Universidad Autónoma de Querétaro
Facultad de Derecho
Licenciatura en Criminología

SOCIEDAD DE LA INFORMACIÓN Y NUEVAS FORMAS DE VICTIMIZACIÓN

Tesis
Que como parte de los requisitos para obtener el grado de

Licenciatura en Criminología

Presentan:
María Yajaira Alvarez Monjaraz
María Guadalupe Balderas Méndez

Centro Universitario, febrero 2023

SOCIEDAD DE LA INFORMACIÓN Y NUEVAS FORMAS DE VICTIMIZACIÓN

por

María Guadalupe Balderas Méndez

Maria Yajaira Alvarez Monjaraz

Clave RI: DELIN-228032

Universidad Autónoma de Querétaro
Facultad de Derecho
Licenciatura en Criminología

SOCIEDAD DE LA INFORMACIÓN Y NUEVAS FORMAS DE VICTIMIZACIÓN

TESIS

Que como parte de los requisitos para obtener el grado de

Licenciatura en Criminología

Presentan:
María Yajaira Alvarez Monjaraz

María Guadalupe Balderas Méndez

Dirigido por:
Mtra. María Guadalupe García Martínez

SINODALES

Mtra. María Guadalupe García Martínez Presidente	_____ Firma
Mtro. Emilio Paulín Larracoechea Secretario	_____ Firma
Dra. Aceneth González López Vocal	_____ Firma
Lic. Edgar Francisco Álvarez Mayorga Suplente	_____ Firma
Dr. Juan Alberto Pichardo Hernández Suplente	_____ Firma

_____

Dr. Edgar Pérez González

Director de la Facultad

Centro Universitario
Querétaro, Qro.
Febrero 2023

AGRADECIMIENTOS

Agradecemos a la Universidad Autónoma de Querétaro, por permitirnos formar parte no solo de su institución sino de los planes de estudio, la enseñanza, el prestigio y educación que nos deja.

Asimismo, agradecemos a la Maestra. María Guadalupe García Martínez, Coordinadora de la Lic. en Criminología, por ser nuestra asesora y presidenta de la presente investigación, por el apoyo que nos brindó y el conocimiento que nos transmitió para poder llevar a cabo y concluir con esta tesis colectiva.

A todos los maestros de la licenciatura que durante nuestra formación académica estuvieron presentes para nosotras, brindando apoyo, resolviendo dudas, generando conocimiento y alentándonos cada día para concluir con una carrera universitaria y ser unas profesionistas preparadas.

DEDICATORIA

Dedico el presente proyecto de Tesis a mis padres María Carmen Méndez y José Juan Balderas, por haberme apoyado incondicionalmente no solo durante mi carrera universitaria, sino en toda mi vida personal, profesional y educativa, quienes han sido mi pilar fundamental para salir adelante, que han estado en todo momento conmigo sin dejarme sola. Agradecida infinitamente con las únicas personas que no han dudado de mí, y que me siguen alentando día con día a ser mejor y cumplir mis objetivos y sueños.

A mis hermanos, que desde siempre he tenido admiración por ellos y han estado conmigo, que me han apoyado y alentado para salir adelante.

A la mejor amiga y compañera de Tesis que la universidad me pudo dar, Maria Yajaira (mi yaqui), por haber estado conmigo desde el primer día hasta el último, siendo un apoyo fundamental dentro y fuera de la escuela, agradecida con su amistad sincera y apoyarme en mis momentos difíciles.

Por último, dedico este proyecto a mi amiga Erandi Paola, que nunca dudó de mí, siempre confió y estuvo apoyándome. Hoy me encuentro concluyendo mi carrera, siendo así uno de mis mayores logros de mi vida. Un abrazo hasta el cielo.

María Guadalupe Balderas Méndez

DEDICATORIA

Agradezco infinitamente a mis padres Salvadora Monjaraz y Gustavo Alvarez por todo el apoyo, confianza y esfuerzo que hicieron para que pudiera tener mis estudios universitarios y por nunca dejarme sola en todo este camino, ya que sin ellos esto no hubiera sido posible. A mis hermanos por sus palabras de aliento y motivarme a siempre superarme y no rendirme en el proceso.

Agradecimiento total a mi hermana Karla Tamara que siempre me ayudó en todo mi proceso, que siempre me acompañó durante mis noches de desvelo estudiando para exámenes o exposiciones, que siempre me escuchó, motivó y aconsejó para seguir siempre dando más de mi.

A mi mejor amiga y compañera de aventuras Guadalupe Balderas (mi lupis), por siempre estar para mi en los momentos más críticos de la carrera y por tomar esta aventura de Tesis a mi lado. Por sus palabras, consejos y motivaciones, por su amistad dentro y fuera de la universidad.

Por último, a mi hijo Edrick Sebastián, por ser una gran motivación para superarme profesionalmente y motivarme a realizar esta Tesis Colectiva. ¡Te amo hijo, mi mayor logro en la vida, ya fue el ser tu madre!.

Maria Yajaira Alvarez Monjaraz

CONTENIDO

Resumen

Las herramientas digitales son, desde hace algunos años, parte de la vida diaria, las nuevas tecnologías han ido ocupando cada vez más territorios de la vida social. Ver las noticias, postular a un trabajo, asistir a clases, agendar una reunión con amigos, encontrar la mejor ruta para llegar a un lugar, entre otras muchas actividades exigen el uso y dominio básico de tecnologías de la información y la comunicación.

