatos eléctricos, electrónicos, mecánicos, alámbricos o inalámbricos, sistemas o equipos informáticos, claro mediante una previa solicitud por escrito a un juez de distrito,¹⁴¹ así como por

¹³⁹ Peña Libien, Hiram Raúl, “Los delitos Informáticos previstos y sancinados en el Ordenamiento Jurídico Mexicano” en Memorias del Segundo Congreso Nacional de Cultura y Legalidad Informática Jurídica, México, SEGOB, 2012, pp. 9- 14. Varias citas del original fueron omitidas.

¹⁴⁰ Publicada en el Diario Oficial de la Federación de 7 de noviembre de 1996, y reformada por última ocasión el 21 de diciembre de 2004.

¹⁴¹ Artículo 18 de la Ley Federal contra la Delincuencia Organizada, Publicada en el Diario Oficial de la Federación el 7 de noviembre de 1996, última reforma del 7 de abril de 2017.

cualquier otro medio sin embargo a la fecha no se tiene información sobre alguna organización con fines trata en redes sociales.

La Ley de Seguridad Nacional (LSN),¹⁴² establece que las acciones que se establezcan de manera inmediata y directa, dirigidas a mantener la integridad, estabilidad y permanencia del Estado Mexicano, se rigen por los principios de legalidad, responsabilidad, respeto a los derechos fundamentales de protección a la persona humana y garantías individuales y sociales, confidencialidad, lealtad, transparencia, eficiencia, coordinación y cooperación.

El Estado mexicano para determinar o prevenir una amenaza a la Seguridad Nacional, primero se evalúa por el Consejo Nacional de Seguridad Nacional o del Centro de Investigación y Seguridad Nacional, este una vez que tenga clara la amenaza debe guardar secreto y confidencialidad respecto a la información que conozcan o tengan acceso en o con motivo de su función.¹⁴³ La idea es que se

¹⁴² Publicada en el Diario Oficial de la Federación de 31 de enero de 2005.

¹⁴³ Respecto al carácter confidencial de determinada información en relación con la seguridad nacional, ha sostenido el Pleno de la Suprema Corte de Justicia de la Nación, mediante tesis aislada, que: El derecho a la información consagrado en la última parte del artículo 6o. de la Constitución Federal no es absoluto, sino que, como toda garantía, se halla sujeto a limitaciones o excepciones que se sustentan, fundamentalmente, en la protección de la seguridad nacional y en el respeto tanto a los intereses de la sociedad como a los derechos de los gobernados, limitaciones que, incluso, han dado origen a la figura jurídica del secreto de información que se conoce en la doctrina como "reserva de información" o "secreto burocrático". En estas condiciones, al encontrarse obligado el Estado, como sujeto pasivo de la citada garantía, a velar por dichos intereses, con apego a las normas constitucionales y legales, el mencionado derecho no puede ser garantizado indiscriminadamente, sino que el respeto a su ejercicio encuentra excepciones que lo regulan y a su vez lo garantizan, en atención a la materia a que se refiera; así, en cuanto a la seguridad nacional, se tienen normas que, por un lado, restringen el acceso a la información en esta materia, en razón de que su conocimiento público

pretende sancionar la revelación de información contenida en equipos informáticos, obtenida a través de mecanismos distintos a la intervención de comunicación privada, mediante el empleo de aparatos o dispositivos electrónicos o través de la suplantación de identidad. Es interesante el caso en el que un particular solicitó información a la Procuraduría General de Justicia para conocer el número de denuncias que se han presentado sobre robo de identidad a través de redes sociales, la respuesta de las autoridades no fue la más adecuada como se deja expuesto a continuación:

Lo anterior fue dado a conocer en respuesta a una solicitud de información abordada por el pleno del Instituto de Acceso a la Información Pública y Protección de Datos Personales del Distrito Federal (INFODF).

De acuerdo con un comunicado del organismo, un particular requirió a las autoridades judiciales datos sobre denuncias presentadas por el delito de robo, usurpación y uso ilegal de datos personales.

En su solicitud, el particular pidió conocer de la PGJ [...], **cuántas denuncias han versado sobre el robo de identidad a través de redes sociales**; cuántas han sido interpuestas en razón del robo de identidad tratándose de mecanismos de pago electrónicos (tarjetas de crédito, debito, o cualquier instrumento de pago electrónico), y en cuántas averiguaciones previas y/o carpetas de investigación se ha decretado el archivo de las mismas y cuál ha sido el motivo en cada una de ellas. (Énfasis añadido).

[...]

puede generar daños a los intereses nacionales y, por el otro, sancionan la inobservancia de esa reserva; por lo que hace al interés social, se cuenta con normas que tienden a proteger la averiguación de los delitos, la salud y la moral públicas, mientras que por lo que respecta a la protección de la persona existen normas que protegen el derecho a la vida o a la privacidad de los gobernados. Semanario Judicial de la Federación y su Gaceta, Novena Época, t. XI, abril de 2000, Tesis P. LX/2000, página 74, bajo el Rubro: Derecho a la información. Su ejercicio se encuentra limitado tanto por los intereses nacionales y de la sociedad, como por los derechos de terceros.

En respuesta, las autoridades de la PGJ explicaron al particular que, de conformidad con las atribuciones y datos de la Dirección de Política y Prospectiva Criminal, sí contaban con información sobre ese delito, pero no al nivel de desagregación que era requerido.¹⁴⁴

Casos como este dejan al descubierto la poca o nula preparación que se tiene en las autoridades para si quiera poder responder a una solicitud de acceso de información aun cuando se esté en la posibilidad de tener los datos a su disposición. Esta situación por supuesto obstaculiza y oscurece la realidad que sucede en nuestro país con respecto a las cifras y los estudios en materia de suplantación de identidad a través de las redes sociales.

2.2.3 Contexto internacional en materia de suplantación de identidad

En el contexto internacional existen varias acciones que se han implementado para paliar la suplantación de identidad algunas de estas se mencionan a continuación.

Por parte de las Naciones Unidas, el Consejo Económico y Social, a través de su Oficina contra la Droga y el Delito elaboró un estudio denominado *La Cooperación internacional en la prevención, investigación, persecución y castigo del fraude, el uso indebido y falsificación de la identidad relacionada a los fines delictivos* del año 2007, que siguió a la primera reunión del grupo intergubernamental de expertos de Viena 2005, que preparó el estudio sobre fraude, el uso indebido y la falsificación de identidad. El estudio fue preparado con material provisto por los mismos expertos y por fuentes gubernamentales, incluidas políticas, legislación, investigaciones y todo tipo de materiales relevantes. En estos estudios se concluye que no hay un uso uniforme sobre los términos falsificación de identidad o robo de identidad ya que no era lo mismo que se creara una nueva

¹⁴⁴ La redacción, “La Procuraduría CDMX abrió 3 mil 38 investigaciones por robo de identidad en 51 meses”, *Proceso*, 2 de agosto de 2017, disponible en <https://www.proceso.com.mx/497332/la-procuraduria-cdmx-abrio-3-mil-38-investigaciones-robo-identidad-en-51-meses>, link consultado el 29 de octubre de 2018.

identidad a partir de datos obtenidos de una manera ilícita a suplantar una identidad para realizar un fraude por ejemplo. ¹⁴⁵

También el Informe sobre el 18º periodo de sesiones del Consejo Económico y Social de las Naciones Unidas a través de la Comisión de Prevención del Delito y Justicia Penal de 2009, apunta la relevancia de la Cooperación internacional en materia de prevención, investigación, enjuiciamiento y castigo del fraude económico y los delitos relacionados con la identidad. El Consejo se manifiesta preocupado por las graves amenazas planteadas por el fraude económico y los delitos relacionados con la identidad y por otras actividades ilícitas propiciadas por esas formas de delincuencia así como la explotación de las nuevas tecnologías de la información y comunicaciones por parte de los autores de los delitos de fraude económico y delitos relacionados con la identidad. ¹⁴⁶

El Informe 2010 denominado *La globalización del crimen, una evaluación de amenazas transnacionales de crimen organizado* destaca que “El hurto de identidad afecta a más de 1,5 millones de personas al año lo que supone una pérdida económica estimada en 1.000 millones de dólares de los EE.UU., mientras que la delincuencia informática está poniendo en peligro la seguridad de las naciones: se

¹⁴⁵ Economic and Social Council, Commission on Crime Prevention and Criminal Justice, International cooperation in the prevention, investigation, prosecution and punishment of fraud, the criminal misuse and falsification of identity and related crimes [Draft 1 short Version], disponible en https://www.unodc.org/pdf/crime/15_commission/study-on-fraud-and-the-criminal-misuse-and-falsification-of-identity-first-draft.pdf, consultado el 4 de noviembre de 2018.

¹⁴⁶ Sobre los delitos que se relacionan con el robo de identidad. Disponible en https://digitallibrary.un.org/record/663002/files/E_2009_30_E_CN.15_2009_20-ES.pdf, link consultado el 4 de noviembre de 2018.

ha burlado la seguridad de redes eléctricas, tráfico aéreo e instalaciones nucleares”.¹⁴⁷

Igual de relevante es el *Manual sobre los delitos relacionados con la identidad*, del año 2013 que señala los “enfoques jurídicos para tificar el delito de hurto de identidad, la tipología y criterios de la tipificación del delito de identidad, cuestiones relativas a las víctimas de los delitos relacionados con la identidad, inventario de mejores prácticas para evitar el hurto de identidad en los sectores público y privado para prevenir el fraude económico y la delincuencia relacionada con la identidad”.¹⁴⁸ Este Manual refiere medidas preventivas del “hurto” de identidad,¹⁴⁹ la aplicación

¹⁴⁷ Oficina de Enlace del Partenariado en Brasil, “Informe de la UNODC: “La delincuencia organizada se ha globalizado convirtiéndose en una amenaza para la seguridad”, disponible en línea en: <https://www.unodc.org/lpo-brazil/es/frontpage/2010/06/17-crime-organizado-se-globalizou-e-se-transformou-em-uma-ameaca-a-seguranca.html>, última fecha de consulta el 23 de diciembre de 2018.

La versión en inglés de The Globalization of crime, A transnational Organized Crime Threat Assessment se puede consultar en http://www.unodc.org/res/cld/bibliography/the-globalization-of-crime-a-transnational-organized-crime-threat-assessment_html/TOCTA_Report_2010_low_res.pdf, link consultado el 4 de noviembre de 2018.

¹⁴⁸ Naciones Unidas, *Manual sobre los delitos relacionados con la identidad*, Naciones Unidas, Nueva York, 2013, disponible en https://www.unodc.org/documents/organized-crime/13-83700_Ebook.pdf, consultado el 4 de noviembre de 2018.

¹⁴⁹ Como se ha venido señalando a lo largo del trabajo, los conceptos de usurpación, robo, suplantación de la identidad se han usado de manera indistinta, en este trabajo se incluye un concepto más que es el de hurto de identidad pero para efectos de esta investigación se tomará como sinónimo de suplantación para no entrar en materia de definir el concepto al no ser la intención del trabajo.

de medidas de seguridad y gestión de la identidad. También hace referencia a la importancia de la cooperación internacional para hacer frente a estos casos de suplantación de la identidad, sin embargo el Manual tiene un enfoque hacia la utilización de la información obtenida por medios fraudulentos para causar daños al patrimonio de las personas y no vislumbra el tema de la trata de personas como uno de los fines que se utilizan en la suplantación de la identidad.

Otras acciones relevantes son por ejemplo en la:

Organización para la Cooperación y el Desarrollo Económicos (OCDE), destaca, en 2009, la publicación de un estudio sobre el robo de identidad en línea y la emisión de las directrices sobre el robo de identidad en línea que datan de 2008, así como una serie de guías y recomendaciones en materia de fraude transfronterizo, seguridad sobre sistemas de información y redes, protección de la privacidad sobre la circulación de datos personales transfronterizos.

En el ámbito de la Unión Europea, sobresalen ante esta problemática las conclusiones 2009/C 62/05, del Consejo de Europa, relativas a una estrategia de trabajo concentrada y a medidas concretas contra las delincuencia informática, mismas que ponen a corto plazo la creación de instrumentos operativos que permita una mejor descripción de lo que entiende por usurpación de identidad en Internet. En este sentido también destaca el propio Consejo, la Convención sobre Cybercrimen (Budapest 2001, modificada en 2004) y la Directiva 95/46 sobre la Protección de los Individuos con Observación hacia el Procesamiento de Datos Personales.[...]

Por su parte la Cooperación Económica Asia-Pacífico (APEC), en su oportunidad, propuso la integración de un grupo de expertos para analizar el tema denominado “Computers Emergency response Teams CERT’s”.¹⁵⁰

¹⁵⁰ Romero Flores, Rodolfo, “El robo de identidad por medios informáticos o telemáticos: su tratamiento jurídico penal”, *Jurismática, El derecho y las nuevas tecnologías*, disponible en <https://archivos.juridicas.unam.mx/www/bjv/libros/6/2958/20.pdf>, link consultado el 4 de noviembre de 2018.

También es de relevancia mencionar que algunos casos como el del proyecto de Ley en Argentina conocida como la Ley Expediente 4643 D-2010 mejor conocida como la Ley sobre el robo de identidad, por medio de la cual se pretende sancionar a aquella persona que creara, adoptara, se apropiara o hiciera uso a través de Internet de cualquier sistema informático o medio de comunicación con la identidad de una persona sea jurídica o física que no le perteneciera. A esta propuesta de ley se sumaba una agravante cuando quien suplantara una identidad lo hiciera haciéndose pasar como un menor de edad para contactar con menores de dieciséis años.¹⁵¹

En los Estados Unidos existe la *Identity Theft and Assumption Deterrence Act* que prevé como un delito el robo de identidad. “La norma penal detectada en este país se orienta a sancionar a quien transfiera, posea o utilice sin mediar autorización, los datos identificativos de una persona con el objeto de cometer, intentar o favorecer cualquier actividad ilícita”.¹⁵²

2.3 Ejemplos de suplantación de identidad

A continuación, se presentan algunos casos de suplantación en personas morales:

El caso de Burger King: No hace mucho, la cadena de comida rápida Burger King sufrió un caso de usurpación en redes sociales cuando su cuenta oficial de Twitter fue hackeada con el objetivo de confundir a los seguidores de la hamburguesería. La broma consistió en cambiar el logo de Burger King por el de su mayor competidor: McDonald's. Los hackers empezaron a hacer circular tuits polémicos y ácidos que, curiosamente, consiguieron que la cuenta oficial de Burger King incrementase en 30,000 su número de seguidores, pero haciendo peligrar la reputación online de esta empresa. Burger King acabó volviendo a controlar la cuenta en una hora aproximadamente y optó por el sentido del humor para disculparse de lo sucedido.

El caso de Jeep: Muy similar fue el caso de Jeep, que se tuvo que enfrentar también a una usurpación en redes sociales que consistió en la publicación de

¹⁵¹ Romero Flores, Rodolfo, “El robo o usurpación de identidad por medios informáticos o telemáticos: su patrimonio jurídico-penal”, *op. cit.*, nota 137, p. 314.

¹⁵² *Ibidem*, p. 316.

fotografías relacionadas con la marca Cadillac y, lo que es peor, haciendo circular imágenes de gente tomando drogas o pastillas y diciendo que a esto se dedicaban tanto el CEO como los empleados de Jeep. Su cuenta de Twitter fue hackeada, en la cual se aseguró que en Jeep ya no habría más producción y que la empresa se había vendido a Cadillac por el problema falso de su plantilla con los estupefacientes. Jeep no tardó en controlar la situación recuperando la cuenta, restableciendo sus imágenes y borrando los tuits ofensivos, pero no tuvo tanta suerte como Burger King y perdió 2,000 seguidores.¹⁵³

En ambos casos lo que podemos observar es que inclusive las grandes empresas pueden ser víctimas de la suplantación de identidad.

Al tratarse de empresas reconocidas la repercusión en su imagen y en el número de sus seguidores que a su vez representan posibles compradores puede afectar incluso sus ventas, pero cuando la suplantación de identidad se realiza en personas físicas y en especial en menores la afectación puede ser la trata con fines ya no solo de explotación sexual como se anotó anteriormente sino que en ocasiones se hace con la finalidad de extraer órganos o tejidos de las víctimas, situación alarmante sin lugar a dudas por lo que urge la difusión, educación y prevención de este tema.

Iván Portilla, egresado de la carrera de Ciencias de la Comunicación en la UNAM, descubrió que había un perfil de Facebook con sus fotos pero con el nombre de Brayan Martínez, quien se encargaba de contactar a sus contactos. Cuando intentó hacer una denuncia ante la red social se sorprendió de que la respuesta fuera que el autor del perfil falso no se encontraba incurriendo en alguna de las normas comunitarias de la red social.¹⁵⁴

¹⁵³ Cortés García, Rosa “La usurpación en redes sociales: casos reales”, *Inventtatte*, 13 de julio de 2015, disponible en línea <https://inventtatte.com/la-usurpacion-redes-sociales-casos-reales/>. Link visitado el 17 de noviembre de 2017.

¹⁵⁴ Sun, “Mi otro yo en Facebook: usurpación de identidad”, *el Informador.mx*, 18 de junio de 2016, disponible en <https://www.informador.mx/Tecnologia/Mi-otro-yo->

Por su parte ya en España en la comunidad de Elda se ha presentado el caso de una menor a quien le fuera suplantada su identidad a través de una cuenta de Facebook, una de Instagram y otra más de Twitter en cuyas redes de podían ver imágenes de “alto contenido sexual con su cara a modo de montaje”.¹⁵⁵

2.4 Normatividad nacional en materia de trata de personas

La trata de personas es una actividad delictiva por medio de la cual se capta a mujeres y niños para ser trasladados con fines de explotación de algún tipo. “Hoy día, este delito se considera el tercer negocio ilícito más lucrativo del mundo, sólo superado por el tráfico de drogas y armas, y cada año genera ganancias que van de 32,000 a 36,000 millones de dólares, aproximadamente, según estimaciones del Foro de Viena para Combatir la Trata de Personas, organizado por diversas agencias de las Naciones Unidas”.¹⁵⁶

Nuestro país se ha convertido en un lugar de origen, tránsito y destino de este ilícito que daña principalmente a mujeres y niños.¹⁵⁷ Gracias a que en el año 2000 México fue parte de la Convención de Palermo, (referida en la siguiente sección), es que su compromiso de combatir la trata a nivel nacional se ve cristalizada para 2007, fecha en la que se expide la Ley para Prevenir y Sancionar la Trata de Personas.

en-Facebook-usurpacion-de-identidad-20160618-0089.html, última fecha de consulta el 19 de noviembre de 2018.