Sin embargo, este no ha sido el único elemento desencadenante de la asimilación de nuestras vidas al orden digital. La evolución, independiente e imparable, de internet, sumado al incremento de los mercados de producción e innovación de las TIC's han construido en nuestras sociedades nuevos marcos de desarrollo personal y colectivo, han permitido también la existencia de nuevas formas de ser y estar en el mundo, formas que las generaciones pasadas apenas imaginaban o atribuían a obras literarias y cinematográficas de ciencia ficción.

En este sentido, es previsible y casi inevitable proyectar el surgimiento de nuevas formas de victimización. Mismas que, ancladas en la sociedad de la información representan retos jurídicos, tecnológicos, criminológicos y por supuesto victimológicos. Por ello, es importante identificar estas nuevas formas de victimización, conceptualizarlas, describirlas, hallar patrones y dibujar sus causas.

Abstract

Digital tools, have been for a few years part of our every day life, new technologies have occupied more social life territory day by day, Watching the news, applying for a job, assisting classes and organizing a simple reunion with friends, finding the best route in order to get to a destination, among many more activities demand the domain of technologies, information and communication.

However, this element has not been the only trigger to the assimilation of our lives in the digital order. The independent and unstoppable evolution of the internet, adding an increase in production markets and innovation of TICs have built in our society's new frameworks for personal and collective development, allowing the existence of new ways to be and exist in the world, ways that our past generations could only imagine, or they would attribute it to literary forms and science fiction cinema.

In that regard, it's very predictable and almost unavoidable to project the immerse of new forms of victimization. Same as which are announced to society and this information represents legal, technological, criminological and of course victimological challenges. Therefore, it's important that we identify these new forms of victimization and conceptualize, describe, find their patterns and draw their causes.

I. INTRODUCCIÓN

En la era de los datos, la información, las tecnologías de la información y la comunicación, así como del internet de las cosas; las cartografías físicas, sociales y simbólicas han cambiado de tal forma que los mapas habituales y familiares se encuentran irreconocibles. Pensemos en un sujeto que falleció apenas conociendo los primeros teléfonos celulares, qué pensaría si pudiera estar en nuestro presente y escuchara el término ciberseguridad, o si pudiera observar que los dispositivos celulares han reducido al menos 2 veces su tamaño y cuando menos 8 veces su grosor, entendería la lógica que se esconde detrás de adquirir activos virtuales o serían pautas descabelladas y sin sentido para él.

Probablemente este sujeto no comprendería mucho de cómo funciona el mundo actual, desconocería muchas palabras y conceptos que se adhieren con facilidad y casi naturalidad a nuestro lenguaje. Además, es altamente probable que nuestras formas de relación social y representación individual le resultaran exóticas, por decir lo menos. Los cambios que ha experimentado el mundo, y el humano, no se limitan al aumento de tecnología y dispositivos; cambió nuestro lenguaje, se modificaron las formas de transitar por el mundo y de relacionarnos con él, aparecieron nuevos riesgos y amenazas y por tanto formas alternas de victimización.

A propósito de ello, el estudio *Digital 2021 Global Overview Report,* realizado por la firma We Are Social Hootsuite proporciona información particularmente relevante sobre el estado de las redes digitales en el mundo. A finales de 2020, la Internet World Stats (IWS) estimó la población mundial en 7,838,004,158 personas, de las cuales, 4,949,868,338 eran usuarios de Internet. De acuerdo con estos datos, la IWS estableció el progreso mundial del Internet en 63.2%. Esto se traduce a que, en la actualidad, por lo menos 6 de cada 10 personas en el mundo tienen acceso a Internet.

Por otra parte, el Instituto Nacional de Estadística y Geografía (INEGI), en colaboración con la Secretaría de Comunicaciones y Transportes (SCT) y el Instituto Federal de Telecomunicaciones (IFT), publica la Encuesta Nacional sobre Disponibilidad y Uso de Tecnologías de la Información en los Hogares 2019

(ENDUTIH, 2019) donde se estimó que, en México, hay 80.6 millones de usuarios de internet, que representan 70.1% de la población de seis años o más. Esta cifra revela un aumento de 4.3% respecto de la registrada en 2018 (65.8%) y de 12.7% respecto a 2015 (57.4%). De los 80.6 millones de usuarios de internet de seis años o más, 51.6% son mujeres y 48.4% son hombres.

Esto resulta importante ya que las formas de socialización actual están marcadas por el auge del uso de las TIC'S y el internet, teniendo como consecuencia el surgimiento de diversos fenómenos sociales como; cyberbullying, robo de datos, usurpación de identidad, fraude, manipulación digital, mercadotecnia emocional y Fake News.

El incremento, producción e innovación de las TIC's es imparable, pareciera que la victimización que trae de fondo cumple ese mismo camino. La mirada debe fijarse en el incremento del uso de las TIC´S, sus alcances, así como sus consecuencias. La latente necesidad de estudiar este fenómeno se presenta en que el uso de estos medios se vuelve cada vez más necesario para las personas y sus formas de interacción e intercambio de información. De esta manera, el actuar de las y los profesionales de la criminología y victimología es de gran relevancia para prevenir acciones o conductas que causen algún daño físico, psicológico o económico a nivel individual o colectivo.

Por lo tanto, es importante identificar el surgimiento de las nuevas formas de victimización debido a que, en su mayoría, aún no se consideran como tal, sino que han sido normalizadas como consecuencias naturales del avance tecnológico y las dinámicas digitales. Por otra parte, el marco normativo y la legislación, se encuentran rezagados de tal manera que el Estado no está preparado para atender a las víctimas que surgen por dichas victimizaciones, o ni siquiera cuenta con elementos contextuales y conceptuales para reconocerlas.

La sociedad de la información constituye una evolución de las formas de socialización basadas en el conocimiento humano. Esta evolución ha permitido al ser humano desarrollar nuevas capacidades y constituye un recurso que altera el modo en que se relaciona. Una de las formas de relación es a través de los medios

de comunicación digital que establecen y fomentan contactos indirectos en la actividad cotidiana

El uso adecuado e inadecuado de los medios digitales permiten el flujo de información (académica, cultural, y política), la expansión de redes y vínculos sociales. Así como el cúmulo de información personal y privada que en ocasiones llegan a colocar a los usuarios en un estado de vulnerabilidad y en situaciones más particulares en un estado de victimización. Cabe destacar que el desarrollo de las nuevas tecnologías trae consigo diversificación en las formas de victimización, debido al incremento del flujo de información y los usuarios, quienes se encuentran activamente inmersos en estos mecanismos de socialización y comunicación.

En el contexto actual, se puede considerar que existe un crecimiento exponencial de víctimas de medios digitales. Esto hace necesario un estudio y descripción de las causales de la victimización y el tipo de víctimas, para la prevención y una posible atención, ya que hasta el momento no se le ha dado la visibilidad y reconocimiento a las víctimas y tampoco se le ha otorgado la importancia necesaria a esta problemática social.

Para fines de la presente investigación, se han dividido en tres grupos las nuevas formas de victimización, esto de acuerdo a la relación víctima - victimario:

- Formas de victimización de persona a persona:
- Formas de victimización de empresas a personas.
- Formas de victimización desde el Estado a personas.

Cada una de estas categorías serán identificadas, descritas y analizadas en el apartado de resultados.

II. ANTECEDENTES

En diferentes partes del mundo se han realizado investigaciones que abordan el tema sobre las víctimas que surgen en las dinámicas de las redes sociales digitales y las nuevas tecnologías. Sin embargo, no se habla directamente sobre las nuevas formas de victimización, únicamente se abordan modalidades ya exploradas, tal es el caso del cyberbullying, ciberacoso, suicidio, sexting, etc.

Un ejemplo de este tipo de estudios es el realizado en Madrid, por Sergio Tudela de Marcos y Ana Barrón López de Roda en el 2017, titulado *"Redes sociales: del ciberacoso a los grupos de apoyo online con víctimas de acoso escolar"*. En él, los autores entienden al "ciberacoso" como una conducta voluntaria de hacer daño a otro a través de acciones directas (pegar e insultar) o indirectas (aislar a la víctima).

El "ciberacoso" explicado por Oliveros (2012) implica que, a mayor disponibilidad de dispositivos, como móviles u ordenadores, con conexión a internet y redes sociales, así como la falta de supervisión por parte de un adulto, aumentan las probabilidades de un uso irresponsable de las tecnologías. Es en el uso inadecuado de las TIC´S y las redes sociales, donde los usuarios que forman parte del mundo digital se exponen de tal manera que se vuelven vulnerables frente a situaciones que los convierten en víctimas.

Otra investigación, realizada en España, *"Riesgos y oportunidades en internet y uso de dispositivos móviles entre menores españoles"* por Maialen Garmendia Larrañaga, Estefanía Jiménez Iglesias, Miguel Ángel Casado & Giovanna Mascheroni (2016); describe al "bullying" como una forma de agresión intencional, contínua y reincidente que implica una desigualdad de poder entre víctima y agresor. Por consecuencia, el cyberbullying se ejerce utilizando cualquier tipo de aparato tecnológico, el teléfono móvil, medios digitales, etc.

Aunque el cyberbullying es una actividad que busca hostigar, ridiculizar o dañar a otra persona, también se puede considerar la implicación de la desigualdad de roles sociales o jerarquías. Una característica importante del cyberbullying es el anonimato, ya que este puede incrementar la amenaza o la impotencia de la víctima.

Muchos usuarios de los medios digitales se presentan de manera anónima a través de perfiles e información falsa, de esta manera exponen a usuarios reales con; fotografías, comentarios, insultos, mensajes sexuales, etc., a los cuales vuelven víctimas de ciberacoso, extorsión, pornografia infantil, entre otros.

Dentro de la misma investigación *"Riesgos y oportunidades en internet y uso de dispositivos móviles entre menores españoles",* se abarca otro tema de gran importancia: el *sexting*. Éste consiste en el intercambio de imágenes por medios digitales e involucra: crear, compartir y difundir imágenes de desnudos o semidesnudos sexualizados de sí mismos o de alguien a quien se conoce. Por otra parte, los autores identifican 3 supuestos básicos de sexting, cuando el intercambio de imágenes sexuales ocurre:

1. Cuando los sujetos establecen el intercambio de contenidos como parte de su identidad sexual e intimidad, sin necesariamente pasar a lo físico o ser sexualmente activos.
2. Entre dos compañeros, como parte de una relación sexual;
3. Como el inicio de una actividad sexual entre dos personas que aún no tienen una relación o intercambio físico.

Por consecuencia, se considera que gran parte de las personas que practican el *sexting* son las que forman o tienen una relación sexual. Estas prácticas se pueden suscitar a través de distintas redes sociales tales como WhatsApp, Facebook, Snapchat, Telegram, Instagram, Messenger, entre otras. Dicho contenido puede ser fácilmente distribuido, ya que se tiene acceso a internet, medios digitales, incluso las redes en las cuales se pueden difundir y por lo tanto, causar una forma de victimización directa hacia la o las personas que protagonizan dichas fotografías, videos y contenido sexual.