¹⁵⁵ V. P., “Roban la identidad de una menor en internet y escriben frases ofensivas”, en *Diario Información*, disponible en <https://www.diarioinformacion.com/elda/2017/04/05/roban-identidad-menor-internet-escriben/1880013.html>, link consultado por última ocasión el 19 de noviembre de 2018.

¹⁵⁶ Comisión Nacional de Derechos Humanos, *Diagnóstico sobre la situación de la trata de personas en México*, México, CDNH, 2013, p. 15, disponible en <http://200.33.14.34:1033/archivos/pdfs/diagnosticoTrataPersonas.pdf>, link consultado el 4 de noviembre de 2018.

¹⁵⁷ *Ibidem*, p. 17.

La Ley para Prevenir y Sancionar la Trata de Personas,¹⁵⁸ fue hecha para prevenir y sancionar la trata de personas, desde sus aspectos de persecución, prevención, protección a las víctimas y coordinación institucional. Gracias a esta ley se reforman, adicionan y derogan diversas disposiciones de la Ley Federal contra la Delincuencia Organizada; el Código Federal de Procedimientos Penales y el Código Penal Federal.

A nivel federal 29 entidades federativas promulgaron leyes especiales en materia del delito de trata de personas.¹⁵⁹

El Reglamento de esta Ley se publicó hasta el año 2009 y en esta misma fecha comenzó a funcionar la Comisión Intersecretarial para Prevenir y Sancionar la Trata de Personas. Esta Comisión tuvo su Reglamento hasta 2010. Es hasta el siguiente año, 2011, que el Estado mexicano tiene una política en la materia bajo el nombre de Programa Nacional para Prevenir y Sancionar la Trata de Personas.

En el año “2012 se publicó la Ley General para Prevenir, Sancionar y Erradicar los Delitos en Materia de Trata de Personas y para la Protección y Asistencia a las Víctimas de estos Delitos, que sustituye y abroga la Ley para Prevenir y Sancionar

¹⁵⁸ Ley para Prevenir y Sancionar la Trata de Personas, disponible en línea en https://docs.mexico.justia.com/federales/ley_para_prevenir_y_sancionar_la_trata_de_personas.pdf, link consultado 17 de diciembre de 2017.

¹⁵⁹ Aguascalientes, Baja California, Chiapas, Chihuahua, Ciudad de México, Coahuila, Colima, Durango, Estado de México, Guanajuato, Guerrero, Hidalgo, Jalisco, Michoacán, Nayarit, Nuevo León, Oaxaca, Puebla, Querétaro, Quintana Roo, San Luis Potosí, Sinaloa, Sonora, Tabasco, Tamaulipas, Tlaxcala, Veracruz, Yucatán y Zacatecas.

Véase “Marco Normativo de trata de Personas de la Comisión Nacional de los Derechos Humanos disponible en línea en http://www.cndh.org.mx/Marco_Normativo_Trata, última fecha de consulta el 23 de diciembre de 2018.

la Trata de Personas. El reglamento correspondiente fue publicado en el Diario Oficial de la Federación el 23 de septiembre de 2013”.¹⁶⁰

De la Ley General para Prevenir, Sancionar y Erradicar Delitos en Materia de Trata de Personas y para la Protección y Asistencia a las Víctimas nos interesa resaltar los siguientes artículos:

Artículo 15. Será sancionado con pena de 5 a 15 años de prisión y de un mil a 30 mil días multa, al que se beneficie económicamente de la explotación de una persona mediante el comercio, distribución, exposición, circulación u oferta de libros, revistas, escritos, grabaciones, filmes, fotografías, anuncios impresos, imágenes u objetos, de carácter lascivo o sexual, reales o simulados, sea de manera física o *a través de cualquier medio*. [...].

Artículo 16. Se impondrá pena de 15 a 30 años de prisión y de 2 mil a 60 mil días multa, así como el decomiso de los objetos, instrumentos y productos del delito, incluyendo la destrucción de los materiales resultantes, al que procure, promueva, obligue, publicite, gestione, facilite o induzca, por cualquier medio, a una persona menor de dieciocho años de edad, o que no tenga la capacidad de comprender el significado del hecho, o no tenga capacidad de resistir la conducta, a realizar actos sexuales o de exhibicionismo corporal, con fines sexuales, reales o simulados, con el objeto de producir material a través de video grabarlas, audio grabarlas, fotografiarlas, filmarlos, exhibirlos o describirlos a través de anuncios impresos, *sistemas de cómputo, electrónicos o sucedáneos*, y se beneficie económicamente de la explotación de la persona. Si se hiciere uso de la fuerza, el engaño, la violencia física o psicológica, la coerción, el abuso de poder o de una situación de vulnerabilidad, las adicciones, una posición jerárquica o de confianza, o la concesión o recepción de pagos o beneficios para obtener el consentimiento de una persona que tenga autoridad sobre otra o cualquier otra circunstancia que disminuya o elimine la voluntad de la víctima para resistirse, la pena prevista en el párrafo anterior se aumentará en una mitad. Se impondrán las mismas sanciones previstas en el primer

¹⁶⁰ Comisión Nacional de Derechos Humanos, *Diagnóstico sobre la situación de la trata de personas en México*, *op. cit.*, nota 104, pp. 20 y 21.

párrafo del presente artículo, a quien financie, elabore, reproduzca, almacene, distribuya, comercialice, arriende, exponga, publicite, difunda, adquiera, intercambie o comparta, por cualquier medio, el material a que se refieren las conductas anteriores.

Artículo 17. Se impondrá pena de 5 a 15 años de prisión y de un mil a 20 mil días multa al que almacene, adquiera o arriende para sí o para un tercero, el material a que se refiere el artículo anterior, sin fines de comercialización o distribución

Artículo 104. La Secretaría de Seguridad Pública y autoridades de las entidades federativas y municipales, dentro del ámbito de sus competencias, supervisarán negocios que puedan ser propicios para la comisión del delito previsto en esta Ley, realizando inspecciones en agencias de modelaje o artísticas, salas de masajes, bares, cantinas, hoteles, cines, *servicio de Internet*, baños públicos u otros.

Para autorizar la operación de los negocios que presten *servicio de Internet*, deberán contar con filtros parentales y defensa contra intromisiones no deseadas.¹⁶¹

Finalmente es preciso mencionar que dentro del Programa Nacional para Prevenir y Sancionar la trata de Personas dentro del Capítulo II. Objetivos, Estrategias y líneas de acción en su Objetivo 1. Prevenir el delito de trata de personas, sus modalidades y fomentar la visibilización del fenómeno delictivo, en la estrategia 1.1 Sensibilizar e informar a la población sobre las características y modalidades de la trata de personas en su línea de acción 1.1.1 se señala

¹⁶¹ Ley General para Prevenir, Sancionar y Erradicar los Delitos en Materia de Trata de Personas y para la Protección y Asistencia a la Víctimas de estos Delitos, disponible en

https://www.gob.mx/cms/uploads/attachment/file/310904/LEY_GPSEDM_TRATA_19-01-2018.pdf, link consultado el 4 de noviembre de 2018. El énfasis fue añadido.

textualmente “Desarrollar programas educativos sobre el uso de internet, redes sociales y sus riesgos en materia de trata de personas”.¹⁶²

2.5 Normatividad internacional en materia de trata de personas

Dentro del Programa Nacional para Prevenir, Sancionar y erradicar los Delitos en Materia de Trata de Personas y para la Protección y Asistencia a las Víctimas de estos Delitos 2014-2018 se mencionan los siguientes instrumentos internacionales:

Convención Americana sobre Derechos Humanos.

Protocolo Adicional a la Convención Americana sobre Derechos Humanos en Materia de Derechos Económicos, Sociales y Culturales, "Protocolo de San Salvador".

Protocolo a la Convención Americana sobre Derechos Humanos relativo a la Abolición de la Pena de Muerte.

Retiro Parcial de las Declaraciones Interpretativas y de la Reserva que el Gobierno de México formuló al párrafo 3 del artículo 12 y al párrafo 2 del artículo 23 respectivamente de la Convención Americana sobre Derechos Humanos.

Convención contra la Tortura y otros Tratos o Penas Cruelles, Inhumanos o Degradantes.

Declaración para el Reconocimiento de la Competencia del Comité contra la Tortura, de la Convención contra la Tortura y otros Tratos o Penas Cruelles, Inhumanos o degradantes.

Enmiendas a los artículos 17 párrafo 7 y 18 párrafo 5 de la Convención contra la Tortura y otros Tratos o Penas Cruelles, Inhumanos o Degradantes.

Protocolo Facultativo de la Convención contra la Tortura y otros Tratos o Penas Cruelles, Inhumanos o Degradantes.

¹⁶² Plan Nacional para Prevenir y Sancionar la trata de Personas, 2014-2018, disponible en http://dof.gob.mx/nota_detalle.php?codigo=5343079&fecha=30/04/2014, link consultado el 4 de noviembre de 2018.

Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional.

Protocolo para Prevenir, Reprimir y Sancionar la Trata de Personas, especialmente Mujeres y Niños, que complementa la Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional.

Convención de Naciones Unidas contra la Droga y el Delito.

Convención Interamericana para la Eliminación de todas las formas de Discriminación contra las Personas con Discapacidad.

Convención Interamericana para Prevenir, Sancionar y Erradicar la Violencia Contra la Mujer, "Convención de Belém Do Pará".

Convención Interamericana para Prevenir y Sancionar la Tortura.

Convención Interamericana sobre Asistencia Mutua en Materia Penal.

Convención Interamericana sobre Desaparición Forzada de Personas.

Convención Interamericana sobre Tráfico Internacional de Menores.

Convención Internacional sobre la Eliminación de todas las formas de Discriminación Racial.

Declaración para el Reconocimiento de la Competencia del Comité para la Eliminación de la Discriminación Racial, de la Convención Internacional sobre la Eliminación de Todas las Formas de Discriminación Racial.

Enmiendas al artículo 8 de la Convención Internacional sobre la Eliminación de Todas las Formas de Discriminación Racial.

Convención Internacional sobre la Protección de los Derechos de todos los Trabajadores Migratorios y de sus Familiares.

Convención sobre la Eliminación de todas las Formas de Discriminación contra la Mujer.

Enmienda al párrafo 1 del artículo 20 de la Convención sobre la Eliminación de Todas las Formas de Discriminación contra la Mujer.

Protocolo Facultativo de la Convención sobre la Eliminación de todas las Formas de Discriminación contra la Mujer.

Retiro de la Declaración Interpretativa que el Gobierno de los Estados Unidos Mexicanos formuló al aprobar la Convención sobre la Eliminación de Todas las Formas de Discriminación contra la Mujer.

Convención sobre la Protección de Menores y la Cooperación en Materia de Adopción Internacional.

Convención sobre los Derechos del Niño.

Enmienda al párrafo 2 del artículo 43 de la Convención sobre los Derechos del Niño.

Protocolo Facultativo de la Convención sobre los Derechos del Niño relativo a la Participación de Niños en los Conflictos Armados.

Protocolo Facultativo de la Convención sobre los Derechos del Niño relativo a la Venta de Niños, la Prostitución Infantil y la Utilización de los Niños en la Pornografía.

Retiro de la Declaración Interpretativa formulada por el Gobierno de los Estados Unidos Mexicanos al depositar su instrumento de ratificación Protocolo Facultativo de la Convención sobre los Derechos del Niño relativo a la Participación de Niños en los Conflictos Armados.

Convenio de La Haya relativo a la Competencia, la Ley Aplicable, el Reconocimiento, la Ejecución y la Cooperación en Materia de Responsabilidad Parental y las Medidas de Protección de los Niños.

Convenio de la Organización Internacional del Trabajo, 29, sobre el Trabajo Forzoso.

Convenio OIT 105 sobre la Abolición del Trabajo Forzoso.

Convenio OIT 129 sobre la Prohibición del Trabajo Infantil.

Convenio OIT 169 sobre Pueblos Indígenas y Tribales en Países Independientes.

Convenio OIT 182 sobre la Prohibición de las Peores formas del Trabajo Infantil.

Declaración Americana de los Derechos y Deberes del Hombre.

Declaración Universal de los Derechos Humanos.

Declaración sobre los principios fundamentales de justicia para las víctimas de delitos y del abuso de poder.

Pacto de los Derechos Civiles y Políticos.

Retiro Parcial de la Reserva que el Gobierno de México formuló al artículo 25 Inciso B) del Pacto Internacional de Derechos Civiles y Políticos.

Protocolo Facultativo del Pacto Internacional de Derechos Civiles y Políticos.

Segundo Protocolo Facultativo del Pacto Internacional de Derechos Civiles y Políticos destinado a Abolir la Pena de Muerte.

Pacto de los Derechos Económicos, Sociales y Culturales.

Uno de los instrumentos internacionales de los que México forma parte es la Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional que se conoce comúnmente como la Convención de Palermo que prevé a su vez tres protocolos adicionales 1) Protocolo contra el tráfico ilícito de migrantes por tierra, mar y aire, 2) el Protocolo contra la fabricación y el tráfico ilícito de armas de fuego, sus piezas y componentes y municiones y 3) el Protocolo para prevenir, reprimir y sancionar la trata de personas, especialmente mujeres y niños, que es la que interesa para esta propuesta de intervención debido a que la trata de personas que se realiza a través de los perfiles de Facebook impacta directamente a esta población.

La tecnología digital nos ha cambiado la vida a todos: especialmente a los niños. Uno de cada tres usuarios de internet es menor de edad y, sin embargo, no se hace lo suficiente para protegerlos de los peligros del mundo digital ni para facilitar su acceso a contenidos seguros. Esta es una de las conclusiones del nuevo informe del Fondo de las Naciones Unidas para la Infancia (UNICEF) sobre la infancia y la tecnología digital.¹⁶³

Debido a este tipo de cifras y datos es que urge que se difunda y prevenga sobre los riesgos que se corren al hacer uso de redes sociales sin una adecuada conciencia de los riesgos como es la trata de personas.

El acceso a internet es muy desigual entre los jóvenes del mundo: 346 millones (el 29%) siguen desconectados. África es el continente con el índice más alto de jóvenes sin acceso a la tecnología digital (tres de cada cinco), mientras que en Europa es tan solo uno de cada 25.

La brecha digital ahonda en otras diferencias económicas, lo que desfavorece todavía más a los jóvenes en contextos de pobreza, marginación o conflicto. Estos pierden oportunidades de aprendizaje y acceso a información, tan

¹⁶³ Noticias ONU, “Crecer en el mundo digital: Cómo internet afecta al bienestar y seguridad de los niños”, 11 de diciembre de 2017, disponible en línea en, <https://news.un.org/es/story/2017/12/1423682#.WILaKhP1XfY>, link consultado el 11 de diciembre de 2017.

necesarias para aquellos que viven en comunidades remotas o cuando hay una crisis humanitaria.¹⁶⁴

13º Congreso de las Naciones Unidas sobre Prevención del Delito y Justicia

Penal:

La cooperación internacional se ve facilitada cuando en los marcos jurídicos nacionales se tipifican como delito las mismas conductas sustantivas subyacentes. En el caso de la ciberdelincuencia, se requieren habitualmente disposiciones penales específicas para tipificar como delito conductas dirigidas contra datos o sistemas informáticos, como por ejemplo el delito de acceso ilegal a un sistema o a datos informáticos.¹⁶⁵

Reconocemos que proponer una unificación de legislaciones en materia de los delitos en materia de usurpación de identidad excede a nuestra propuesta de intervención por ello se decidió tener una propuesta más sencilla apostando a la información y difusión del tema de trata de personas por medio de perfiles de Facebook para alertar sobre estas conductas en la Internet.

Finalmente queremos resaltar la Declaración Interamericana para Enfrentar la Trata de Personas publicada en Diario Oficial el 5 de diciembre de 2014 en cuyo texto en el punto 7 menciona como objetivo

Fomentar la implementación sostenida, por parte de los Estados Miembros, de campañas de información, sensibilización u concientización sobre las regulaciones migratorias, las falsas ofertas laborales, el uso de las tecnologías de la información y la comunicación como mecanismos de captación y ofrecimiento así como sobre los riesgos que estos conllevan para los sectores más vulnerables a la trata de personas; e incluso la implementación de mecanismos de denuncia y líneas telefónicas gratuitas orientadas a la

¹⁶⁴ *Idem.*

¹⁶⁵ 13º Congreso de las Naciones Unidas sobre Prevención del Delito y Justicia Penal disponible en línea en, https://www.unodc.org/documents/congress/Documentation/A-CONF.222-12_Workshop3/ACONF222_12_s_V1500666.pdf, link consultado 13 de noviembre de 2017.

prevención y asistencia en un idioma que las víctimas de trata de personas puedan comprender.¹⁶⁶

Es justamente el uso de las tecnologías de la información y la comunicación y en especial la red social de Facebook la que en este modelo de intervención queremos resaltar a fin de que se tomen las medidas necesarias para prevenir la trata de personas por medio de la suplantación de la identidad, una actividad que se ha vuelto cada vez más común entre los delincuentes que buscan enganchar a sus posibles víctimas por este medio.

Si bien se observa que existe un gran número de instrumentos internacionales que pretenden prevenir estos ilícitos la realidad supera por mucho los esfuerzos de la comunidad internacional para erradicarlos.

2.6 Anonimato tecnológico

Una de las características que hacen factible el ilícito del robo de identidad con fines de trata es precisamente el anonimato que tienen los delincuentes.

Para un agresor en línea, puede ser factible mantenerse oculto con cierta facilidad. Mientras lleva a cabo su agresión, puede crear un perfil falso, una cuenta de correo falsa, y los más aventajados, pueden enmascararse tras servidores en Internet que dificulten mucho poder localizarlos. Frecuentemente resulta necesario acudir a las diferentes unidades de Policía Cibernética de los países (en caso de que cuenten con ellas), quienes poseen los conocimientos y recursos tecnológicos para dar con ellos.

Sin embargo como se ha dejado de manifiesto a lo largo del presente capítulo las normas en materia de robo de identidad, suplantación o usurpación de la misma no son uniformes lo que ocasiona que en existan lagunas jurídicas que son

¹⁶⁶ Declaración Interamericana para Enfrentar la Trata de Personas “Declaración de Brasilia”, 5 de diciembre de 2014, p. 3, disponible en http://www.cndh.org.mx/sites/all/doc/Programas/TrataPersonas/MarcoNormativoTrata/InsInternacionales/Regionales/Declaracion_IETP.pdf, link consultado el 4 de noviembre de 2018.

aprovechadas por los delincuentes para realizar sus actividades y salir bien librados.

En el caso de la usurpación con fines de trata hemos manifestado que los delincuentes hacen uso de nombres falsos para poder contactar con las víctimas lo que hace que también sus nombres reales se mantengan secretos y sea difícil saber quién es el perpetrador de estas conductas. Al respecto se pudiera acabar con el anonimato de las personas en el uso de las redes sociales, esto no quiere decir que no se pueda utilizar un alias o un pseudónimo, lo que significa es que siempre se pueda tener la certeza de quién es la persona detrás de la red social y con esto evitar el ciberacoso, la pederastia, las injurias o el acoso. Sin embargo reconocemos que este tipo de acciones no necesariamente evitarían los ilícitos y por el contrario podrían ser medidas que pudieran vulnerar la privacidad e intimidad de las personas.¹⁶⁷

Vale la pena reflexionar sobre la pertinencia de conservar el anonimato en las redes sociales pero exigir a las empresas como Facebook, Instagram o Twitter que mantengan un control más riguroso sobre la creación de perfiles, evitando comportamientos sociales irresponsables y con menos impunidad para que las redes sociales puedan ser ambientes sanos y democráticos y no espacios ideales para la comisión de actos delictivos como ha resultado ser hasta el día de hoy.

2.7 Víctimas de trata contratadas por medios digitales

¹⁶⁷ Véase la nota “El anonimato en las redes sociales podría tener los días contados”, *Diario la voz de Galicia*, 26 de diciembre de 2017, disponible en <https://www.lavozdegalicia.es/noticia/espana/2017/12/26/anonimato-redes-sociales-tener-dias-contados/00031514300273165278820.htm>, última fecha de consulta el 19 de noviembre de 2018.

También véase el Informe del Relator Especial de la Libertad de Expresión, David Kaye, respecto del cifrado, el anonimato y el marco de los derechos humanos, disponible en línea en <https://www.ohchr.org/EN/Issues/FreedomOpinion/Pages/CallForSubmission.aspx>, última fecha de consulta el 23 de diciembre de 2018.

Como hemos investigado en los apartados anteriores la finalidad por la cual alguien es capturada para ser víctima de trata pueden ser que sea sometido a realizar trabajos forzados, explotación sexual, matrimonio forzado y hasta tráfico de órganos, hemos estudiado las formas de enganche de un delincuente cibernético las cuales aprovechan la vulnerabilidad económica, social, cultural y psicológica de la víctima para que caiga más fácilmente en la trampa del tratante por medio de la ingeniería social. Y así facilitar su traslado al lugar donde mantengan privada de su libertad a la persona.

La siguiente es una cita es un testimonio: “Un día me llega un mensaje de texto a mi celular. Solicitándome servicios sexuales. Insultándome, denigrándome horrible’, recodó Olivia, víctima de trata virtual [...] comenzó a recibir mensajes y llamadas de desconocidos que le pedían sexo a cambio de dinero; sus datos personales aparecieron súbitamente en una página donde trabajadores sexuales ofrecen sus servicios”.¹⁶⁸

La captación de víctimas de trata que realizan los delincuentes por medios digitales en ocasiones se debe al desconocimiento que se tiene de los riesgos.

Hace apenas tres meses, Liz desapareció. A través de Facebook, un criminal manipuló a esta niña de 14 años hasta que consiguió convencerla de abandonar a su familia para irse a Puebla a trabajar con él.

La captación de menores en la red con fines sexuales puede llevar unos minutos, horas, días o meses, según los objetivos y necesidades del agresor y las reacciones de los niños, de acuerdo con el Fondo de las Naciones Unidas para la Infancia (Unicef).

¹⁶⁸ Noticieros Televisa, “Víctima de trata virtual comparte su testimonio” noviembre 2018, disponible en línea en <https://noticieros.televisa.com/ultimas-noticias/victima-trata-virtual-comparte-su-testimonio/>, última fecha de consulta el 23 de diciembre de 2018.

Al pederasta que engatusó a Liz, le tomó 45 días obtener su amor, su lealtad y hasta sus más íntimos secretos, mientras todos en casa la creían a salvo.¹⁶⁹

Para así proceder con la explotación en el lugar donde sea que se encuentre la víctima.

2.8 Procedimiento para denunciar la suplantación de identidad digital en México

Una vez que se es víctima de la suplantación digital menester saber que se debe de hacer:

- 1) Si se ha creado un perfil falso de nosotros sin autorización se recomienda conseguir pruebas y cerciorarse si se ha creado solo el perfil o si se están realizando actividades en nuestro nombre.
- 2) Hacer capturas de pantalla del perfil, recopilar pruebas de las conversaciones que se pudiera haber sostenido con el usurpador para poder ofrecerlas como prueba ante las autoridades.
- 3) Es importante contactar con amigos o familiares que el suplantador haya podido contactar para que también puedan aportar pruebas a la investigación.
- 4) Se puede presentar una denuncia en línea ante la Comisión Nacional de Seguridad.
- 5) El portal oficial del gobierno ofrece también información relevante sobre el acoso cibernético.
- 6) También existen números de atención como el 52425100 extensión 5086 de la Policía de Ciberdelincuencia Preventiva de la Ciudad de México.
- 7) También deberá acudirse a presentar una denuncia ante el ministerio público.

¹⁶⁹ “La trata de blancas en los tiempos de internet” en La Crónica de Chihuahua, disponible en línea en <http://www.cronicadechihuahua.com/La-trata-de-blancas-en-los-tiempos.html>, última fecha de consulta el 23 de diciembre de 2018.

- 8) Finalmente también es pertinente denunciar el acto ante la propia red social para que se elimine el perfil falso aunque si bien la mayoría de las redes sociales tienen un procedimiento para la denuncia, no siempre resulta ser efectivo como más adelante se deja ver con un testimonio.

“No se haga ilusiones al presentar denuncias ante este tipo de autoridades pues las unidades de policía cibernética prácticamente se dedican a realizar ‘patrullajes en internet’, orientar al público y apoyar a otras autoridades con las investigaciones informáticas. La única autoridad que le puede ‘ayudar’ con su caso es un ministerio público (local o federal), y a su vez un juez que esté convencido de la probable responsabilidad de un individuo”¹⁷⁰

Resulta bastante desilusionante conocer la realidad sobre la situación de las denuncias de suplantación de identidades ante las autoridades pues como se ha venido anotando a lo largo del trabajo, el tema se relaciona más con temas de daños patrimoniales que sobre los riesgos que hay en materia de trata de personas.

2.9 Elementos para denunciar la trata de personas en México

De acuerdo a datos obtenidos de la Secretaría de Gobernación los elementos para identificar la trata de personas son las conductas, los medios y los fines. “La manera como la víctima es captada, trasladada y acogida en el lugar de destino: los medios, son aquellos procedimientos utilizados para cometer los delitos en materia de trata de personas y los fines son aquellas formas o modalidades de explotación que se tenga la intención de practicar con la víctima”.¹⁷¹

¹⁷⁰ DelitosInformáticos.mx, “¿Cómo denunciar delitos cibernéticos en México?”, disponible en línea en <https://www.delitosinformaticos.mx/que-es-un-delito-informatico/como-denunciar-delitos-ciberneticos-en-mexico/>, última fecha de consulta el 23 de diciembre de 2018.

¹⁷¹ Secretaría de Gobernación, Elementos de la trata de personas, disponible en http://www.gobernacion.gob.mx/es_mx/SEGOB/Elementos_de_la_Trata_de_Personas, link consultado el 4 de noviembre de 2018.

En la presente propuesta de intervención se trata de hacer énfasis en las conductas por las cuales las víctimas son captadas, en este caso por medio del uso de la red social Facebook.

Las diversas conductas que se consideran punibles referentes a la trata de personas se encuentran:

Promover	Para si	Para otro	Violencia física Violencia moral	<ul style="list-style-type: none"> • Explotación sexual • Trabajo o servicio forzado • Esclavitud o prácticas análogas • Servidumbre • Extracción de órganos, tejidos o componentes
Facilitar				
Ofrecer				
Conseguir				
Trasladar				
Entregar				
Recibir				

Tabla elaborada con información tomada de la página de la Secretaría de Gobernación.¹⁷²

A lo largo de este capítulo se ha dejado de manifiesto que aún no existe una uniformidad en el uso de conceptos que se refieran al robo, la suplantación o la usurpación de la identidad en medios digitales. Se ha dejado de manifiesto que en la mayoría de los intentos de normar esta conducta ilícita se hace más referencia hacia el daño que se busca hacer patrimonialmente a las personas cuando se realiza esta conducta delictiva y poco se hace referencia a la usurpación de identidad con fines de trata de personas.

Es en el contexto internacional donde vemos reflejada la intensión de los Estados para hacer frente a esta realidad y el motivo por el cual se presenta esta propuesta de intervención que se aterriza con más detalle en el siguiente capítulo.

¹⁷² *Idem.*



Capítulo 3

Propuestas para evitar la usurpación de identidad y alertar la trata de personas por medio de Facebook



Capítulo 3: Propuestas para evitar la usurpación de identidad y alertar sobre la trata de personas que se realiza haciendo uso de Facebook

En este capítulo presentamos algunas prácticas erróneas de los usuarios de Facebook que son utilizadas por los suplantadores para obtener información de las cuentas de sus posibles víctimas y de este modo poder contactar a las personas con fines de trata.

3.1 Entender qué es y cómo funciona Facebook

Como se adelantaba en el capítulo primero de esta investigación Facebook es una red social que se creó en el 2009 por Mark Zuckerberg, estudiante de la universidad de Harvard. “Su objetivo era un espacio de comunicación para los alumnos de dicha universidad donde pudieran intercambiar contenido de forma sencilla a través de Internet. Su proyecto fue tan innovador que tuvo un gran alcance, hasta el punto de estar disponible para cualquier usuario de la red”.¹⁷³

Algunos de los mejores usos que se le puede dar a están gran red social son el de promover algún trabajo, seguir a personas y marcas interesantes, la promoción de eventos, encontrar contactos útiles o atención a clientes.

Sin embargo, no todo es benéfico en Facebook, las principales críticas se han centrado en la supuesta falta de privacidad que sufren sus millones de usuarios. “Estas críticas se acrecentaron en 2013, cuando se descubrió que la Agencia de Seguridad Nacional de Estados Unidos y otras agencias de inteligencia vigilan los perfiles de millones de usuarios y sus relaciones con amigos y compañeros de trabajo”.¹⁷⁴

¹⁷³ Definición de Facebook, tomada de la página de Definición.de, disponible en línea en <http://definicion.de/facebook/>, link consultado el 4 de mayo de 2017.

¹⁷⁴ Simpson, David y Brown, Pamela, “NSA mines Facebook for connections, including Americans' profiles”, *CNN.com* (en inglés). Disponible en

Los medios de comunicación hacen referencia a instrumentos de contenido por el cual se realiza el proceso de comunicación. Usualmente se utiliza el término para hacer referencia a los medios de comunicación masivos;

‘Facebook es un nuevo tipo de plataforma. No es una empresa de tecnología tradicional. No es una compañía de medios tradicional. Ya saben, construimos tecnología y nos sentimos responsables de cómo se usa. No escribimos las noticias que la gente lee en la plataforma. Pero, al mismo tiempo, también sabemos qué hacemos mucho más que distribuir noticias y que somos una parte importante del discurso público’. Ahora sí, la red social se identifica como compañía tecnológica y como medio de comunicación.¹⁷⁵

Gracias al caso Cambridge Analítica y poner en cuestión si Facebook era culpable o no se tomaron medidas por Mark Zuckerberg para evitará el uso indebido de las herramientas de segmentación en la red social, es por eso que Facebook prohibirá usar herramientas de segmentación hasta no contar previa autorización,¹⁷⁶ recordemos que una de las herramientas que utilizan los suplantadores y los delincuentes de trata de personas son justamente las herramientas de segmentación para tener perfiladas sus víctimas.

Crear correo falso: Para crear un correo falso y después usarlo para crear una cuenta de Facebook falsa o suplantada necesitamos entrar en un sitio, donde podamos crear un correo falso o temporal ya que lo necesitamos para crear la cuenta en Facebook y confirmarla, existen varias herramientas como es “10

http://edition.cnn.com/2013/09/30/us/nsa-social-networks/index.html?hpt=ibu_c2

link consultado el 4 de mayo de 2017.

¹⁷⁵ Martínez, A., “Zuckerberg recula: Facebook sí es un medio de comunicación”, @abc_tecnología, ABC redes, España, disponible en línea en http://www.abc.es/tecnologia/redes/abci-zuckerberg-recula-facebook-si-medio-comunicacion-201612222024_noticia.html, link consultado el 16 de mayo de 2017.

¹⁷⁶ Galeano, Susana “Facebook prohibirá usar Custom Audiences para realizar campañas segmentadas a usuarios que no hayan dado su autorización”, M4rketing Ecommerce, disponible en línea en, <https://marketing4ecommerce.net/facebook-prohibira-usar-custom-audiences/>, link consultado el 12 de mayo de 2017.

Minutos Mail”¹⁷⁷ y “YopMail”¹⁷⁸ pero estas herramientas no sólo fueron creadas para estos fines fue pensado para sitios donde piden un correo y después te envían mucha publicidad o spam (correo electrónico no solicitado que se envía a un gran número de destinatarios con fines publicitarios o comerciales.) Es por eso que, en lugar de colocar un correo real se comenzó a utilizar este tipo de recursos.

Conseguir número telefónico que no te relacione para validaciones: En México existe una gran competencia entre las compañías de telecomunicaciones por el posicionamiento entre los clientes las cuales se disputan los números que le asigna el IFT a cada compañía y es muy común que estas compañías tengan estos datos y que incluso los compartan con terceros.

Grupos de Facebook: A través de los grupos que ofrece Facebook es posible que los delincuentes aprovechen el alcance masivo que tiene esta herramienta, existen grupos dedicados a la educación, deportes, cultura, viajes entre otros más, pero existen algunos con temáticas ilegales y no apropiadas para público menor de edad.

Actualmente hay grupos con una privacidad elevada que tienen cientos de miles de seguidores por lo regular jóvenes menores con cuentas falsas que se crean especialmente para entrar a esos grupos, ya que tienen temor de exponer sus verdaderas identidades por el material ilegal que posee el grupo.

Cualquier persona puede sufrir de la suplantación de su identidad y no solamente las personas famosas.

En Europa, el suplantar la identidad digital es un delito, dependiendo de qué suplante y para qué lo suplante la Oficina de Seguridad del Internauta señala que:

Si la suplantación consiste únicamente en el registro de un perfil falso en el que no se utiliza información personal del suplantado como por ejemplo una fotografía, la única acción legal que puede tomarse es notificar esta situación a la

¹⁷⁷ Crear cuenta de correo por 10 minutos, en línea <https://10minutemail.com> link consultado el 10 de mayo de 2017.

¹⁷⁸ Crear cuenta de correo con yopmail, en línea <http://www.yopmail.com/es/> link consultado el 10 de mayo de 2017.

red social implicada para que elimine dicho perfil de su página. Suplantar únicamente el nombre de una persona, si no lleva también la publicación de alguna imagen, no se considera delito.¹⁷⁹

Si se crea un perfil falso suplantando la identidad de una persona y en este caso sí se utilizan datos personales de la persona suplantada, como la fotografía, se estaría vulnerando el derecho al honor, a la intimidad y a la propia imagen de una persona, que recoge el artículo **18 de la Constitución Española**.¹⁸⁰

Si alguien accede al servicio de un usuario y se hace pasar por él, por ejemplo, correo electrónico, Facebook, Twitter, etcétera, claramente se está infringiendo la ley y es denunciabile, ya que se traspasa la barrera de la privacidad de una persona (usurpación de la identidad). Además, el suplantador está cometiendo un delito al haber realizado alguna práctica no lícita para acceder a dicha información del usuario: robo de contraseñas, entrometerse en sistemas informáticos, etcétera.¹⁸¹ Además, en este caso, en el artículo 401 del **Código Penal español**, “el que usurpare el estado civil de otro será castigado con la pena de prisión de seis meses a tres años”.¹⁸²

¹⁷⁹ Dato tomado de la página oficial de la Oficina de Seguridad del Internauta, Cómo denunciar una suplantación de identidad en Internet, publicado el 14 de mayo de 2014, disponible en línea en <https://www.osi.es/es/actualidad/blog/2014/05/14/como-denunciar-una-suplantacion-de-identidad-en-internet>, link consultado el 3 de mayo de 2017.

¹⁸⁰ *Idem*.

¹⁸¹ Ley No. 53-07 sobre Crímenes y Delitos de Alta Tecnología., en línea https://www.oas.org/juridico/PDFs/reptom_ley5307.pdf, link consultado el 3 de mayo de 2017.

¹⁸² Grupo Wolters Kluwer Formación S.A., España, Noticias Jurídicas, Artículo 401 del Código Penal, disponible en línea en http://noticias.juridicas.com/base_datos/Penal/lo10-1995.l2t18.html#c4, link consultado el 3 de mayo de 2017.

En estos ejemplos podemos ver claramente que existen varias conductas que derivan a diferentes clases de delitos, que a su vez conllevan a distintas penas. El primero es suplantación de la identidad pero si se utiliza parte de la información o se inventa el perfil no es un delito. El segundo es la utilización de la fotografía y datos reales de la persona, que sí se considera un delito pero no se especifica la pena o sanción. El tercero se maneja la palabra usurpación porque se está accediendo a la cuenta de alguien más utilizando herramientas que le permitan obtener la contraseña o cambiarla para obtener la posesión de la cuenta, en esta situación se están cometiendo varios delitos como practica ilícita para el acceso y usurpación de la cuenta.

En esta lista podemos leer las formas más comunes de usurpación de la identidad:

- Robo de buzón de correo: es uno de los métodos más básicos disponibles para el robo de identidad.
- Cambio de dirección: los delincuentes cambian la dirección donde se recibe el correo electrónico y desvían así la información personal.
- Intercambio de archivos P2P: diferentes sitios para compartir música o documentos que ha propiciado la obtención de todo tipo de información personal.
- Phishing de Facebook: El cibercriminal, conocido como phisher, se hace pasar por una persona o empresa de confianza en una aparente comunicación oficial electrónica, por lo común un correo electrónico.
- Vishing:¹⁸³ obtención de información personal a través de Vishing-voicecalls hechas a teléfonos móviles o fijos.¹⁸⁴

¹⁸³ Formas comunes de usurpar identidad, <http://www.nordsterntech.com/seguridad-informatica/vishing-smishing-hoax-y-los-fraudes-mas-populares-en-internet/>, consultado 15 de febrero de 2018.

¹⁸⁴ Cañete, Borja, “¿Por qué se produce el robo de identidad?”, *Ranika.com*, disponible en línea en <https://www.rankia.com/blog/opiniones/2057426-por-que-produce-robo-identidad>, consultado 15 de febrero de 2018

Como podemos observar son actividades que podemos realizar casi a diario, pero estas son aprovechadas por los criminales para realizar actos que perjudican a la gente, incluso, pueden pasar sin que nos percatemos.