En otro artículo, este de corte criminológico, realizado en México *"Uso de internet y conductas suicidas en adolescentes de 14 a 18 años en México"* por Susana Olivares Pérez en el 2018*,* hace referencia al fenómeno social del suicidio y un factor relevante es el uso del internet. En dicho documento menciona que La Organización Mundial de la Salud (OMS), considera el suicidio como un problema de salud

pública. Asimismo, la conducta suicida de una persona no se considera como un acto principalmente dirigido por el deseo de morir, sino que el intento suicida involucra un debate interno entre el deseo de morir y el de seguir vivo.

El internet forma parte de la vida diaria de las personas, y pasar gran tiempo frente a un dispositivo móvil genera un impacto directo en su realidad, modificando su forma de interactuar y de relacionarse con otras personas. Este es un factor importante que debe considerarse en el fenómeno del suicidio, ya que existe evidencia de páginas web que incitan a la consumación del mismo. En ese sentido, se considera "cibersuicidio" a la acción de quitarse la vida, motivada por la influencia de los llamados chatsroom, páginas pro-suicidas, foros de internet, redes sociales, etc.

Por otra parte, en cuanto a la victimización ejercida por empresas y entidades estatales hacia personas se identificaron antecedentes relacionados con el software *Pegasus*. De acuerdo con Andrés Meza (2021), el caso "pegasus" se desarrolla a partir de un software creado por la empresa de tecnología Israelí Grupo NSO, **NSO** Technologies (**NSO** que significa Niv, Shalev y Omri, los nombres de los fundadores de la compañía). Este es un programa que se encargaba de combatir el terrorismo y la delincuencia. Sin embargo, también se considera como un programa malicioso, ya que se puede instalar en un dispositivo sin aviso y sin consentimiento. Pegasus, puede instalarse a través de un mensaje de texto sin la necesidad de "hacer click" y no produce ninguna notificación.

Este software tiene la capacidad de acceder a todos los datos de un teléfono: micrófono, cámara, sms, llamadas, contactos y todo lo que se produce en el dispositivo móvil. El reportero Alejandro Santos Cid (2021), menciona que pegasus funciona como un virus, que permite acceder a la agenda, fotografías, cámara o archivos guardados en los dispositivos móviles.

La investigación de la Unidad de Inteligencia Financiera (UIF) considera que, en México, la utilización del software Pegasus, no solo se utilizó para un espionaje informático y obtener información relevante, sino que también generó un desvío de fondos públicos.

Otro antecedente de este tipo de eventos es el que ocurrió cuando varias fiscalías estatales estatales, la Fiscalía General de la República (FGR), la Comisión Nacional de Seguridad y la Comisión Nacional de Búsqueda (CNB), entregaron datos genéticos (entre los años 2016 y 2018), relacionados con familiares de víctimas de desaparición, a la empresa ADN México.

De acuerdo con la Red de Defensa de los Derechos Digitales (R3D), en 2016, la titular de la Dirección de Laboratorios Criminalísticos, indicó a la titular del Laboratorio de Genética Forense de la institución, que le diera la base completa de perfiles genéticos del laboratorio en una USB. Posteriormente, esta información sería compartida con ADN México obteniendo a través de distintos convenios, un aproximado de 49 mil datos genéticos de víctimas de desaparición de todo el país, con el fin de contactarlas y solicitar dinero por servicios de información e incluso filtrar información de casos confidenciales a particulares, sin estar previamente informadas las víctimas y las autoridades.

III. FUNDAMENTACIÓN TEÓRICA

Para adentrarnos en identificar y describir las formas de victimización propias de la sociedad de la información, es necesario partir del entendimiento de dos elementos: 1) las características, dinámicas y conceptualizaciones de la sociedad de la información; 2) víctima y victimización. Una vez comprendidas estas dos dimensiones, se podrá abordar el apartado de resultados de manera más precisa.

3.1 Sociedad de la información

Existen distintas formas de nombrar la época histórica que estamos viviendo y a la sociedad que ésta engendra. Algunos autores le llaman por ejemplo sociedad líquida (Sigmund Bauman), sociedad de la transparencia (Byung-Chul Han) o sociedad del riesgo (Ulrick Beck). Para efectos de la presente tesis, abordaremos la época actual desde su concepción como sociedad de la información (SI).

> *A partir de los años sesenta, aparece una nueva sociedad caracterizada por el incremento de la información, como una definición del mundo moderno creándose un nuevo paradigma para interpretar el desarrollo social sobre la base del uso y empleo de tecnologías de información.* (Estudillo G.,J., 2001,pág.2)

Actualmente, la idea de la SI es analizada desde perspectivas históricas. Por un lado, se pueden mencionar posturas que anuncian una nueva organización de sociedad que ha surgido del pasado; donde se encuentran exponentes de las corrientes como el postindustrialismo, posmodernismo y desarrollo informacional. Estas posturas coinciden en que la información es parte importante del mundo contemporáneo.

Torres Rosa María (2005), menciona que en 1973 el sociólogo Daniel Bell, uno de los primeros pensadores que abordaron el tema, consideraba al sector de la información como el motor de cambio que haría posible una sociedad moderna, en donde podría observarse un cambio en la economía de la producción de bienes, a una de servicios basados en la información, con profesionales y técnicos

reemplazando a los trabajadores, donde el conocimiento se convertiría en el pilar de la innovación, la elaboración de políticas y las tecnologías en la clave para continuar un constante desarrollo, por lo que la tecnología de la información representa una nueva forma de vida que modifica las actividades de la estructura social.