En ocasiones, los atacantes pueden instalar programas no deseados en nuestro equipo de cómputo, ya que éstos se instalan o ejecutan de manera muy sigilosa y a veces es indetectable por algunos softwares antivirus.

Una vez instalado, el malware puede ejecutar programas en el ordenador sin consentimiento, incluida la transmisión de información personal a ordenadores remotos, donde se almacena y se vende a los falsificadores y extorsionadores.

Existen tutoriales en la red donde se enseña a crear phishing de manera rápida, analizaremos este caso, en primer lugar cabe destacar que el blog visitado toca temáticas de hacking ético.

El tutorial consiste en duplicar una página para hacer que la víctima ingrese sus credenciales (correo y contraseña) de acceso en la página falsa, donde solo necesitamos un bloc de notas, y en el navegador abrir la opción ver código fuente de la página y un servidor gratuito de hosting donde podremos alojar temporalmente la URL maliciosa.¹⁸⁵

Lo que tenemos como aprendizaje en este tutorial es siempre verificar que tengamos el HTTPS activado en todo momento, verificar que los correos de notificaciones de Facebook sean los correctos, revisar la ortografía es importante, ya que si hacen falta caracteres en la página debemos dudar de la seguridad de la misma.

3.2 Software malicioso en Facebook

Algunos softwares que se utilizan para delinquir es el malware. En este caso hablamos de un malware para robar una contraseña de Facebook. La compañía de seguridad australiana LMNTRIX Labs el año pasado detectó un malware que es capaz de robar contraseñas de Facebook, solo que en este caso se hace identificar

¹⁸⁵ Esaú, A., "Hacking tutorial: Phishing en Facebook", *openwebinars.net*, disponible en línea en <https://openwebinars.net/blog/hacking-tutorial-phishing-en-facebook/>, link consultado el 29 de octubre de 2018.

por un software llamado “Facebook Password Stealer” o en otro nombre como “Facebook Password Recovery” el cual es un ejecutable para Windows, el cual imita la interfaz web de Facebook, solicitando al usuario el correo, su contraseña y la URL de Facebook para supuestamente iniciar el ataque.¹⁸⁶

El ataque supuestamente comenzaba y ejecutaba en segundo plano un proceso sospechoso, iniciando así el troyano para que el atacante tenga acceso remoto al equipo y algunas credenciales, el proceso llamado “spoolsvfax.exe” es detectado por varios antivirus como malware, por lo que es removido inmediatamente por el antivirus.¹⁸⁷

Este virus se descarga vía web casi desde cualquier página que ofrezca descargas gratuitas, para los usuarios sin experiencia se les hace simple tratar de robar una contraseña, pero lo que no tienen en cuenta son los riesgos de proporcionar las credenciales de acceso a una aplicación del cual no conocen el nombre del desarrollador ni la reputación de la aplicación, como se ha mencionado el sentido común también va de la mano con el uso de Software Antivirus.

Las recomendaciones son principalmente evitar acceder a sitios en Internet que pudieran ser no oficiales, fraudulentos o aceptar correos electrónicos que se desconozca quien los envía o simplemente acceder a mensajes que de pronto aparecen en pantalla y ofrecen juegos gratis, por mencionar algunos ejemplos.

3.3 SPAM en Facebook

¹⁸⁶ Arteaga, Sandra, “Detectando nuevo malware para robar la contraseña de Facebook”, CICESE, Seguridad de la información, disponible en línea en <https://seguridad.cicese.mx/alerta/181/Detectado-nuevo-malware-para-robar-la-contrase%C3%B1a-de-Facebook>, última fecha de consulta el 23 de diciembre de 2018.

¹⁸⁷ Hatmaker, Taylor “Facebook password stealing software comes packed with a trojan that steals your passwords”, *Techcrunch*, disponible en línea en <https://techcrunch.com/2017/08/10/facebook-password-stealing-software-comes-packed-with-a-trojan-that-steals-your-passwords/>, link consultado el 29 de octubre de 2018.

El uso de correos masivos es otra de las formas en que los delincuentes contactan con sus víctimas.

Se ha visto recientemente páginas o publicaciones en Facebook donde supuestamente se puede conseguir un iPhone completamente gratis, por señalar un “me gusta” a determinada página o por compartir las publicaciones de la página que lo sortea. En ocasiones pueden pedir el relleno de encuestas en línea a través de acortadores de enlaces monetizados para así aprovechar las visitas y generar ganancias para el administrador de la página, o bien para captar los datos de las personas para así lograr el cometido de robar dicha información, lograr suplantar la identidad o hacerse pasar por otra persona para contactar a posibles víctimas de trata.

Algunas de las preguntas, por ejemplo en la primera opción, incluyen edad, peso, tipo de dieta y cantidad de horas de sueño diarias, entre otras. Al finalizar, el sistema pide un número de teléfono celular y la compañía a la que este pertenece, probablemente para luego ser destinatario de mensajes SMS Premium. Una vez más, destacamos que este no es comportamiento malicioso ni implica una infección al usuario, pero sí se trata de un engaño ya que el prometido iPhone 6 nunca llegará: luego de finalizar la encuesta e ingresar el número de teléfono, el sistema indica que hubo un error en el registro y que será necesario completar cualquiera de las tres encuestas para acceder.¹⁸⁸

El spam implica ponerse en contacto con otras personas con contenido o solicitudes no deseadas. Este término comprende el envío de mensajes en masa, la publicación excesiva de enlaces o imágenes en las biografías de otras personas o el envío de solicitudes de amistad a personas desconocidas.

¹⁸⁸ Pagnotta, Sabrina, “¿iPhone 6 gratis? Ten cuidado con los últimos scams”, *welivesecurity*, disponible en línea en <https://www.welivesecurity.com/la-es/2014/09/17/iphone-6-gratis-cuidado-ultimos-scams/>, link consultado el 29 de octubre de 2018.

En algunos casos, el spam se propaga cuando se hace clic en enlaces incorrectos o se instala software malicioso. Otras veces, los estafadores obtienen acceso a la cuenta de Facebook, la cual utilizan para enviar spam.

3.4 Condiciones de uso de Facebook

Las condiciones de uso de Facebook son una serie de cláusulas que encontramos al utilizar y/o instalar un *software* por primera vez. Lo más común es que el usuario jamás lea completamente esos términos.

El texto inicia dando la bienvenida a la red social. Y señalando que “Estas son las condiciones que rigen el uso de Facebook y los productos, las funciones, las aplicaciones, los servicios, las tecnologías y el software que ofrecemos (...), excepto cuando indiquemos expresamente que se aplican otras condiciones (distintas a estas)”.¹⁸⁹

Los servicios se explica están personalizados haciendo uso de los datos sobre las conexiones que se hacen, las configuraciones que se seleccionan asó como la información que se comparte tanto por medio de los productos de la red social como fuera de ellos.

Como uno de sus servicios se contempla “ofrecer ayuda, eliminar contenido, bloquear el acceso a ciertas funciones, inhabilitar una cuenta o comunicarnos con las fuerzas del orden. Compartimos datos con otras empresas de Facebook cuando detectamos que una persona usa alguno de nuestros Productos de forma inapropiada o perjudicial”.¹⁹⁰

Facebook en sus condiciones señala que los menores de 13 años no pueden usar la plataforma, ni los delincuentes condenados por delitos sexuales Prohíbe el uso de la plataforma también para realizar actividades engañosas, ilegales, discriminatorias o fraudulentas o infringir derechos de otras personas.¹⁹¹

¹⁸⁹ Las condiciones de servicio de Facebook se pueden consultar en <https://www.facebook.com/legal/terms/update>, última fecha de consulta el 23 de diciembre de 2018.

¹⁹⁰ *Idem.*

¹⁹¹ *Idem.*

Específicamente estas últimas prohibiciones son las que reconocemos relevantes en el tema de suplantación de identidades con fines de trata de personas a través de esta red social. En estos casos las políticas de uso de Facebook también advierte que es posible cambiar el nombre de usuario por ejemplo si no guarda relación con el nombre que se usa en la vida cotidiana.¹⁹²

Facebook en estas condiciones de uso reconoce que “Nos esforzamos por proporcionar los mejores Productos posibles y definir pautas claras para todos aquellos que los usen. No obstante, nuestros Productos se proporcionan tal como están y no podemos garantizar que siempre serán seguros [...] No controlamos ni dirigimos lo que las personas u otros hacen o dicen, ni somos responsables por sus acciones o conductas (dentro o fuera de internet) ni por el contenido que comparten, incluido contenido ofensivo, inapropiado, obsceno, ilegal o cuestionable”.¹⁹³ La fecha de la última revisión es del 19 de abril de 2018.

Si bien es cierto que al aceptar un contrato de adhesión como este aceptamos todos los términos y condiciones del mismo siempre podemos cancelar la cuenta de usuario y dejar de utilizar esta plataforma, situación que la mayoría de sus usuarios no haremos aún que estemos consientes de los riesgos de la misma.

3.5 Seguridad y protección de datos en Facebook

Como se ha venido indicando como una medida de seguridad se recomienda la instalación de antivirus, que deben ser actualizados ya que hay dominios que falsifican la interfaz de Facebook para que el usuario introduzca su contraseña y sea robada inmediatamente por el delincuente cibernético. Y almacene esta información en servidores donde puede vender o hacer mal uso de la información. El *phishing* usa este método, prácticamente duplica páginas *web*, siempre es necesario que al ingresar datos sea en la página correcta y con el HTTPS activo.

Con tecnologías de robo de datos es necesario que actualicemos nuestro *software* antivirus y activar el *Firewall* en todo momento, usar el monitor de red puede ayudarnos a detectar que se está enviando tráfico de red sin que nos demos

¹⁹² *Idem.*

¹⁹³ *Idem.*

cuenta. Debemos estar alerta en cualquier aspecto porque ya prácticamente ningún lugar es seguro para nuestros datos.

Cuando eliminamos un contenido de Facebook, no es descabellado pensar que éste desaparezca de la red social; sin embargo, las cosas no son tan simples. Facebook nos avisa que aunque borremos algo puede que no desaparezca del todo porque, como buena empresa tecnológica, guarda copias de seguridad de sus bases de datos y contenidos y los retiene durante un tiempo para poder recuperar información. Por tanto, aunque borremos algo, lo más seguro es que Facebook lo siga conservando.

Que una aplicación acceda a nuestros datos, según Facebook, es algo que depende de nosotros. Facebook se asegura de mostrar qué información y acceso requiere la aplicación conectada y queda de nuestro lado aceptar estas condiciones de la aplicación (y compartir nuestra información con un tercero). Por el hecho de usar Facebook, los usuarios nos convertimos en “producto” de los anunciantes de la plataforma. Al registrarnos estamos aceptando tácitamente que Facebook use nuestra foto de perfil, nuestro nombre o nuestros contenidos para sus campañas publicitarias o algoritmos de segmentación; de esta forma, usan nuestros datos para modelar la publicidad que vemos o la que puedan ver otros usuarios (indicando a nuestros amigos que a nosotros nos gusta una determinada marca). Nuestra implicación en la publicidad es obligatoria y, por supuesto, no recibiremos dinero alguno por nuestra participación.

Al usar Facebook consentimos que nuestros datos se almacenen en Estados Unidos y, por tanto, les aplique la legislación vigente en el país. De todas formas, hay una curiosa excepción para los usuarios de Alemania que cuentan con unas condiciones especiales tras los distintos procesos legales contra la red social en este país.

3.5.1 Seguridad y protección de los usuarios en FB

Facebook no garantiza que su plataforma sea segura; sí que es cierto que impone ciertas "reglas de uso" y mecanismos para informar si nos topamos con usuarios que ejerzan de stalkers, publiquen contenidos violentos, sean spammers o realices actividades comerciales fuera de las normas establecidas.

Para poder registrar una cuenta en Facebook, el usuario debe ser mayor de 13 años y ofrecer información real (nada de nombres falsos o registrarnos suplantando a otra persona). De hecho, al registrarnos, uno adquiere una serie de compromisos con Facebook que, teóricamente, debemos cumplir: mantener actualizada la información de contacto, no compartir nuestra contraseña (aunque esto debería ser obvio), no transferir la cuenta a un tercero, usar datos reales y, además, acatar que Facebook pueda reclamar (y quitarnos) nuestro nombre de usuario porque una marca lo reclame o se queje. Facebook se reserva el derecho de retirar contenidos publicados si considera que violan sus políticas o si alguien ha denunciado una violación de derechos de propiedad intelectual. Además, para los usuarios reincidentes, Facebook puede considerar la desactivación de las cuentas sin previo aviso.¹⁹⁴

Nuevamente reiteramos el comentario de la sección anterior que se refiere a que en cualquier momento se puede tomar la decisión de eliminar la cuenta de la red social y evitar que estas actividades se puedan realizar con nuestra información, sin embargo debemos estar ciertos de que la información con la que se ha nutrido la red social permanecerá por algún tiempo en resguardo por la misma empresa.

3.6 Derechos del usuario

Las personas que tenemos una cuenta de Facebook como se ha mencionado aceptamos un contrato de adhesión, esto quiere decir que aceptamos todos los términos y condiciones. Uno de nuestros derechos es conocer cuándo estas políticas y condiciones cambien, aun así si estas políticas de uso o condiciones de servicio cambian y volvemos a aceptar el nuevo contrato se están aceptando las nuevas reglas.

Existe la posibilidad de eliminar la cuenta:

Nuestra cuenta puede darse de baja o desactivarse tanto si lo solicitamos nosotros mismos como de manera unilateral por parte de Facebook (por ejemplo, por un mal uso). La desactivación es temporal, es decir, podemos volver a Facebook y reactivar la cuenta sin que los datos se hayan perdido. En el caso de eliminar nuestra cuenta, Facebook eliminará nuestros datos aunque,

¹⁹⁴ *Idem.*

eso sí, con la prerrogativa que comentábamos al inicio: las copias de seguridad se mantienen.

Aunque eliminemos nuestra cuenta del servicio, Facebook mantiene vigente algunas cláusulas de sus condiciones de servicio y, además de mantener los backups, los likes que hayamos hecho o los contenidos que se hayan compartido como "públicos".

Facebook es una empresa estadounidense, por tanto, la legislación que aplica es la de su país: la ley estadounidense de protección de los derechos de autor (Digital Millennium Copyright Act) o la ley de protección de la privacidad de vídeo (Video Privacy Protection Act, VPPA) y, en caso de demanda, el fuero que aplica es el del tribunal del Distrito Norte de California o en un tribunal estatal del Condado de San Mateo. Además, Facebook queda exenta de toda responsabilidad por nuestros actos y en caso de demanda por algo que hayamos hecho, ellos permanecerán al margen.

Facebook no ofrece garantías de disponibilidad del servicio ni tampoco se hace responsable de lo que hagan los usuarios, ellos redactan un código de conducta que intentan que se cumpla, pero tampoco garantizan que esto vaya a ocurrir en el 100% de los casos.¹⁹⁵

De este resumen de las cláusulas podemos ver que las siguientes tienen mucho que ver con la privacidad y protección de datos.

Más allá de la situación normativa nacional e internacional aplicable a la problemática que se intenta abordar en el presente trabajo, existe otro marco normativo aplicable y es aquel dispuesto a través de la Declaración de Derechos y Responsabilidades de la propia plataforma Facebook.

A momento de registrar una cuenta, es obligatoria y necesaria la aceptación de estos términos y condiciones legales establecidos por Facebook, entre los cuáles se pueden encontrar distintas cláusulas aplicables al tema-. Entre ellas, el inciso 4to. Sobre "Seguridad de la cuenta y registro", establece que:

Los usuarios de Facebook proporcionan sus nombres y datos reales, y necesitamos tu colaboración para que siga siendo así. Estos son algunos

¹⁹⁵ *Idem.*

de los compromisos que se aceptan en relación con el registro y el mantenimiento de la seguridad de una cuenta:

1. No proporcionarás información personal falsa en Facebook, ni crearás una cuenta para otras personas sin su autorización.
2. No crearás más de una cuenta personal.
3. Si inhabilitamos tu cuenta, no crearás otra sin nuestro permiso.
4. No utilizarás tu biografía personal para tu propio beneficio comercial, sino que para ello te servirás de una página de Facebook.
5. No utilizarás Facebook si eres menor de 13 años.
6. No utilizarás Facebook si fuiste declarado culpable de un delito sexual.
7. Mantendrás la información de contacto exacta y actualizada.
8. No compartirás tu contraseña (o, en el caso de los desarrolladores, tu clave secreta), no dejarás que otra persona acceda a tu cuenta, ni harás nada que pueda poner en peligro la seguridad de tu cuenta.
9. No transferirás la cuenta (incluida cualquier página o aplicación que administres) a nadie sin nuestro consentimiento previo por escrito.
10. Si seleccionas un nombre de usuario o identificador similar para tu cuenta o página, nos reservamos el derecho de eliminarlo o reclamarlo si lo consideramos oportuno (por ejemplo, si el propietario de una marca comercial se queja por un nombre de usuario que no esté estrechamente relacionado con el nombre real del usuario).¹⁹⁶

3.7 Protección de los derechos de otras personas

La red social deja de manifiesto que “Respetamos los derechos de otras personas y esperamos que tú hagas lo mismo” Para ello enlisa una serie de obligaciones para todos los usuarios que se enlistan a continuación.

¹⁹⁶ Temperini, Marcelo G.I., y Macedo, Maximiliano, “La problemática de los perfiles falsos en Facebook y su relación con el Cibercrimen”, *SID 2015, 15o. Simposio Argentino de Informática y Derecho*, p. 196, disponible en línea en <http://44jaiio.sadio.org.ar/sites/default/files/sid185-198.pdf>, link consultado el 29 de octubre de 2018.

1. No publicarás contenido ni realizarás ninguna acción en Facebook que infrinja o vulnere los derechos de terceros o que vulnere la ley de algún modo.
2. Podemos retirar cualquier contenido o información que publiques en Facebook si consideramos que infringe esta Declaración o nuestras políticas.
3. Te proporcionamos las herramientas necesarias para ayudarte a proteger tus derechos de propiedad intelectual. Para obtener más información, visita nuestra página [Cómo reportar vulneraciones de derechos de propiedad intelectual](#).
4. Si retiramos tu contenido debido a una infracción de los derechos de autor de otra persona y consideras que cometimos un error, tendrás la posibilidad de apelar la decisión.
5. Si infringes repetidamente los derechos de propiedad intelectual de otras personas, inhabilitaremos tu cuenta cuando lo estimemos oportuno.
6. No utilizarás nuestros derechos de autor, nuestras marcas comerciales ni ninguna marca que se parezca a las nuestras, excepto si lo permiten nuestras Normas de uso de las marcas de forma expresa o si recibes un consentimiento previo por escrito de Facebook.¹⁹⁷
7. Si obtienes información de los usuarios, deberás obtener su consentimiento previo, indicar claramente que eres tú (y no Facebook) quien recopila la información y publicar una política de privacidad que explique qué datos recopilas y cómo los usarás.
8. No publicarás los documentos de identidad ni la información financiera confidencial de nadie en Facebook.
9. No etiquetarás a los usuarios ni enviarás invitaciones por correo electrónico a quienes no sean usuarios sin su consentimiento. Facebook ofrece herramientas

¹⁹⁷ “Aviso a navegantes, derechos de autor y Facebook”, 9 de junio de 2012, disponible en línea en <https://www.facebook.com/notes/autismodiario/aviso-a-navegantes-derechos-de-autor-y-facebook/482364728447421/>, link consultado el 29 de octubre de 2018.

de reporte social para que los usuarios puedan hacernos llegar sus comentarios sobre el etiquetado.¹⁹⁸

Para crear una cuenta de Facebook no se requieren más de 5 minutos, ya que el formulario es muy fácil de llenar y los datos fáciles de inventar, solo se necesita un nombre completo, un correo, una contraseña, y una fecha aleatoria, se recibe un correo de confirmación con un código y se puede comenzar a usar Facebook.

Facebook sugiere que se utilice el nombre real, pero es más vulnerable a recibir amenazas o que alguien usurpe nuestra identidad al crear un perfil falso con las mismas características que el perfil original. Actualmente existe la verificación, es decir algunas páginas de celebridades, entre otras reciben un símbolo de verificado, pero esto no es para todos.

Prácticamente todos los servicios *web* tienen cláusulas y acuerdos de uso que en ocasiones no se leen, porque son muy extensos, confusos o bien por estar en otro idioma, se complica la comprensión ya que están redactados en forma jurídica, se debe leer la mayoría o en el mejor de los casos leer todas las cláusulas y cumplir con la obligación como usuarios las cuales serían respetar el entorno de la plataforma para evitar problemas futuros.

Facebook brinda opciones desde su sitio de ayuda para reconocer un intento de phishing.

Desconfía de:

Mensajes con faltas de ortografía, erratas, varios tipos de letra o acentos mal colocados.

Mensajes que dicen tener una contraseña para ti en un archivo adjunto.

Facebook nunca te enviará una contraseña como archivo adjunto.

Enlaces que no coinciden: Al pasar el mouse por un enlace, mira la barra de estado situada en la parte inferior de la ventana del navegador. Asegúrate de

¹⁹⁸ “5 protección de los derechos de otras personas”, disponible en <https://www.coursehero.com/file/p6b4j13/5-Protecci%C3%B3n-de-los-derechos-de-otras-personas-Respetamos-los-derechos-de-otras/>, fecha de consulta el 29 de octubre de 2018.

que el enlace realmente te conducirá al destino que se indica en el correo electrónico.

Mensajes que te piden tus datos personales. Facebook nunca te pedirá:

La contraseña de tu cuenta

Tu número de la seguridad social o tu número de identificación fiscal

El número de tu tarjeta de crédito o el PIN

Mensajes que te amenazan con la eliminación o bloqueo de tu cuenta si no realizas alguna acción de forma inmediata.

Recuerda que puedes reportar los correos electrónicos de phishing en phish@fb.com o a través de los enlaces de reportes que aparecen en diversos lugares de Facebook. Como no podemos responder a todos los reportes de phishing que recibimos, usaremos la información que nos proporcionas para investigar el asunto y tomar las medidas apropiadas si corresponde.¹⁹⁹

A pesar de estas obligaciones y sugerencias la realidad nos demuestra que la red social no es segura por si misma sino que se requiere también por parte de los usuarios una conducta responsable y consciente sobre los posibles ilícitos que se pudieran cometer haciendo uso de los perfiles de los usuarios o si no se tiene un buen uso y protección de los datos personales.

3.8 Cómo denunciar la suplantación de identidad en Facebook

En párrafos anteriores se mencionó el caso de Iván Portilla, egresado de la carrera de Ciencias de la Comunicación en la UNAM, quien descubrió que había un perfil de Facebook con sus fotos pero con el nombre de Brayan Martínez, este es un caso de suplantación y el estudiante después de siete meses podía constatar que el perfil que se había creado haciendo uso de sus fotografías y que incluso se había contactado a algunos de sus contactos seguía activo y que la empresa no lo había eliminado.

Facebook pone a disposición la manera de “Reportar un hecho”, específicamente por suplantación de identidad Facebook señala que:

¹⁹⁹ Facebook “¿Qué puedo hacer frente al phishing? 2017 disponible en línea en <https://www.facebook.com/help/166863010078512?helpref=search>, link visitado el 10 de septiembre de 2017.

Facebook no permite cuentas ni páginas que suplantan la identidad de otras personas. Si ves una cuenta que se hace pasar por ti, por alguien que conoces o por una figura pública (por ejemplo, un famoso o un político), te animamos a avisarnos. No es necesario que tengas una cuenta de Facebook para reportar cuentas que tal vez estén suplantando la identidad de otra persona.

Si quieres reportar una cuenta de suplantación de identidad, determina en primer lugar si estás reportando un perfil o una página.

Si tienes una cuenta de Facebook y quieres reportar un perfil:

1. Ve al perfil de la cuenta que se hace pasar por ti.
 - Si no puedes encontrarlo, busca el nombre usado en el perfil o pide a tus amigos que te envíen un enlace al perfil.
2. Haz clic en  en la foto de portada y selecciona Reportar.
3. Sigue las instrucciones que aparecen en la pantalla sobre suplantación de identidad para enviar un reporte.

Si no tienes una cuenta de Facebook y quieres reportar a alguien que se está haciendo pasar por ti o por alguien que conoces, completa este formulario”.²⁰⁰

La suplantación de las identidades en perfiles de Facebook puede causar distintos daños:

Los daños y perjuicios causados por el robo de identidad no se limitan únicamente a problemas financieros, éste puede tener un alto costo tanto en el aspecto personal y sentimental de la víctima, debido a que puede dejar una sensación de violación a la vida privada. El impacto de este crimen sobre la víctima es económico, emocional y psicológico.

Los efectos negativos en su reputación y las subsecuentes dificultades para restablecer su credibilidad, son cuestiones que lamentablemente afectan la vida del individuo a escala social dando lugar a eventos como la pérdida de empleo, expulsión de círculos personales, profesionales o académicos, divorcios o separaciones, litigios legales, entre otras.

²⁰⁰ Información tomada de la página de Facebook, “Reporta un Hecho”, disponible en línea en <https://www.facebook.com/help/www/263149623790594/>, última fecha de consulta el 24 de diciembre de 2018.

Si sospecha ser víctima del robo de identidad debe actuar inmediatamente, contacte a su institución financiera para solicitar interponga una "alerta de fraude", así como el cierre y la cancelación de las cuentas que podrían estar involucradas. Alerta a sus proveedores de servicios virtuales, cambie las contraseñas o bloquee las cuentas que pudieran estar comprometidas, denuncie además ante la autoridad correspondiente. En México algunas de las entidades a las que se puede acudir son la CONDUSEF, la PROFECO y la Policía Federal.²⁰¹

Por su parte la Asociación Civil, Alianza por la Seguridad en Internet hace algunas sugerencias sobre las posibles actividades ilícitas que se cometen por medio del Internet:

Si es la primera vez que recibes un mensaje que te moleste de parte de otra persona:

Ignóralo. Cuando te llega por primera vez lo mejor que se puede hacer es: nada. Ignora el mensaje, no lo respondas ni lo re-transmitas. Si lo respondes estás cayendo en el juego del agresor, quien necesita de tu retro-alimentación para ir incrementando sus ataques. Mucho menos se recomienda amenazar de regreso al agresor.

Si eres menor de edad, informa a tus padres de inmediato, y si los mensajes implican violencia, repórtalo a la policía. Una, y sólo una vez responde al remitente que no deseas ser molestado. Usa un tono relajado pero serio y firme, nunca agresivo. Si lo consideras necesario, pide a tus padres que lo redacten por ti.

Si puedes identificar al proveedor de correo de la persona que te envía los mensajes, reporta la cuenta con la empresa, casi siempre tienen políticas que impiden utilizar sus servicios para molestar a otros usuarios. Si continúas recibiendo mensajes ofensivos o que de cualquier forma te molesten:

Guarda todos los mensajes como evidencia, es posible que la policía llegue a necesitarlos en caso que las cosas se compliquen y proceda una denuncia formal.

²⁰¹ DGTIC, "Robo de identidad y consecuencias sociales", 25 de octubre de 2010, disponible en línea en <https://www.seguridad.unam.mx/robo-de-identidad-y-consecuencias-sociales>, link consultado el 29 de octubre de 2018.

Es necesario que lo comentes con un adulto de confianza, preferentemente tus padres, para que te ayuden a denunciarlo. Recuerda que, si los mensajes incluyen amenazas, chantaje o extorsión, pueden ser constitutivos de delito, por lo que deberás reportarlo a la policía.²⁰²

También el blog de la Presidencia de la República para evitar ser víctimas de trata de personas emite las siguientes recomendaciones:

- En los perfiles de tus redes sociales nunca publiques información personal, por ejemplo, tu nombre completo, domicilio, número telefónico, o el de otras personas que tú conozcas ni compartas fotos de tus familiares o amigas y amigos, o cualquier información tuya de manera pública.
- Limita el acceso a tu información sólo a las personas más cercanas a ti, no uses las redes para conocer gente ya que puede ser muy peligroso.
- Desconfía de anuncios o personas que ofrecen trabajos muy atractivos, principalmente si el trabajo es fuera de la ciudad donde vives, más aún si te piden que te tomes fotografías en traje de baño o con poca ropa.
- Nunca vayas sola o solo a entrevistas de trabajo, pídele a un familiar o amigo que te acompañe.
- Aléjate de personas que te aborden en la calle para conocerte.
- Si recibes mensajes en los que busquen seducirte, ilusionarte, amenazarte, chantajearte, intimidarte, o con la promesa de regalarte cosas que te gustan, plátalo con una persona de tu confianza, de preferencia con tus padres o profesoras o profesores.
- Si las políticas de seguridad del sitio te lo permiten, reporta todo tipo de abuso cuando exista una amenaza o alguien exprese comentarios que te incomoden, no sólo te ayudará a ti, sino protegerás a las demás personas que navegan.
- Nunca hables con personas desconocidas en Internet y mucho menos actives tu webcam con ellas.

²⁰² Alianza por la Seguridad en Internet A.C., “Guía A.S.I para prevención del ciber-Bullying”, disponible en línea en http://www.asi-mexico.org/sitio/archivos/Guia2012_SOLO-ASI_Ciber-Bullying_WP_FINAL.pdf, p. 28, link consultado el 3 de mayo de 2017.

- Coquetear en línea con personas extrañas puede tener graves consecuencias, ya que algunas mienten y pueden hacerse pasar como personas de tu edad, nunca puedes saber realmente con quién estás tratando.
- Nunca compartas fotografías con poca ropa o en situaciones íntimas con nadie.
- Conserva los mensajes, correos electrónicos y toda información indebida, (como frases o imágenes ofensivas) servirán en caso de que sea necesario denunciar ante las autoridades.
- No permitas el acceso o aceptes invitaciones de amistad de personas desconocidas, aunque se presenten como de la escuela, de algún club o equipo deportivo al que perteneces o amistades de familiares.
- Nunca compartas información que sirva para identificarte o localizarte fuera de Internet, por ejemplo, los lugares que frecuentas, los días y la hora en que lo haces, los horarios en que estás en tu casa o los momentos en que te quedas a solas.
- Crea contraseñas seguras: tienen que contar como mínimo con ocho caracteres; contener letras mayúsculas, minúsculas, símbolos y signos de puntuación; créala con base en una frase que puedas recordar fácilmente, y cámbiala frecuentemente.
- Si cuando estás en línea te sientes amenazada o amenazado por alguna persona o te molesta algo que te muestre en la pantalla, es necesario que se lo digas a una persona con la que tengas confianza para que denuncie este hecho a las autoridades.
- Se debe de estar consciente de que nuestros actos en Internet con frecuencia tienen consecuencias fuera de la web.²⁰³

Para evitar que algún integrante de la familia se una a estos grupos es necesaria la supervisión de su uso del Internet, así como por parte de los padres informarse sobre cada red social que exista, y los usos que tiene, las políticas de

²⁰³ Presidencia de la República México “Recomendaciones para evitar ser víctima de trata de personas”, en línea 30 de julio de 2015 <https://www.gob.mx/presidencia/articulos/recomendaciones-para-evitar-ser-victima-de-trata-de-personas>, link visitado el 13 de septiembre de 2017.

privacidad, la reputación del grupo, leer sus normas comunitarias y conocer a sus administradores y moderadores.

3.9 El ABC para prevenir la suplantación de la identidad y la trata en Facebook

Finalmente en esta propuesta de intervención queremos dejar de manifiesto en este capítulo algunas recomendaciones que nos parecen apropiadas para hacer un frente en contra de la suplantación de identidad en Facebook, que si bien no es una solución al fenómeno de trata de personas cuando se utiliza Facebook como herramienta de contacto por lo menos es una manera de evitar que los delincuentes contacten a sus posibles víctimas.

Deseamos firmemente que estas propuestas sirvan para paliar este fenómeno.

A- Prevención

Existen organizaciones que están trabajando internacionalmente como es la Oficina de las Naciones Unidas contra la Droga y el Delito, esta oficina tiene como mandato de ayudar a los estados miembros en su lucha contra las drogas ilícitas, la delincuencia transnacional en todas sus dimensiones, “Para la consecución de sus objetivos, la UNODC, acrónimo en inglés para United Nations Office on Drugs and Crime, hace todos los esfuerzos para integrar e incorporar la perspectiva de género, sobre todo en sus proyectos para la provisión de medios de vida alternativos, así como aquellos en contra de la trata de personas”.²⁰⁴

Existen algunas organizaciones en diferentes partes del mundo que combaten la trata de personas utilizando como estandarte la prevención, la fundación María de los Ángeles, “lucha contra la trata de personas desde el 2007,

²⁰⁴ Acerca de la UNODC, disponible en línea en <https://www.unodc.org/unodc/en/about-unodc/index.html?ref=menutop>, link consultado el 12 de mayo de 2017.

quien inicia esta fundación la inicio Susana Trimarco desde el secuestro y desaparición de su hija el 3 de abril de 2002”.²⁰⁵

La explotación va desde hombres, mujeres, niños y niñas, son forzados a trabajos forzados y en ocasiones se les fuerza al matrimonio, son las principales víctimas de la trata ya que son engañadas por los métodos antes mencionados, en ocasiones supuestos amigos tienen que ver con el engaño.

B- La cooperación internacional

Es fundamental en la materia ya que de esta dependerán el éxito de las acciones e investigaciones que surjan al respecto dada la dimensión internacional de la trata de personas. Se debe de trabajar en una serie de directrices que esclarezcan cómo se deben de atender las solicitudes de cooperación internacional en materia de suplantación de identidades ya que los procedimientos formales suelen obstaculizar las investigaciones y solo teniendo acuerdos de asistencia judicial recíproca se podrá dar respuesta ágil y rápida a los incidentes y solicitudes de cooperación internacional.

C. Protección de Datos

Finalmente los usuarios de las redes sociales somos responsables de los datos que compartimos por ello es importante:

1. No revelar nuestros nombres, en su lugar usar alias o seudónimos en nuestras distintas redes sociales.
2. Usar distintas contraseñas en las distintas redes y cambiarlos con cierta periodicidad.
3. Entender los contratos de adhesión que establecen las redes sociales y sitios de Internet en general así como sus condiciones de uso antes de aceptarlos.
4. Revisar cómo se debe de configurar la privacidad de la red que se utilice y elegir siempre los estándares más altos aunque eso signifique no recibir notificaciones o perder “beneficios”.

²⁰⁵ Fundación María de los Ángeles, disponible en línea en <http://fundacionmariadelosangeles.org/fundacion-maria-de-los-angeles.htm>, link consultado el 12 de mayo de 2017.

5. No involucrarse con personas desconocidas, ni acordar conocerse aunque sea en espacios públicos y mucho menos en lugares distantes o secretos.
6. No cargues información personal como edad, dirección, colegio en el que estudias, no menciones nombres de familiares, no permitas que se conozcan quiénes son tus contactos.
7. No accedas a sitios que sean sospechosos o no seguros como pueden ser páginas de juegos gratuitos, casinos, ofertas de viajes, portales que ofrecen ganar ciertos premios solo por completar encuestas.
8. No aceptes llenar formularios en los que tengas que dar tus datos.
9. Por ningún motivo comparas contraseñas.
10. Cuando te encuentres navegando por la red y se abran ventanas emergentes cierra el navegador completamente, nunca descargues archivos o accedas a vínculos que se te sugieran.
11. Si tienes una cuenta de correo electrónico y llegues a recibir correos de remitentes desconocidos o en idioma extranjero simplemente elimínalos, no los abras, mucho menos accedas a archivos adjuntos de correos desconocidos.
12. En la medida de lo posible trata de no utilizar redes WiFi abiertas, no accedas a tus cuentas de correo electrónico o redes sociales en computadoras que sean de uso público y en caso de que lo tengas que hacer cerciérate de cerrar las sesiones y de borrar los cachés para que no se pueda guardar de manera automática tu cuenta y contraseña para fácil acceso.
13. Mantén actualizados tus antivirus, antispysware.



Conclusiones



Conclusiones

La presente propuesta de intervención pretende contribuir a informar y prevenir la captación de personas para someterlas a trata por medio de perfiles de Facebook, objetivo que creemos se alcanza con la infografía digital que se elaboró luego de obtener todos los datos en la investigación del tema.

A lo largo de la investigación se dejan de manifiesto varias situaciones que sirven para elaborar estas conclusiones. En primer lugar se observa que existe aún una indefinición por el uso de conceptos entre los que se usan casi indistintamente la usurpación de identidad, el robo de identidad, la suplantación de identidad o el fraude de identidad. Se observó que en la materia ni a nivel internacional se ha decidido cuál es el concepto que debe prevalecer.

Se observó también que al estudiar el tema de robo de identidad se hace referencia a los ilícitos que se comenten con fines de afectación a las personas en su economía, es decir que se roba o suplanta la identidad con fines principalmente de hacer fraudes y extraer el dinero de las personas de quien se logran obtener los datos financieros y bancarios y muy pocos son los estudios que se están concentrando para alertar, investigar y tratar de paliar la suplantación de identidad con fines de trata de personas.