Joel Estudillo (2001), afirma que desde la perspectiva de William J. Martin y Frank Webster, se distinguen cinco elementos que describen qué es la sociedad de la información:

1. Elemento tecnológico
2. Elemento económico
3. Elemento ocupacional
4. Elemento tiempo-espacio
5. Elemento cultural

Elemento tecnológico: Las TIC´S representan el establecimiento de una nueva forma de vida que modifica las actividades de la estructura social. El aspecto tecnológico ha hecho posible procesar, almacenar, recuperar y transmitir información, que ha guiado a la aplicación de tecnologías de información en todos los ámbitos de la sociedad.

Elemento económico: El conocimiento es una pieza importante de la economía conforme existe un cambio de una economía de bienes a una economía del conocimiento. Actualmente se puede argumentar que nos desarrollamos en una sociedad donde la característica distintiva es el conocimiento y su globalización como creadores de riqueza. Bajo este enfoque, los datos adquieren e incrementan exponencialmente su valor en el mercado.

Elemento ocupacional: Esta tendencia es reforzada por muchos reportes de la Organización para la Cooperación y Desarrollos Económicos (OCDE), dando importancia al contínuo crecimiento de aquellas ocupaciones que se enfocan en la creación y manejo de la información, así como su infraestructura de apoyo y asignación de trabajadores a categorías particulares.

Elemento tiempo-espacio: Este elemento se enfoca en la importancia de redes de información que vinculan localidades, ciudades, países, regiones y continentes, haciendo posible la globalización de la información. Ello da pauta a un nuevo tipo de sociedad, donde las cosas suceden en lugares particulares y en tiempos específicos. En la sociedad de la información, el tiempo y las distancias son más relativas que en cualquier otro panorama histórico.

Elemento cultural: La cultura actual es más informativa pues vivimos en una interacción simbólica en donde todo lo que se intercambia y recibe es reconocible. Habitamos en una sociedad que está inmersa en los medios de comunicación e información.

De esta manera, se puede decir que la Sociedad de la Información (SI) plantea una evolución tecnológica que modifica las formas de socialización, dando paso al enfoque espacial que juegan las redes de la información y la comunicación de acuerdo al tiempo-espacio en el que se desarrollan, mismas que repercuten en todos los sectores sociales.

Por otra parte, un elemento importante de la SI es la digitalización, misma que se concibe como *un proceso que ha dado lugar a nuevos medios, nuevas formas de producir, almacenar y difundir la información, lo que modifica las relaciones interpersonales, los sistemas de producción, educación y entretenimiento. (Crovi D., Delia, 2002, pág.16)*

El elemento digitalizador permite que exista una sobreproducción de información, donde se generan datos a todas horas. Esto ha generado, que con el paso del tiempo, las unidades de almacenamiento en dispositivos se vean obligadas a evolucionar debido al volumen de información que se genera diariamente. Es por ello, que se han creado distintas unidades que van desde el byte hasta el Petabyte y otras unidades aún mayores.

> Para entender esto, es necesario partir de la unidad básica, el bit o dígito binario. Un bit es la unidad de información más pequeña que el procesador manipula y físicamente se representa con un elemento como un pulso o un

punto. Después de esta unidad, se encuentran unidades cada vez más complejas:

- Byte o unidad de almacenamiento: está constituido por 8 bits. Equivale a un solo carácter, como una letra o un número.
- Kilobyte (kB): equivale a 1.024 bytes y a menudo es la unidad en la que se registra el almacenamiento de archivos pequeños como documentos de texto o imágenes en baja resolución.
- Megabyte (MB): equivale a más de un millón de bytes, y comúnmente son archivos de tamaño considerable los que se almacenan en esta unidad. Por ejemplo, imágenes en alta resolución, archivos, carpetas, documentos y programas.
- Gigabyte (GB): equivale a mil millones de bytes. Es la unidad que más típicamente se maneja hoy en día, y las computadoras más comunes proveen de un espacio de más de 100 GB para memoria. Los archivos de todo un ordenador de tamaño considerable se mide en GB.
- Terabyte (TB): equivale a 1024 Gigabytes y es una medida que se utiliza para referir a ordenadores de alta capacidad.

No obstante, el TeraByte (TB) no es la unidad de almacenamiento más grande que existe, pues actualmente la unidad de almacenamiento de mayor capacidad es el GeoByte (GB), equivalente a 1024 BrontoByte (BB).

Tabla 1. Unidades de Medida de Almacenamiento

MEDIDA	SIMBOLOGÍA	EQUIVALENCIA	EQUIVALENTE EN BYTES
BYTE	B	8 BITS	1 BYTES
KILOBYTE	KB	1024 KB	1 024 BYTES
MEGABYTE	MB	1024 MB	1 048 576 BYTES
GIGABYTE	GB	1024 GB	1 073741 824 BYTES
TERABYTE	TB	1024 TB	1 099 511 627 776 BYTES
PETABYTE	PB	1024 PB	1 125 899 906 842 624 BYTES

EXABYTE	EB	1024 EB	1 152 921 504 606 846 976 BYTES
ZETABYTE	ZB	1024 ZB	1 180 591 620 717 411 303 424 BYTES
YOTTABYTE	YB	1024 YB	1 208 925 819 614 629 174 706 176 BYTES
BRONTOBYTE	BB	1024 BB	1 237 940 039 285 380 274 899 124 224 BYTES
GEOPBYTE	GB	1024 GB	1 267 650 600 228 229 401 496 703 205 376 BYTES

Fuente: Elaboración propia con datos de Vázquez-Moctezuma, 2015.

Para dimensionar de forma práctica la importancia de la información y la capacidad de almacenamiento, se ofrecen los siguientes datos relacionados con Norteamérica en 2019, y que generaron impacto económico:

En cuestión de tecnología e internet de acuerdo con el sitio web de Grupo Bit Business Analitycs (2018), los norteamericanos producían por minuto 3,138,420 GB de datos en internet, se vendían 2,833 teléfonos celulares, se enviaban 159,362,760 e-mails, Skype soportaba 176,220 llamadas, se enviaban 12,986,111 mensajes de texto y se producían 3,877,140 búsquedas en Google. En media, entretenimiento y redes, se reproducían 97,222 horas de video en Netflix, los usuarios de Youtube miraban 4,333,560 videos, se subían 400 horas de video a Youtube, se escribían 473,400 tweets en Twitter, se publicaban 49,380 fotos en Instagram y Spotify reproducía más de 750,000 canciones.

En retail, Amazon envió 1,111 paquetes y vendió $332,876 dólares, se generaron 73,249 transacciones por internet y los compradores dejaron $7,610,350 dólares abandonados en sus carritos de compras.

Cabe destacar que todos los datos anteriores, además de corresponder al 2019, se generaron por minuto. Se estimaba que para el 2020, por cada persona en el mundo se produjera 1.7 MB de datos cada segundo y que cada año se duplicará la cantidad de datos producidos en el año anterior. A su vez, la población global que tiene acceso a internet crece casi en la misma proporción.

En este tenor, es necesario saber la diferencia entre dato, información y conocimiento, ya que son conceptos que van de la mano y se necesita una mejor comprensión por su relación entre los mismos.

De acuerdo con Juan Carrión (s.f.) por dato, se entiende un conjunto discreto de factores objetivos sobre un hecho real. El dato en sí mismo no dice el por qué de las cosas, sino solamente sirve como base para la creación de la información. La información, a diferencia de los datos, está organizada para algún propósito. Los datos se convierten en información cuando se les atribuye algún significado. Esta cumple la función de un "mensaje" donde existe un emisor y un receptor, en donde el receptor interpreta o percibe dicha información de distinta manera, dependiendo de la contextualización, juicios de valor, etc.

Por último, para Davenport y Prusak (1999), citado por Juan Carrión, el conocimiento es una mezcla de experiencia, valores, información y "saber hacer" que sirve como base para la incorporación de nuevas experiencias e información. Así como la información se deriva de los datos, el conocimiento se deriva de la información; y para que esto se lleve a cabo, las personas deben transformar dicha información a través de la comparación, conversación, consecuencias y conexiones.

De esta manera, un dato es algo vago, como por ejemplo 12,500. La información es algo más precisa, por ejemplo; las ventas del mes de junio fueron de 12,500 pesos, y el conocimiento se obtiene mediante el análisis de la información, por ejemplo; las ventas del mes de junio fueron de 12,500 pesos, junio es el mes más alto en ventas de souvenir de playa.

Uno de los grandes problemas de la sociedad de la información es que pese a los grandes volúmenes de datos y la gran trazabilidad de objetos, el análisis y la reflexión han quedado en segundo plano frente a las dinámicas de hipercomunicación.

En este sentido, la sociedad de la información se torna transparente. El filósofo norcoreano Byung–Chul Han argumenta que se revelan como transparentes cosas, acciones, tiempo e imágenes, siendo quizá más evidentes estas últimas que *"se*

hacen transparentes cuando, liberadas de toda dramaturgia, coreografía y escenografía, de toda profundidad hermenéutica, de todo sentido, se vuelven pornográficas", es decir cuando existe un *"contacto inmediato entre la imagen y el ojo"* (2012, p.12).

Para este mismo autor, la transparencia es violenta en el sentido de que "la coacción de la transparencia nivela al hombre hasta convertirlo en un elemento funcional de un sistema" (Han, 2012, p.14) cuyo valor se mide "tan solo en la cantidad y la velocidad del intercambio de información" (Han, 2012, p.23). En este sentido, se aprecia a los sujetos únicamente por su valor de exposición.

En la sociedad de la información, las imágenes, experiencias y personas son convertidas en mercancía y tratadas como tal "han de exponerse para ser, desaparece su valor cultural a favor del valor de exposición (…), la mera existencia es por completo insignificante" (Han, 2012, p.26).

3.2 Víctimas y procesos de victimización.

Corresponde a esta sección, profundizar en la conceptualización de víctima, sus tipologías y procesos de victimización, así como otros elementos importantes para comprender las formas de victimización propias de la sociedad de la información.

3.2.1 Sobre el concepto de víctima.

Es necesario analizar este concepto desde distintos enfoques: el ámbito penal, la victimología, la sociología e incluso la filosofía. Para iniciar la exploración dentro del ámbito penal, y el marco normativo, la Ley General de Víctimas (LGV), en el capítulo II, artículo 4 hace una primera distinción entre víctimas directas e indirectas:

> *Se denominarán víctimas directas aquellas personas que directamente hayan sufrido algún daño o menoscabo económico, físico, mental, emocional, o en general cualquiera puesta en peligro o lesión a sus bienes jurídicos o derechos como consecuencia de la comisión de un delito o violaciones a sus derechos humanos reconocidos en la*

> *Constitución y en los Tratados Internacionales de los que el Estado mexicano sea parte.*
> *Los familiares o personas a cargo que tengan relación inmediata con la víctima directa y toda persona que de alguna forma sufra daño o peligre en su esfera de derechos por auxiliar a una víctima son víctimas indirectas.*
> *La calidad de víctimas se adquiere con la acreditación del daño o menoscabo de los derechos en los términos establecidos en la presente Ley, e independientemente de que se identifique, aprehenda, o condene al responsable del daño, o de su participación en algún procedimiento judicial o administrativo.*

Bajo esta conceptualización, se observa como condición de posibilidad la acreditación del daño o menoscabo de los derechos para que una persona pueda ser considerada como víctima. Esto puede generar pautas de revictimización y deja ver que para el aspecto normativo no basta con experimentar los hechos sino que además habrá que acreditarlos.