En el contexto legal pudimos observar que en México aún no existen leyes que prevén a la suplantación de la identidad en medios digitales como un ilícito.

Se observó que la plataforma de Facebook es un medio ideal para los delincuentes ya que por medio de perfiles falsos suelen aproximarse a sus víctimas en especial aprovechándose de la poca experiencia que tienen los menores y lo sencillo que les resulta engañarlos para que revelen su ubicación, datos personales, los lugares que frecuentan e inclusive datos sobre los colegios a los que asisten entre muchos otros detalles que sirven para que puedan ser presa fácil de los tratantes.

Finalmente se realizó un poster digital donde se utilizaron los datos de la investigación para concretar la propuesta de intervención que es la difusión y prevención de la trata de personas por medio de perfiles de Facebook y se concluye que existen temas en los que aún se debe trabajar como es la prevención, la

cooperación internacional, la legislación en la materia y por supuesto la protección de datos que recae por ahora en gran parte sobre las acciones que implementemos los usuarios de las redes sociales.

Bibliografía

ÁLARCÓN GARCÍA, Daniela, *Trata de personas: Uno de los delitos más lucrativos del mundo*, Monografía para optar por el título de Bachiller Académico, Gimnasio Josegina Castro de Escobar, Bogotá, D.C., 2013.

ALONSO, Julio, *Identidad digital y reputación on line*, Madrid, Evoca Comunicación e imagen, 2011.

BARTH, Fredrik, Los grupos étnicos y sus fronteras. La organización social de las diferencias culturales, 1a. ed., en español, México, Fondo de Cultura Económica, 1976.

CASTELLS, Manuel, *La galaxia Internet: Reflexiones sobre Internet, empresa y sociedad*, Barcelona, Plaza & Janés, 2001.

COMISIÓN NACIONAL DE DERECHOS HUMANOS, *Diagnóstico sobre la situación de la trata de personas en México*, México, CDNH, 2013.

EZETA, Fernanda, *Trata De Personas: Aspectos Básicos*, México, Comisión Interamericana de Mujeres de la Organización de Estados Americanos, Organización Internacioal para las Migraciones, Instituto Nacional de Migración e Instituto Nacional de las Mujeres, 2006.

FERRADA BUBNIAK, Nicole Eden e INIESCAR MEDINA, Fernanda Jesús, “Usurpación de identidad en las redes sociales: Facebook y Twitter. Tratamiento legal y jurisprudencia en Chile”, Memoria para optar por el grado de licenciado en Ciencias Jurídicas y Sociales, Facultad de Derecho, Departamento de Derecho Procesal, Universidad de Chile, 2015.

FUNDACIÓN TELEFÓNICA, *Identidad digital: El nuevo usuario en el mundo digital en línea*, Madrid, Ariel-Fundación telefónica y Editorial Planeta, 2013.

GARCÍA RICCI, Diego, “Artículo 16 Constitucional Derecho a la privacidad”, en *Derechos Humanos en la Constitución: Comentarios y Jurisprudencia Constitucional e Interamericana*, México, Instituto de Investigaciones Jurídicas, UNAM, Suprema Corte de Justicia de la Nación y la Fundación Konrad Adenauer, 2013.

NACIONES UNIDAS, Manual sobre los delitos relacionados con la identidad, Naciones Unidas, Nueva York, 2013.

NAVA GARCÉS, Alberto Enrique, *La prueba electrónica en materia penal. Nuevas tecnologías de la información, redes sociales, telefonía celular, dispositivos electrónicos, geolocalización, cadena de custodia, prueba ilícita, casos*, México, Porrúa, 2015

OROZCO, Rosi, *Trata de personas*, México, Instituto Nacional de Ciencias Penales, 2011.

PEÑA LIBIEN, Hiram Raúl, “Los delitos Informáticos previstos y sancionados en el Ordenamiento Jurídico Mexicano” en Memorias del Segundo Congreso Nacional de Cultura y Legalidad Informática Jurídica, México, SEGOB, 2012.

PONCE SERNICHARO, Gabriela y KÁNTER CORONEL, Irma del Rosario, *Al día las cifras hablan núm. 70. Día mundial contra la trata de personas*, México, Instituto Belisario Domínguez del Senado de la República, s/f.

RUIZ GUTIÉRREZ, Urbano, *Diccionario de Jurisprudencia penal 1983-1988*, Ministerio de Justicia, Tomo VII, Secretaría General Técnica. Centro de Publicaciones, Madrid, 1991.

S/A, Guía para prevenir el robo de identidad, México, INAI, s/f.

TREJO GARCÍA, Elma del Carmen, *et. al., Compendio de Instrumentos Internacionales Relativos a la Trata de Personas*, Servicio de Investigación y Análisis, Subdirección de Política Exterior, Cámara de Diputados LXI Legislatura y Dirección General de Bibliotecas SIID, 2006.

Cibergrafía

Alianza por la Seguridad en Internet A.C., “Guía A.S.I para prevención del ciber-Bullying”, disponible en línea en http://www.asi-mexico.org/sitio/archivos/Guia2012_SOLO-ASI_Ciber-Bullying_WP_FINAL.pdf, p. 28, link consultado el 3 de mayo de 2017.

APF, “Facebook alcanza los 2,000 millones de usuarios”, *El economista*, disponible en línea en <https://www.economista.com.mx/tecnologia/Facebook-alcanza-los-2000-millones-de-usuarios-20170627-0013.html>, link consultado el 23 de diciembre de 2018.

BBC Mundo, “5 claves para entender el escándalo de Cambridge Analytica que hizo que Facebook perdiera US\$37.000 millones en un día”, disponible en

<https://www.bbc.com/mundo/noticias-43472797>, última fecha de consulta el 19 de noviembre de 2018.

BLOG DE ESTRADA VILLEGAS, Carina, “ONU: Identidad digital como derecho humano básico”, 7 de agosto de 2017, disponible en línea en <https://carinaestradasite.wordpress.com/2017/08/07/onu-identidad-digital-como-derecho-humano-basico/>, link consultado el 22 de octubre de 2017.

BLOG NORMOL, Redes sociales, “Historia de las redes sociales”, disponible en línea en <http://histinf.blogs.upv.es/2011/12/20/redes-sociales/>, link visitado el 22 de octubre de 2018.

Boletín “División Científica de la Policía Federal Detecta Nuevas Amenazas Cibernéticas que Suplantán Identidades, Comisión Nacional de Seguridad”, Sala de Prensa de la Comisión Nacional de Seguridad, Secretaría de Gobernación, 8 de agosto de 2014, disponible en http://www.cns.gob.mx/portalWebApp/appmanager/portal/desk?_nfpb=true&_windowLabel=portlet_1_1&portlet_1_1_actionOverride=%2Fboletines%2FDetalleBoletin&portlet_1_1id=1348059, link consultado el 4 de mayo de 2017.

BUBNIAK FERRADA, Nicole Edén, INIESCAR MEDINA, Fernanda Jesús, “Usurpación de identidad en las redes sociales: facebook y twitter. Tratamiento legal y jurisprudencial en Chile” 2015 en línea <http://repositorio.uchile.cl/bitstream/handle/2250/135613/Usurpaci%C3%B3n-de-identidad-en-las-redes-sociales.pdf?sequence=1&isAllowed=y>, link visitado 9 de septiembre de 2017.

BUSTILLOS, “Que hacer ante la usurpación de identidad en internet” (sic), entrada en respuesta a pregunta en el espacio Toluna.com, disponible en línea en <https://es.toluna.com/opinions/2242983/Que-hacer-ante-la-usurpacion-de-identidad-en-interne>, link consultado el 29 de octubre de 2018.

CAÑETE, Borja, “¿Por qué se produce el robo de identidad?”, *Ranika.com*, disponible en línea en <https://www.rankia.com/blog/opiniones/2057426-por-que-produce-robo-identidad>, consultado 15 de febrero de 2018.

CONDUSEF, “Robos de identidad”, disponible en <https://www.condusef.gob.mx/gbmx/?p=estadisticas>, consultado el 4 de noviembre de 2018.

DGTIC, “Robo de identidad y consecuencias sociales”, 25 de octubre de 2010, disponible en línea en <https://www.seguridad.unam.mx/robo-de-identidad-y-consecuencias-sociales>, link consultado el 29 de octubre de 2018.

ESAÚ, A, “Hacking tutorial: Phishing en Facebook”, *openwebinars.net*, disponible en línea en <https://openwebinars.net/blog/hacking-tutorial-phishing-en-facebook/>, link consultado el 29 de octubre de 2018.

GALEANO, Susana “Facebook prohibirá usar Custom Audiences para realizar campañas segmentadas a usuarios que no hayan dado su autorización”, *M4rketiing Ecommerce*, disponible en línea en, <https://marketing4ecommerce.net/facebook-prohibira-usar-custom-audiences/>, link consultado el 12 de mayo de 2017.

GLOBAL MEDIA, “¿Cómo identificar a una víctima de trata de personas?”, 4 de septiembre de 2017, disponible en línea <https://globalmedia.mx/articles/C%C3%B3mo-identificar-a-una-v%C3%ADctima-de-trata-de-personas->, link visitado el 13 de septiembre de 2017.

HATMAKER, Taylor “Facebook password stealing software comes packed with a trojan that steals your passwords”, *Techcrunch*, disponible en línea en <https://techcrunch.com/2017/08/10/facebook-password-stealing-software-comes-packed-with-a-trojan-that-steals-your-passwords/>, link consultado el 29 de octubre de 2018.

INFOEM, *El abc de los datos personales*, disponible en https://www.infoem.org.mx/doc/publicaciones/ABC_Datos.pdf, link consultado el 30 de octubre de 2018.

LABARCA CASTRO, Raphael, “El robo de identidad y sus cifras en América Latina, *welivesecurity by eset*, 8 de abril de 2011, disponible en línea en <https://www.welivesecurity.com/la-es/2011/04/08/robo-identidad-cifras-america-latina/>, link consultado el 23 de octubre de 2017.

MARTÍNEZ, A., “Zuckerberg recula: Facebook sí es un medio de comunicación”, @abc_tecnología, *ABC redes*, España, disponible en línea en

http://www.abc.es/tecnologia/redes/abci-zuckerberg-recula-facebook-si-medio-comunicacion-201612222024_noticia.html, link consultado el 16 de mayo de 2017.

MENDOZA, Miguel Ángel, “El derecho a la privacidad en la era digital”, *welivesecurity by eset*, 2 de marzo de 2017, disponible en línea en <https://www.welivesecurity.com/la-es/2017/03/02/derecho-a-la-privacidad-era-digital/>, link consultado el 23 de octubre de 2017.

OFICINA DE SEGURIDAD DEL INTERNAUTA, BLOG, “Cómo puedo denunciar una suplantación de identidad en Internet”, publicado el 14 de mayo de 2014, disponible en línea en <https://www.osi.es/es/actualidad/blog/2014/05/14/como-denunciar-una-suplantacion-de-identidad-en-internet>, link consultado el 3 de mayo de 2017.

OMICRONO, “Cuales (sic) son los peligros reales de utilizar redes WiFi públicas y cómo prevenirlos” 14 de mayo de 2015, disponible en línea en <http://omicro.no.elespanol.com/2015/05/peligros-de-utilizar-redes-wifi-publicas/>, link visitado el 10 de septiembre de 2017.

PAGNOTTA, Sabrina, “¿iPhone 6 gratis? Ten cuidado con los últimos scams”, *welivesecurity*, disponible en línea en <https://www.welivesecurity.com/la-es/2014/09/17/iphone-6-gratis-cuidado-ultimos-scams/>, link consultado el 29 de octubre de 2018.

POLICÍA FEDERAL, Acciones y Programas, “Trata de personas en el marco de operaciones encubiertas”, disponible en línea en <https://www.gob.mx/policiafederal/acciones-y-programas/trata-de-personas-en-el-marco-de-operaciones-encubiertas>, link visitado el 23 de octubre de 2017.

Presidencia de la República México “Recomendaciones para evitar ser víctima de trata de personas”, en línea 30 de julio de 2015 <https://www.gob.mx/presidencia/articulos/recomendaciones-para-evitar-ser-victima-de-trata-de-personas>, link visitado el 13 de septiembre de 2017.

ROBLES MONTOYA, Benjamín, citando *El derecho a la identidad como derecho humano*, enero de 2011, versión electrónica: disponible en línea en http://www.senado.gob.mx/64/gaceta_del_senado/documento/73846, link visitado el 22 de octubre de 2018.

RT, ¿Por qué Zuckerberg tapa la cámara y el micrófono de su ordenador?, 27 de junio de 2016, disponible en línea en <https://actualidad.rt.com/actualidad/211460-zuckerberg-tapar-camara-microfono-laptop>, link visitado el 9 de septiembre de 2017.

S/A, “El protocolo HTTPS no garantiza la seguridad”, *Kaspersky*, 17 de enero de 2018, disponible en línea en el link <https://latam.kaspersky.com/blog/https-does-not-mean-safe/12331/>, consultado por última ocasión el 19 de noviembre de 2018.

S/A, “¿Qué significa el protocolo HTTPS y cómo funciona?”, *Intenet Lab* disponible en línea 29/ de enero de 2010 disponible en línea en <https://www.internetlab.es/post/888/que-significa-el-protocolo-https-y-como-funciona/>, link visitado el 9 de septiembre de 20117.

S/A, “14 Estudio sobre los hábitos de los usuarios de Internet en México 2018”, *Asociación de Internet. Mx*, disponible en línea en <https://www.asociaciondeinternet.mx/es/component/remository/Habitos-de-Internet/14-Estudio-sobre-los-Habitos-de-los-usuarios-de-Internet-en-Mexico-2018/lang,es-es/?Itemid=>, link consultado el 30 de octubre de 2018.

S/A, Diccionario de la lengua española de la Real Academia Española, “Privacidad”, disponible en línea <http://dle.rae.es/?id=UD4g0KW> link visitado el 9 de septiembre de 2017.

S/A, Diccionario de la Real Academia Española del vocablo latín *identitas*, disponible en línea <http://dle.rae.es/srv/fetch/fetch?id=bCI7km6>, link consultado el 3 de mayo de 2017.

S/A, Diccionario de la Real Academia Española, definición de “Intimidad” disponible en línea en <http://dle.rae.es/?id=LyCn6I9>, link visitado el 9 de septiembre de 2017.

S/A, Diccionario Oxford en español, “Internauta”, en línea en <https://es.oxforddictionaries.com/definicion/internauta>, link visitado el 13 de septiembre de 2017.

S/A, Facebook Notes, Fundación María de los Ángeles, “Trata de personas, métodos de reclutamiento”, en línea <https://www.facebook.com/notes/fundaci%C3%B3n-mar%C3%ADa-de-los->

%C3%A1ngeles/trata-de-personas-m%C3%A9todos-de-reclutamiento/154776674564328/, link visitado 13 de septiembre de 2017.

S/A, *internetpasoapaso.com*, de Granada en España, disponible en <https://internetpasoapaso.com/que-es-una-actualizacion/>.

S/A, Kaspersky Lab, “¿qué es el pharming y cómo evitarlo?”, disponible en <https://latam.kaspersky.com/resource-center/definitions/pharming>, última fecha de consulta el 19 de noviembre de 2018.

S/A, La historia de AOL Instant Messenger, se encuentra disponible en Wikipedia, disponible en línea en https://es.wikipedia.org/wiki/AOL_Instant_Messenger, link consultado el 2 de mayo de 2017.

S/A, La historia de Facebook adelanta a MySpace como red social líder, disponible en línea en <https://www.ecured.cu/Myspace>, link consultado el 2 de mayo de 2017.

S/A, La historia de Facebook, disponible en línea en la página oficial de Facebook en <https://newsroom.fb.com/company-info/>, link consultado el 2 de mayo de 2017.

S/A, La historia de MySpace, disponible en línea en http://www.laccei.org/LACCEI2010-Peru/published/TTL146_SanMartin.pdf, link consultado el 2 de mayo de 2017.

S/A, La historia de Sixdegrees.com, puede consultarse en su página oficial en Sixdegrees.com, disponible en línea en <http://sixdegrees.com/>, link consultado el 2 de mayo de 2017.

S/A, La historia de theglobe.com puede ser consultada en su página oficial: theglobe.com, disponible en línea <http://www.theglobe.com/>, link consultado el 2 de mayo de 2017. Texto en idioma inglés.

S/A, La historia de Twitter, disponible en línea en http://www.cad.com.mx/historia_de_twitter.htm, link consultado el 2 de mayo de 2017.

S/A, La historia del portal Friendster, disponible en línea en <http://timerime.com/es/evento/2530833/Se+lanza+el+portal+Friendster/>, link consultado el 2 de mayo de 2017.

S/A, Legálitas, “La usurpación de identidad”, 1 de julio de 2015, disponible en línea en <https://www.legalitas.com/pymes-autonomos/actualidad/articulos-juridicos/contenidos/La-usurpacion-de-identidad>, link visitado el 25 de octubre de 2018.

S/A, Legálitas, “Suplantación de Identidad”, 3 de marzo de 2016, disponible en línea en <https://www.legalitas.com/actualidad/suplantacion-de-identidad>, link visitado el 9 de septiembre de 2017.

S/A, Noticias ONU, “Crecer en el mundo digital: Cómo internet afecta al bienestar y seguridad de los niños”, 11 de diciembre de 2017, disponible en línea en <https://news.un.org/es/story/2017/12/1423682#.WILaKhP1XfY>, link consultado el 11 de diciembre de 2017.

S/A, Universia España, “5 consejos para cuidar tu identidad digital en Internet”, 14 de julio de 2016, disponible en línea en <http://noticias.universia.es/ciencia-tecnologia/noticia/2016/07/14/1141808/5-consejos-cuidar-identidad-digital-internet.html>, link visitado el 10 de septiembre de 2017.

Secretaría de Gobernación, Elementos de la trata de personas, disponible en http://www.gobernacion.gob.mx/es_mx/SEGOB/Elementos_de_la_Trata_de_Personas, link consultado el 4 de noviembre de 2018.

SIMPSON, David y BROWN, Pamela, “NSA mines Facebook for connections, including Americans' profiles”, *CNN.com* (en inglés). Disponible en http://edition.cnn.com/2013/09/30/us/nsa-social-networks/index.html?hpt=ibu_c2 link consultado el 4 de mayo de 2017.

Statista.com, “Ranking mundial de los 10 países con más usuarios de Facebook a la fecha de abril de 2018”, portal de estadísticas, disponible en línea en <https://es.statista.com/estadisticas/518638/ranking-de-los-paises-con-mas-usuarios-de-facebook-a-nivel-mundial/>, link consultado el 30 de octubre de 2018.