Por otra parte, la Organización de las Naciones Unidas (ONU), esta reconoce en la Declaración Sobre los Principios Fundamentales de Justicia para las Víctimas de Delitos y de Abuso de Poder que, se constituyen como víctimas de delitos a:

> *Las personas que, individual o colectivamente, hayan sufrido daños, inclusive lesiones físicas o mentales, sufrimiento emocional, pérdida financiera o menoscabo sustancial de los derechos fundamentales, como consecuencia de acciones u omisiones que violen la legislación penal vigente en los Estados Miembros, incluida la que proscribe el abuso de poder* (1985, p.1).

De esta manera, se pueden considerar víctimas a los usuarios que hayan sufrido algún daño, siempre y cuando sea por un delito tipificado dentro de la legislación penal. Es importante mencionar que este documento emitido por la ONU no hace diferencia en víctimas directas e indirectas, sino que contempla dentro de una sola categoría a ambas: *se incluye además, en su caso, a los familiares o personas a*

cargo que tengan relación inmediata con la víctima directa y a las personas que hayan sufrido daños al intervenir para asistir a la víctima en peligro o para prevenir la victimización (1985, p.1).

Además, esta misma Declaración incorpora parámetros para conceptualizar a las víctimas de abuso de poder, entendiendolas como:

> *Las personas que, individual o colectivamente, hayan sufrido daños, inclusive lesiones físicas o mentales, sufrimiento emocional, pérdida financiera o menoscabo sustancial de sus derechos fundamentales, como consecuencia de acciones u omisiones que no lleguen a constituir violaciones del derecho penal nacional, pero violen normas internacionalmente reconocidas relativas a los derechos humanos* (1985, p.2).

A pesar de la amplitud de estas definiciones, resulta insuficiente para agrupar a las nuevas víctimas, surgidas en la sociedad de la información. Ya sea porque las conductas que les han generado daño no se encuentran previstas en las normas penales o porque no están contempladas por las normas internacionales, en algunos casos se debe, incluso, a que no se consideran agresiones contra los derechos humanos.

Definiciones desde la criminología y la victimología

El criminólogo Benjamín Mendelsohn, citado por Hernández, no identificaba a la víctima con una persona, sino con un carácter, es por ello que considera como víctima a la personalidad del individuo o de la colectividad en la medida en que esta es afectada por las consecuencias sociales determinadas por factores de origen físico, psíquico, económico, político y social.(Hernández, Y., 2020, p. 85).

Por otra parte, para Hans Von Hentig, citado por Hernández, la víctima es un blanco fijo al que el autor dirige sus disparos. "*Es la persona que ha sido lesionada objetivamente en alguno de sus bienes jurídicamente protegidos y que experimenta subjetivamente el daño con malestar o dolor."* (Hernández, Y., 2020, p. 85).

En visiones más amplias encontramos las definiciones aportadas por Góppinger y Nieves. En primer lugar, Góppinger señala que, *en el objeto de la Victimología, "son subsumidas no sólo las víctimas de los delincuentes, sino también aquellas personas que llegan a ser víctimas sin la intervención de otros, o que llegan a sufrir daños (accidentes laborales, accidentes en viaje, etc., 'el accidentado'); para la Criminología, estos campos ofrecen, a lo sumo, interés a los fines de una contemplación comparativa* (p. 362).

Esta argumentación, deja claras dos cosas: 1) existen víctimas de otras conductas que no necesariamente figuran en los códigos y normativas, 2) la criminología misma ha dejado de lado y prestado poco interés a víctimas que no están relacionadas con delitos.

En segundo lugar, Nieves afirma que deberían ser incluidas conductas no tipificadas como hecho punible, y que *los análisis y estudios victimológicos, deben extenderse a conductas que si bien no son descritas por la ley como delitos o falta (...) poseen un gran índice victimogénico* (Nieves, 1975, p.5).

La criminología crítica pone sobre la mesa otras visiones de la víctima, por ejemplo, plantea un reproche persistente a la victimología clásica por ignorar la existencia de una *victimización silenciosa y tolerada en amplios colectivos trabajadores, inmigrantes, consumidores, et.); victimización social e institucional, cotidiana, sometida a la violencia de la pobreza y la exclusión social* (Herrera, p. 74). En este sentido la crítica es acertada, la víctima no se reduce a aquella que ha experimentado las consecuencias del delito o la vulneración de los derechos humanos, se trata también de personas y sectores que de manera silenciosa viven los aspectos negativos de la construcción sistemática del sistema mundo capitalista.

La idea de la víctima como ente invisible es cercana a la noción del Homo Sacer, propuesto por Giorgio Agamben. Este autor sostiene que la principal aportación del poder soberano es la producción de la nuda vida como elemento político, siendo la nuda vida aquella vida que se puede quitar y sacrificar, es decir, la vida del homo sacer. El poder político, es por tanto, el dueño de la vida y muerte del ciudadano.

> *Es posible, entonces, dar una primera respuesta a la pregunta que nos habíamos formulado en el momento de delinear la estructura formal de la excepción. Aquello que queda apresado en el bando soberano es una vida humana a la que puede darse muerte pero que es insacrificable: el homo sacer* (Agamben, 2006, p.109).

Los privilegios del poder soberano inundan el cuerpo, vida y muerte de los sujetos, ciudadanos y no, y condena a los invisibles al sacrificio en pos de un sistema que les aplasta. Las víctimas son, en este sentido, meras piltrafas invisibilizadas, sin sentido y sin valor.