TEMPERINI, Marcelo G.I., y MACEDO, Maximiliano, “La problemática de los perfiles falsos en Facebook y su relación con el Cibercrimen”, *SID 2015*, 15o.

Simposio Argentino de Informática y Derecho, p. 196, disponible en línea en <http://44jaiio.sadio.org.ar/sites/default/files/sid185-198.pdf>, link consultado el 29 de octubre de 2018.

TORRES, Rubén y MONROY, Jorge, “México, sin cifras precisas sobre trata”, *El economista*, México, disponible en línea en <https://www.eleconomista.com.mx/politica/Mexico-sin-cifras-precisas-sobre-trata-20170730-0073.html>. Link visitado el 23 de octubre de 2017.

UNAM-CERT, “Robo de Identidad y Consecuencias Sociales”, 25 de octubre de 2010, disponible en línea en <https://www.cert.org.mx/historico/documento/index.html-id=16> link visitado el 9 de septiembre de 2017.

V. P., “Roban la identidad de una menor en internet y escriben frases ofensivas”, en *Diario Información*, disponible en <https://www.diarioinformacion.com/elda/2017/04/05/roban-identidad-menor-internet-escriben/1880013.html>, link consultado por última ocasión el 19 de noviembre de 2018.

WIKIPEDIA, “Privacidad en Internet”, tomado de disponible en línea en https://es.wikipedia.org/wiki/Privacidad_en_Internet, link visitado el 9 de septiembre de 2017.

WIKIPEDIA, “Privacidad”, disponible en línea en <https://es.wikipedia.org/wiki/Privacidad>, link visitado el 9 de septiembre de 2017.

WIKIPEDIA, Identidad 2.0, disponible en línea en https://es.wikipedia.org/wiki/Identidad_2.0, link consultado el 22 de octubre de 2018.

WIKIPEDIA, Trata de personas, disponible en línea https://es.wikipedia.org/wiki/Trata_de_personas, link consultado el 4 de mayo de 2017.

Normatividad

13º Congreso de las Naciones Unidas sobre Prevención del Delito y Justicia.

Acuerdo Internacional para la Supresión del Tráfico de Trata de Blancas, firmado en París el 18 de mayo de 1904, enmendado por el Protocolo firmado en Lake Success, Nueva York, el 4 de mayo de 1949.

Boletín núm. 2661, “Delito de usurpación de identidad será castigado con uno a seis años de prisión”, 29 de noviembre de 2016, Cámara de Diputados del H. Congreso de la Unión.

Código Penal Federal

Comunicado 017 de la Secretaría de Hacienda y Crédito Público, del 1º de marzo 2018, “El Congreso de la Unión aprueba la “Ley FinTech”.

Constitución Política de los Estados Unidos Mexicanos

Convención Internacional Relativa a la Represión de la Trata de Mujeres Mayores de Edad.

Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional y su Protocolos.

Declaración Interamericana para Enfrentar la Trata de Personas “Declaración de Brasilia”, 5 de diciembre de 2014

Declaración Universal de Derechos Humanos.

Economic and Social Council, Commission on Crime Prevention and Criminal Justice, International cooperation in the prevention, investigation, prosecution and punishment of fraud, the criminal misuse and falsification of identity and related crimes.

Ley Federal de Protección de Datos Personales en Posesión de los Particulares.

Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

Ley General para Prevenir, Sancionar y Erradicar los Delitos en Materia de Trata de Personas y para la Protección y Asistencia a la Víctimas de estos Delitos

Ley No. 53-07 sobre Crímenes y Delitos de Alta Tecnología.

Ley para Prevenir y Sancionar la Trata de Personas.

Plan Nacional para Prevenir y Sancionar la trata de Personas, 2014-2018.

“Proclamación de Teherán” de 1968, adoptada en la Conferencia Internacional de Derechos Humanos.

Resolución 3384 de 10 de noviembre de 1975, “Declaración sobre la Utilización del Progreso Científico y Tecnológico en Interés de la Paz y en Beneficio de la Humanidad”, adoptada por la Asamblea General de la ONU.

Resolución 57/239 Relativa a la Creación de una Cultura Mundial de Seguridad Cibernética.

Resolución 58/199 sobre Creación de una Cultura Mundial de Seguridad Cibernética y Protección de las Infraestructuras de Información Esenciales.

Resoluciones 55/63 y 56/121 de la Asamblea General de las Naciones Unidas sobre la Lucha contra la Utilización de la Tecnología de la Información con Fines Delictivos.

Semanario Judicial de la Federación y su Gaceta, Novena Época, t. XI, abril de 2000, Tesis P. LX/2000, página 74, bajo el Rubro: Derecho a la información. Su ejercicio se encuentra limitado tanto por los intereses nacionales y de la sociedad, como por los derechos de terceros.

Semanario Judicial de la Federación y su Gaceta, Décima Época, 31 de agosto de 2018. Tesis Aislada 1ª XCVI/2018, bajo el Rubro: Interés superior del menor y derecho a la identidad. La ausencia de vínculo biológico en la relación paterno-filial no es suficiente para sustentar la impugnación de paternidad.

Semanario Judicial de la Federación y su Gaceta, Décima Época, 30 de junio de 2017. Tesis Aislada 1ª LXXIII/2017, bajo el Rubro: Derecho a la Identidad de los menores. Injerencia en la realidad social.

Semanario Judicial de la Federación y su Gaceta, Novena Época, 1 de septiembre de 2011. Tesis Aislada 1ª CXV/2011, página 1034, bajo el Rubro: Derecho a la identidad de los niños.

Hemerografía

ALCÁNTARA, Beatriz, “Adolescente que hackeó a la CIA y al FBI tendrá que pagarlo muy caro”, *Urban Tecno*, Tecnología, 22 de abril de 2018.

APARICI, Roberto y OSUNA ACEDO, Sara, “La cultura de la participación”. *Revista Mediterránea de Comunicación*, vol. 2, no. 2, 2013.

AVENDAÑO, Susana, “Una Extraña estadística en Facebook”, *Unocero*, 29 de marzo de 2017.

AVILÉS, Karina, "México, tercer lugar mundial en número de afectados por cibercriminales, revela estudio", *La Jornada*, Política, 29 de enero de 2014.

BADSHAH, Nadeem, "Facebook to contact 87 million users affected by data breach", *The Guardian*, 8 de abril de 2018.

CALDERÓN BETALLELUZ, Víctor Manuel, "La necesidad de toda organización de contar con Proyectos de Inversión, Universidad San Martín De Porres, Perú, *Revista del Centro de Derecho y Economía*, febrero 2012.

CAMARILLO CORTÉS, Mario D., "Robo de identidad, delito al alza y sin estadísticas en el mundo", *Cronica.com.mx*, 29 de enero de 2014.

CARBELLIDO MONZÓ, Carlos, "Identidad digital, reputación on line, el derecho al olvido y cómo borrar contenido de Internet", en *community manager*, consultor de marketing digital, 23 de enero de 2018.

CHAMORRO LUSAR, Andrés, *et al.*, "Gestión de la privacidad de los perfiles de Facebook de adolescentes", en *Revista de Medios de Educación*, núm. 48, enero 2016.

CORTÉS GARCÍA, Rosa "La usurpación en redes sociales: casos reales", *Inventtatte*, 13 de julio de 2015

DE ROSELLÓ MORENO, Rocío, "Usurpación vs suplantación de la identidad", *Info Security News*, año 12, núm. 10, octubre 2016.

FUENTES, Mario Luis, "Trata de personas: jóvenes en riesgo", *Excelsior en línea*, disponible en línea en <http://www.excelsior.com.mx/nacional/2013/09/24/920068>, link consultado el 16 de mayo de 2017.

GONZÁLEZ, Noé, "Bauman, identidad y comunidad", *Espiral*, vol. 14, núm. 40, Guadalajara, septiembre- diciembre 2007.

HERNÁNDEZ, Leopoldo, "México, octavo país con mayor robo de identidad", *El Economista*, 29 de enero de 2016.

La redacción, "La Procuraduría CDMX abrió 3 mil 38 investigaciones por robo de identidad en 51 meses", *Proceso*, 2 de agosto de 2017

MARCÚS, Juliana, "Apuntes sobre el concepto de identidad", *Revista sociológica de Pensamiento crítico*, vol. 5, núm. 1, 2011.

ROMERO FLORES, Rodolfo, “El robo de identidad por medios informáticos o telemáticos: su tratamiento jurídico penal”, *Jurismática, El derecho y las nuevas tecnologías*, disponible en <https://archivos.juridicas.unam.mx/www/bjv/libros/6/2958/20.pdf>, link consultado el 4 de noviembre de 2018.

S/A, “El anonimato en las redes sociales podría tener los días contados”, *Diario la voz de Galicia*, 26 de diciembre de 2017.

S/A, “Policía Federal Detecta Suplantación en la identidad de instituciones y empresas para perjudicar a los usuarios”, *Boletín de Prensa*, núm. 131, 4 de junio de 2014.

SÁNCHEZ PÉREZ, Gabriel y ROJAS GONZÁLEZ, Isai, “Leyes de protección de datos personales en el mundo y la protección de datos biométricos. Parte I”, en *Revista .Seguridad* de la Dirección General de Tecnologías de Información y Comunicación de la Universidad Nacional Autónoma de México, núm. 13.

SÉNECA, Antonio, “Suplantación de identidad en internet, ¿por lo civil o lo penal?”, *Legal Today por y para abogados*, 11 de mayo de 2017.

SUN, “Mi otro yo en Facebook: usurpación de identidad”, *el Informador.mx*, 18 de junio de 2016.

SUPLIGUICHA, Verónica, Vásquez, Grace y Jácome, Paola, “Trata de personas: historias que invisibilizan verdades”, en *Ciudad Segura*, Programa Estudios de la Ciudad, FLACSO-Ecuador, núm. 36, 2009.

TAYLOR, Charles, *Fuentes del yo: La construcción de la identidad moderna*, Paidós Ibérica, Título original: Sources of self, the making of the modern identity en Zárate Ortiz, José Francisco, “La identidad como construcción social desde la propuesta de Charles Taylor” en *Eidos*, núm. 23, Barranquilla, julio-diciembre de 2015

TRUJANO RUIZ, Patricia, Dorantes Segura, Jessica y Trovilla Quesada, Vania, “Violencia en Internet: nuevas víctimas, nuevos retos”, *Liberabit*, vol. 15, núm. 1, Lima, enero-junio, 2009.

VELASCO, J. J., “Condiciones de Facebook: todo lo que aceptaste sin leer, explicado de forma clara”, *Hipertextual.com*, 6 de febrero de 2016

ZAMORA JIMÉNEZ, Arturo, "Por un marco legal para los delitos contra la identidad de las personas en México", *Revista del Instituto Belisario Domínguez*, vol. 6, núm. 28, 2016.

Videografía

Conferencia de identidad, ponentes el filósofo Darío Sztajnszrajber y el historiador Ezequiel Adamovsk, Ministerio de Ciencia Tecnología e Innovación Productiva en Argentina, disponible en <https://www.youtube.com/watch?v=ZP45ANGVST4>, link visitado el 22 de octubre de 2018.



Anexo

INFOGRAFÍA



Anexo e Infografía

Anexo I

SUPLANTACIÓN DE LA IDENTIDAD DIGITAL CON FINES DE TRATA DE PERSONAS EN FACEBOOK

INVESTIGACIÓN POR
EFRAÍN AGUILAR
INTEC

La trata de personas es un fenómeno que se va propagando y actualizando también con la evolución de la tecnología siendo cada vez más complejo. Es con el uso de las tecnologías y las identidades digitales que quedan expuestas en sitios como las redes sociales, que la suplantación es un delito que ha proliferado en particular el uso de los perfiles de Facebook que facilita la captura de víctimas con fines de trata.

Facebook permite a sus usuarios no sólo comunicarse, sino también compartir fotos, videos en línea y hasta revelar información personal, como el correo electrónico, la fecha de nacimiento, creencias religiosas o políticas, la suscripción laboral y el estado civil.

En México, **98%** de las personas que utilizan Internet tienen al menos una cuenta de Facebook.

Tiene **85 millones** de usuarios.

El tema es relevante para nosotros para poder alertar que esta red social está siendo utilizada con fines de trata de personas permitiendo ocasionar lo ilícito, que resulta para los delincuentes hacer uso de esta herramienta para captar a sus víctimas, específicamente a sus niñas y adolescentes vulnerables y confundidos con lo que respecta al manejo de la privacidad y la protección de sus datos.

LA TRATA DE PERSONAS ES:

El comercio ilegal de seres humanos con propósitos de esclavitud laboral, sexual, reproducción, explotación social, trabajo forzado, extracción de órganos o cualquier forma moderna de esclavitud contra la voluntad y el bienestar del ser humano.

Facebook es una empresa por medio de la cual se pretora una red social que es alimentada por los millones de usuarios alrededor del mundo que nacieron desde la página oficial de Facebook y en su mayoría propia, una cuenta denominada "perfil de usuario".

Los engañadores suelen hacer uso de plataformas y redes sociales utilizadas por niños y jóvenes que a través de ellas se comunican y en ocasiones lo hacen sin precaución o supervisión, lo que provoca que sean presas fáciles de los criminales de los delincuentes.

LAS SEÑALES QUE INDICAN QUE SE HA SIDO VÍCTIMA DE UN ROBO DE IDENTIDAD PUEDEN SER:

Intento de registros de información personal o datos de la red social en línea.	Intento de cambio de correo electrónico o número de teléfono.	Intento de cambio de dirección de correo electrónico.
Intento de cambio de contraseña de correo electrónico o de la red social.	Intento de cambio de contraseña de correo electrónico o de la red social.	Intento de cambio de contraseña de correo electrónico o de la red social.
Intento de cambio de contraseña de correo electrónico o de la red social.	Intento de cambio de contraseña de correo electrónico o de la red social.	Intento de cambio de contraseña de correo electrónico o de la red social.

SUPLANTACIÓN DE IDENTIDAD EN FB

Este actor ficticio es cada vez más común, de acuerdo a los datos sobre el robo de identidad del programa de seguridad ProSafe que indica que aproximadamente 50 millones de usuarios en México han sido afectados por el robo de identidad en un año 2017.

Debido a la gran cantidad de datos que se manejan en esta plataforma Facebook, Instagram y Snapchat, con un 40% de porcentaje de riesgo de que los usuarios sean suplantados.

Facebook usa un gran volumen de datos de Cambridge Analytica que desde a 17 millones de usuarios, dejó a disposición la identidad en la que los datos de usuarios pueden ser compartidos con los datos de los mismos para consumo de otros.

EL USO DE TÉCNICAS DE INGENIERÍA SOCIAL EN FB

Prototipo de ingeniería social debe tener un sentido previo de información de la víctima presentada para ser creída y utilizar un lenguaje amigable con el objetivo de persuadir a sus víctimas y obtener información. El atacante puede seleccionar una víctima específica de manera que aumente la probabilidad de conseguir información o los datos reales accede específicamente a su voluntad.

Shoulder surfing o espionaje por encima del hombro es una técnica derivada de la observación, la que consiste en estar en una posición cercana a los usuarios en redes de cerca, para obtener información confidencial. Solo basta con permanecer observado sigilosamente para la mayoría de la víctima las cosas que digan al momento o cualquier otra forma de información que pueda ser de interés para obtener información. Esto incluye su estado de conciencia para obtener correo electrónico, números PIN, códigos de seguridad y datos similares.

Dumpster diving es una técnica que se centra en buscar información valiosa en la basura. Tener cualquier tipo de documentos en un depósito de desechos es un práctica que puede resultar riesgosa para ser pueden recuperar de la basura datos importantes contenidos en documentos desechados sin ser destruidos previamente.

Asalto al buzón de correo es un delito cometido en el momento de la corrección que se enciende en los buzones de correo sin registrar los datos se pueden usar documentos con información valiosa (códigos de cuentas bancarias o de tarjetas de crédito, o cualquier otro documento).

PROPUESTAS PARA EVITAR LA USURPACIÓN DE IDENTIDAD Y DETENER LA TRATA DE PERSONAS POR MEDIO DE FACEBOOK

1. No revelar nuestros nombres en su lugar usar alias o seudónimos en nuestros distintos redes sociales.
2. Usar distantes conversaciones en las distintas redes y cambiarlos con cierta periodicidad.
3. Entender los términos de adhesión que están llenos de palabras y frases de Internet en general en como sus condiciones de uso antes de aceptarlas.
4. Revisar cómo se debe de configurar la privacidad de la red que se utiliza y elegir siempre la configuración más alta aunque eso signifique no recibir notificaciones o perder "beneficios".
5. No involucrarse con personas desconocidas, en redes sociales se siempre sea en entornos públicos y mucho menos en lugares distantes o secretos.
6. No cargar información personal como edad, dirección, código en el que estamos en relaciones familiares, no permitir que sus contactos se conecten entre sí.
7. No acceder a sitios que sean sospechosos o no seguros como pueden ser páginas de juegos gratuitos, casinos, ofertas de trabajo, páginas que ofrecen ganar ciertos premios solo por completar encuestas.
8. No aceptar llenar formularios en los que tengamos que dar los datos.
9. Por ningún motivo compartir contraseñas.
10. Cuando te encuentres navegando por la red y se abran ventanas emergentes o sea el navegador con programas, nunca descargues archivos o accedas a vínculos que te sugieran.
11. Si tienes una cámara de cámara de seguridad y llega a recibir correos de mensajes desconfiados o en idiomas extranjeros simplemente elimínalos, en los últimos muchos usuarios se han visto afectados por correos desconocidos.
12. En la medida de lo posible trata de no utilizar redes WiFi abiertas, no accedes a sus cuentas de correo electrónico o redes sociales en computadores que sean de uso público o de otros de que los hijos, servicios de correo los usuarios de Internet los cambian para que la cuenta y contraseña no se guarden de manera automática y así puedan acceder fácilmente.
13. Mantén actualizados los antivirus y anti-spam.

Fuentes de la Investigación

United Photo, como identificar a través de correos, 4 de septiembre de 2017, disponible en: <http://www.unitedphoto.com/2017/09/04/como-identificar-a-traves-de-correos/>.
 El fraude digital, cómo prevenir y evitar estafas online, disponible en: <http://www.el fraude digital.com/2017/09/04/como-prevenir-y-evitar-estafas-online/>.
 El fraude digital, cómo prevenir y evitar estafas online, disponible en: <http://www.el fraude digital.com/2017/09/04/como-prevenir-y-evitar-estafas-online/>.
 El fraude digital, cómo prevenir y evitar estafas online, disponible en: <http://www.el fraude digital.com/2017/09/04/como-prevenir-y-evitar-estafas-online/>.
 El fraude digital, cómo prevenir y evitar estafas online, disponible en: <http://www.el fraude digital.com/2017/09/04/como-prevenir-y-evitar-estafas-online/>.
 El fraude digital, cómo prevenir y evitar estafas online, disponible en: <http://www.el fraude digital.com/2017/09/04/como-prevenir-y-evitar-estafas-online/>.
 El fraude digital, cómo prevenir y evitar estafas online, disponible en: <http://www.el fraude digital.com/2017/09/04/como-prevenir-y-evitar-estafas-online/>.
 El fraude digital, cómo prevenir y evitar estafas online, disponible en: <http://www.el fraude digital.com/2017/09/04/como-prevenir-y-evitar-estafas-online/>.
 El fraude digital, cómo prevenir y evitar estafas online, disponible en: <http://www.el fraude digital.com/2017/09/04/como-prevenir-y-evitar-estafas-online/>.
 El fraude digital, cómo prevenir y evitar estafas online, disponible en: <http://www.el fraude digital.com/2017/09/04/como-prevenir-y-evitar-estafas-online/>.
 El fraude digital, cómo prevenir y evitar estafas online, disponible en: <http://www.el fraude digital.com/2017/09/04/como-prevenir-y-evitar-estafas-online/>.
 El fraude digital, cómo prevenir y evitar estafas online, disponible en: <http://www.el fraude digital.com/2017/09/04/como-prevenir-y-evitar-estafas-online/>.
 El fraude digital, cómo prevenir y evitar estafas online, disponible en: <http://www.el fraude digital.com/2017/09/04/como-prevenir-y-evitar-estafas-online/>.
 El fraude digital, cómo prevenir y evitar estafas online, disponible en: <http://www.el fraude digital.com/2017/09/04/como-prevenir-y-evitar-estafas-online/>.
 El fraude digital, cómo prevenir y evitar estafas online, disponible en: <http://www.el fraude digital.com/2017/09/04/como-prevenir-y-evitar-estafas-online/>.
 El fraude digital, cómo prevenir y evitar estafas online, disponible en: <http://www.el fraude digital.com/2017/09/04/como-prevenir-y-evitar-estafas-online/>.
 El fraude digital, cómo prevenir y evitar estafas online, disponible en: <http://www.el fraude digital.com/2017/09/04/como-prevenir-y-evitar-estafas-online/>.
 El fraude digital, cómo prevenir y evitar estafas online, disponible en: <http://www.el fraude digital.com/2017/09/04/como-prevenir-y-evitar-estafas-online/>.
 El fraude digital, cómo prevenir y evitar estafas online, disponible en: <http://www.el fraude digital.com/2017/09/04/como-prevenir-y-evitar-estafas-online/>.
 El fraude digital, cómo prevenir y evitar estafas online, disponible en: <http://www.el fraude digital.com/2017/09/04/como-prevenir-y-evitar-estafas-online/>.
 El fraude digital, cómo prevenir y evitar estafas online, disponible en: <http://www.el fraude digital.com/2017/09/04/como-prevenir-y-evitar-estafas-online/>.
 El fraude digital, cómo prevenir y evitar estafas online, disponible en: <http://www.el fraude digital.com/2017/09/04/como-prevenir-y-evitar-estafas-online/>.
 El fraude digital, cómo prevenir y evitar estafas online, disponible en: <http://www.el fraude digital.com/2017/09/04/como-prevenir-y-evitar-estafas-online/>.
 El fraude digital, cómo prevenir y evitar estafas online, disponible en: <http://www.el fraude digital.com/2017/09/04/como-prevenir-y-evitar-estafas-online/>.
 El fraude digital, cómo prevenir y evitar estafas online, disponible en: <http://www.el fraude digital.com/2017/09/04/como-prevenir-y-evitar-estafas-online/>.
 El fraude digital, cómo prevenir y evitar estafas online, disponible en: <http://www.el fraude digital.com/2017/09/04/como-prevenir-y-evitar-estafas-online/>.
 El fraude digital, cómo prevenir y evitar estafas online, disponible en: <http://www.el fraude digital.com/2017/09/04/como-prevenir-y-evitar-estafas-online/>.
 El fraude digital, cómo prevenir y evitar estafas online, disponible en: <http://www.el fraude digital.com/2017/09/04/como-prevenir-y-evitar-estafas-online/>.
 El fraude digital, cómo prevenir y evitar estafas online, disponible en: <http://www.el fraude digital.com/2017/09/04/como-prevenir-y-evitar-estafas-online/>.
 El fraude digital, cómo prevenir y evitar estafas online, disponible en: <http://www.el fraude digital.com/2017/09/04/como-prevenir-y-evitar-estafas-online/>.
 El fraude digital, cómo prevenir y evitar estafas online, disponible en: <http://www.el fraude digital.com/2017/09/04/como-prevenir-y-evitar-estafas-online/>.
 El fraude digital, cómo prevenir y evitar estafas online, disponible en: <http://www.el fraude digital.com/2017/09/04/como-prevenir-y-evitar-estafas-online/>.
 El fraude digital, cómo prevenir y evitar estafas online, disponible en: <http://www.el fraude digital.com/2017/09/04/como-prevenir-y-evitar-estafas-online/>.
 El fraude digital, cómo prevenir y evitar estafas online, disponible en: <http://www.el fraude digital.com/2017/09/04/como-prevenir-y-evitar-estafas-online/>.
 El fraude digital, cómo prevenir y evitar estafas online, disponible en: <http://www.el fraude digital.com/2017/09/04/como-prevenir-y-evitar-estafas-online/>.
 El fraude digital, cómo prevenir y evitar estafas online, disponible en: <http://www.el fraude digital.com/2017/09/04/como-prevenir-y-evitar-estafas-online/>.
 El fraude digital, cómo prevenir y evitar estafas online, disponible en: <http://www.el fraude digital.com/2017/09/04/como-prevenir-y-evitar-estafas-online/>.
 El fraude digital, cómo prevenir y evitar estafas online, disponible en: <http://www.el fraude digital.com/2017/09/04/como-prevenir-y-evitar-estafas-online/>.
 El fraude digital, cómo prevenir y evitar estafas online, disponible en: <http://www.el fraude digital.com/2017/09/04/como-prevenir-y-evitar-estafas-online/>.
 El fraude digital, cómo prevenir y evitar estafas online, disponible en: <http://www.el fraude digital.com/2017/09/04/como-prevenir-y-evitar-estafas-online/>.
 El fraude digital, cómo prevenir y evitar estafas online, disponible en: <http://www.el fraude digital.com/2017/09/04/como-prevenir-y-evitar-estafas-online/>.
 El fraude digital, cómo prevenir y evitar estafas online, disponible en: <http://www.el fraude digital.com/2017/09/04/como-prevenir-y-evitar-estafas-online/>.
 El fraude digital, cómo prevenir y evitar estafas online, disponible en: <http://www.el fraude digital.com/2017/09/04/como-prevenir-y-evitar-estafas-online/>.
 El fraude digital, cómo prevenir y evitar estafas online, disponible en: <http://www.el fraude digital.com/2017/09/04/como-prevenir-y-evitar-estafas-online/>.
 El fraude digital, cómo prevenir y evitar estafas online, disponible en: <http://www.el fraude digital.com/2017/09/04/como-prevenir-y-evitar-estafas-online/>.
 El fraude digital, cómo prevenir y evitar estafas online, disponible en: <http://www.el fraude digital.com/2017/09/04/como-prevenir-y-evitar-estafas-online/>.
 El fraude digital, cómo prevenir y evitar estafas online, disponible en: <http://www.el fraude digital.com/2017/09/04/como-prevenir-y-evitar-estafas-online/>.
 El fraude digital, cómo prevenir y evitar estafas online, disponible en: <http://www.el fraude digital.com/2017/09/04/como-prevenir-y-evitar-estafas-online/>.
 El fraude digital, cómo prevenir y evitar estafas online, disponible en: <http://www.el fraude digital.com/2017/09/04/como-prevenir-y-evitar-estafas-online/>.
 El fraude digital, cómo prevenir y evitar estafas online, disponible en: <http://www.el fraude digital.com/2017/09/04/como-prevenir-y-evitar-estafas-online/>.
 El fraude digital, cómo prevenir y evitar estafas online, disponible en: <http://www.el fraude digital.com/2017/09/04/como-prevenir-y-evitar-estafas-online/>.
 El fraude digital, cómo prevenir y evitar estafas online, disponible en: <http://www.el fraude digital.com/2017/09/04/como-prevenir-y-evitar-estafas-online/>.
 El fraude digital, cómo prevenir y evitar estafas online, disponible en: <http://www.el fraude digital.com/2017/09/04/como-prevenir-y-evitar-estafas-online/>.
 El fraude digital, cómo prevenir y evitar estafas online, disponible en: <http://www.el fraude digital.com/2017/09/04/como-prevenir-y-evitar-estafas-online/>.
 El fraude digital, cómo prevenir y evitar estafas online, disponible en: <http://www.el fraude digital.com/2017/09/04/como-prevenir-y-evitar-estafas-online/>.
 El fraude digital, cómo prevenir y evitar estafas online, disponible en: <http://www.el fraude digital.com/2017/09/04/como-prevenir-y-evitar-estafas-online/>.
 El fraude digital, cómo prevenir y evitar estafas online, disponible en: <http://www.el fraude digital.com/2017/09/04/como-prevenir-y-evitar-estafas-online/>.
 El fraude digital, cómo prevenir y evitar estafas online, disponible en: <http://www.el fraude digital.com/2017/09/04/como-prevenir-y-evitar-estafas-online/>.
 El fraude digital, cómo prevenir y evitar estafas online, disponible en: <http://www.el fraude digital.com/2017/09/04/como-prevenir-y-evitar-estafas-online/>.
 El fraude digital, cómo prevenir y evitar estafas online, disponible en: <http://www.el fraude digital.com/2017/09/04/como-prevenir-y-evitar-estafas-online/>.
 El fraude digital, cómo prevenir y evitar estafas online, disponible en: <http://www.el fraude digital.com/2017/09/04/como-prevenir-y-evitar-estafas-online/>.
 El fraude digital, cómo prevenir y evitar estafas online, disponible en: <http://www.el fraude digital.com/2017/09/04/como-prevenir-y-evitar-estafas-online/>.
 El fraude digital, cómo prevenir y evitar estafas online, disponible en: <http://www.el fraude digital.com/2017/09/04/como-prevenir-y-evitar-estafas-online/>.
 El fraude digital, cómo prevenir y evitar estafas online, disponible en: <http://www.el fraude digital.com/2017/09/04/como-prevenir-y-evitar-estafas-online/>.
 El fraude digital, cómo prevenir y evitar estafas online, disponible en: <http://www.el fraude digital.com/2017/09/04/como-prevenir-y-evitar-estafas-online/>.
 El fraude digital, cómo prevenir y evitar estafas online, disponible en: <http://www.el fraude digital.com/2017/09/04/como-prevenir-y-evitar-estafas-online/>.
 El fraude digital, cómo prevenir y evitar estafas online, disponible en: <http://www.el fraude digital.com/2017/09/04/como-prevenir-y-evitar-estafas-online/>.
 El fraude digital, cómo prevenir y evitar estafas online, disponible en: <http://www.el fraude digital.com/2017/09/04/como-prevenir-y-evitar-estafas-online/>.
 El fraude digital, cómo prevenir y evitar estafas online, disponible en: <http://www.el fraude digital.com/2017/09/04/como-prevenir-y-evitar-estafas-online/>.
 El fraude digital, cómo prevenir y evitar estafas online, disponible en: <http://www.el fraude digital.com/2017/09/04/como-prevenir-y-evitar-estafas-online/>.
 El fraude digital, cómo prevenir y evitar estafas online, disponible en: <http://www.el fraude digital.com/2017/09/04/como-prevenir-y-evitar-estafas-online/>.
 El fraude digital, cómo prevenir y evitar estafas online, disponible en: <http://www.el fraude digital.com/2017/09/04/como-prevenir-y-evitar-estafas-online/>.
 El fraude digital, cómo prevenir y evitar estafas online, disponible en: <http://www.el fraude digital.com/2017/09/04/como-prevenir-y-evitar-estafas-online/>.
 El fraude digital, cómo prevenir y evitar estafas online, disponible en: <http://www.el fraude digital.com/2017/09/04/como-prevenir-y-evitar-estafas-online/>.
 El fraude digital, cómo prevenir y evitar estafas online, disponible en: <http://www.el fraude digital.com/2017/09/04/como-prevenir-y-evitar-estafas-online/>.
 El fraude digital, cómo prevenir y evitar estafas online, disponible en: <http://www.el fraude digital.com/2017/09/04/como-prevenir-y-evitar-estafas-online/>.
 El fraude digital, cómo prevenir y evitar estafas online, disponible en: <http://www.el fraude digital.com/2017/09/04/como-prevenir-y-evitar-estafas-online/>.
 El fraude digital, cómo prevenir y evitar estafas online, disponible en: <http://www.el fraude digital.com/2017/09/04/como-prevenir-y-evitar-estafas-online/>.
 El fraude digital, cómo prevenir y evitar estafas online, disponible en: <http://www.el fraude digital.com/2017/09/04/como-prevenir-y-evitar-estafas-online/>.
 El fraude digital, cómo prevenir y evitar estafas online, disponible en: <http://www.el fraude digital.com/2017/09/04/como-prevenir-y-evitar-estafas-online/>.
 El fraude digital, cómo prevenir y evitar estafas online, disponible en: <http://www.el fraude digital.com/2017/09/04/como-prevenir-y-evitar-estafas-online/>.
 El fraude digital, cómo prevenir y evitar estafas online, disponible en: <http://www.el fraude digital.com/2017/09/04/como-prevenir-y-evitar-estafas-online/>.
 El fraude digital, cómo prevenir y evitar estafas online, disponible en: <http://www.el fraude digital.com/2017/09/04/como-prevenir-y-evitar-estafas-online/>.
 El fraude digital, cómo prevenir y evitar estafas online, disponible en: <http://www.el fraude digital.com/2017/09/04/como-prevenir-y-evitar-estafas-online/>.
 El fraude digital, cómo prevenir y evitar estafas online, disponible en: <http://www.el fraude digital.com/2017/09/04/como-prevenir-y-evitar-estafas-online/>.
 El fraude digital, cómo prevenir y evitar estafas online, disponible en: <http://www.el fraude digital.com/2017/09/04/como-prevenir-y-evitar-estafas-online/>.
 El fraude digital, cómo prevenir y evitar estafas online, disponible en: <http://www.el fraude digital.com/2017/09/04/como-prevenir-y-evitar-estafas-online/>.
 El fraude digital, cómo prevenir y evitar estafas online, disponible en: <http://www.el fraude digital.com/2017/09/04/como-prevenir-y-evitar-estafas-online/>.
 El fraude digital, cómo prevenir y evitar estafas online, disponible en: <http://www.el fraude digital.com/2017/09/04/como-prevenir-y-evitar-estafas-online/>.
 El fraude digital, cómo prevenir y evitar estafas online, disponible en: <http://www.el fraude digital.com/2017/09/04/como-prevenir-y-evitar-estafas-online/>.
 El fraude digital, cómo prevenir y evitar estafas online, disponible en: <http://www.el fraude digital.com/2017/09/04/como-prevenir-y-evitar-estafas-online/>.
 El fraude digital, cómo prevenir y evitar estafas online, disponible en: <http://www.el fraude digital.com/2017/09/04/como-prevenir-y-evitar-estafas-online/>.
 El fraude digital, cómo prevenir y evitar estafas online, disponible en: <http://www.el fraude digital.com/2017/09/04/como-prevenir-y-evitar-estafas-online/>.
 El fraude digital, cómo prevenir y evitar estafas online, disponible en: <http://www.el fraude digital.com/2017/09/04/como-prevenir-y-evitar-estafas-online/>.
 El fraude digital, cómo prevenir y evitar estafas online, disponible en: <http://www.el fraude digital.com/2017/09/04/como-prevenir-y-evitar-estafas-online/>.
 El fraude digital, cómo prevenir y evitar estafas online, disponible en: <http://www.el fraude digital.com/2017/09/04/como-prevenir-y-evitar-estafas-online/>.
 El fraude digital, cómo prevenir y evitar estafas online, disponible en: <http://www.el fraude digital.com/2017/09/04/como-prevenir-y-evitar-estafas-online/>.
 El fraude digital, cómo prevenir y evitar estafas online, disponible en: <http://www.el fraude digital.com/2017/09/04/como-prevenir-y-evitar-estafas-online/>.
 El fraude digital, cómo prevenir y evitar estafas online, disponible en: <http://www.el fraude digital.com/2017/09/04/como-prevenir-y-evitar-estafas-online/>.
 El fraude digital, cómo prevenir y evitar estafas online, disponible en: <http://www.el fraude digital.com/2017/09/04/como-prevenir-y-evitar-estafas-online/>.
 El fraude digital, cómo prevenir y evitar estafas online, disponible en: <http://www.el fraude digital.com/2017/09/04/como-prevenir-y-evitar-estafas-online/>.
 El fraude digital, cómo prevenir y evitar estafas online, disponible en: <http://www.el fraude digital.com/2017/09/04/como-prevenir-y-evitar-estafas-online/>.
 El fraude digital, cómo prevenir y evitar estafas online, disponible en: <http://www.el fraude digital.com/2017/09/04/como-prevenir-y-evitar-estafas-online/>.
 El fraude digital, cómo prevenir y evitar estafas online, disponible en: <http://www.el fraude digital.com/2017/09/04/como-prevenir-y-evitar-estafas-online/>.
 El fraude digital, cómo prevenir y evitar estafas online, disponible en: <http://www.el fraude digital.com/2017/09/04/como-prevenir-y-evitar-estafas-online/>.
 El fraude digital, cómo prevenir y evitar estafas online, disponible en: <http://www.el fraude digital.com/2017/09/04/como-prevenir-y-evitar-estafas-online/>.
 El fraude digital, cómo prevenir y evitar estafas online, disponible en: <http://www.el fraude digital.com/2017/09/04/como-prevenir-y-evitar-estafas-online/>.
 El fraude digital, cómo prevenir y evitar estafas online, disponible en: <http://www.el fraude digital.com/2017/09/04/como-prevenir-y-evitar-estafas-online/>.
 El fraude digital, cómo prevenir y evitar estafas online, disponible en: <http://www.el fraude digital.com/2017/09/04/como-prevenir-y-evitar-estafas-online/>.
 El fraude digital, cómo prevenir y evitar estafas online, disponible en: <http://www.el fraude digital.com/2017/09/04/como-prevenir-y-evitar-estafas-online/>.
 El fraude digital, cómo prevenir y evitar estafas online, disponible en: [http://www.el fraude digital.com/2017/0](http://www.el fraude digital.com/2017/09/04/como-prevenir-y-evitar-estafas-online/)