En ese sentido, la identificación de una persona o un grupo como víctima no es natural, sino que es parte de un proceso histórico, social, cultural, político y económico. Distintos actores intervienen en la definición de quién, cómo y cuándo puede ser nombrado víctima.

3.2.2 Tipos de víctimas

De acuerdo con la Ley General de Víctimas y la Declaración de Naciones Unidas sobre los Principios Fundamentales de Justicia para las Víctimas de Delitos y del Abuso de Poder, los tipos de víctimas son:

- *Víctimas directas: aquellas personas físicas que hayan sufrido algún daño o menoscabo económico, físico, mental, emocional, o en general cualquiera puesta en peligro o lesión a sus bienes jurídicos o derechos como consecuencia de la comisión de un delito o violaciones a sus derechos humanos reconocidos en la Constitución y en los Tratados Internacionales de los que el Estado mexicano sea parte.*

- *Víctimas indirectas:* estas abarcan a *los familiares o aquellas personas físicas a cargo de la víctima directa que tengan una relación inmediata con ella*, *así como las personas que hayan sufrido daños al intervenir para asistir a la víctima en peligro o para prevenir la victimización.*

Por otra parte, Mendelsohn quien fuera el primero en realizar una propuesta sobre los distintos tipos de víctimas propone la siguiente tipología, fundamentada en la correlación de culpabilidad entre víctima y victimario:

- Víctima inocente: es aquella que no ha hecho nada para favorecer o desencadenar el hecho delictivo en el que resulta afectado.
- Víctima provocadora: mediante su conducta, incita al victimario a realizar un hecho criminal.
- Víctima por ignorancia: es aquella que sin desearlo impulsa al otro a cometer un hecho delictivo del cual resulte lesionado.
- Víctima voluntaria: provoca su propia victimización.
- Víctima agresora: puede ser imaginaria o simuladora, ya que no es realmente víctima por algún hecho delictivo.

Esta clasificación logra dos objetivos fundamentales: 1) ubicar a la víctima como un personaje dinámico en el proceso y 2) romper con la idea de la víctima como un sujeto pasivo.

3.2.3 Procesos de victimización

Por victimización se entiende el fenómeno por el cual una persona o grupo se convierte en víctima. En este apartado se mencionan las formas de victimización, la victimogénesis, así como los tipos de víctimas.

De acuerdo con Cesar A. Giner, en su artículo *Aproximación psicológica de la victimología*, clasifica las formas de victimización en:

- *Victimización conocida/desconocida*: la conocida es aquella que forma parte de una estadística, ya que causa un impacto en la sociedad y medios de comunicación; la desconocida es aquella victimización que se queda en la cifra negra.

- *Victimización directa/indirecta*: la directa, es la agresión inmediata que sufre la víctima; la indirecta, es la que sufren las personas del círculo inmediato de la víctima, es decir, su familia, amigos y conocidos.

- *Victimización primaria/secundaria/terciaria*:

a) Victimización primaria

Es un proceso por el cual la víctima, sufre de manera directa daños biopsicosociales que resultan de un hecho delictivo.

b) Victimización secundaria

La victimización secundaria surge principalmente de la interacción entre la víctima y el proceso jurídico-penal del Estado, ya que a través de este proceso se realiza una revictimización por parte de las autoridades competentes.

c) Victimización terciaria

Es el resultado de las vivencias y procesos de etiquetamiento, que sufre el círculo familiar y social de la víctima.

Victimogénesis

Este concepto es empleado para referirse al estudio de los factores que ponen en riesgo a las personas para ser objetos de delitos, o de algún otro elemento vulnerante. En ésta se analiza su estado de vulnerabilidad por el cual aumenta el riesgo de ser víctimas.

Se abarcan dos tipos de factores; los de riesgo y los de vulnerabilidad.

a) Los *factores de riesgo* son todos aquellos elementos que predisponen o potencializan la condición de víctima.

- Situacionales: este varía según el lugar (población, zona urbana, etc.) en que se encuentre la persona.
- Biológicos: abarca desde la raza, edad, sexo o género.

- Socioeconómicos: depende del nivel socioeconómico en que se desarrolle.
- Características relativas a la personalidad del sujeto.

b) Los *factores de vulnerabilidad*: aspectos psicológicos y situacionales adquieren un importante significado ya que estos se relacionan entre el hecho delictivo y el daño psicológico generado en la persona. Entre los factores de vulnerabilidad se encuentran:

- Biológicos: la edad y el sexo.
- Referentes a la personalidad: el comportamiento del individuo (reservado, extrovertido, dependiente, seguro, inseguro), estado emocional, entre otras.
- Sociales: económicos, laborales, apoyo social, roles, redes de apoyo y habilidades.
- Psicológicos: la capacidad de pensar y reflexionar, razonar, aceptación, valoración, o bien si sufre de algún problema psicológico como depresión, ansiedad, etc.

3.3 Víctimas de medios digitales

La víctima y su comportamiento son elementos que pueden llegar a determinar un hecho delictivo de manera digital. En las TIC´S, como en el ciberespacio, la víctima juega un papel de gran importancia, en cómo se posiciona o qué oportunidad da al victimario para realizar el delito, ya que puede propiciar de forma indirecta su grado de vulnerabilidad debido a las conductas o acciones que realiza, tales como dar a conocer datos personales, información de su rutina que resulte relevante, exceso de confianza a usuarios desconocidos, etc.

Siguiendo la línea de los tipos de víctimas se pueden considerar las víctimas de medios digitales, víctimas tangibles, resultado de una victimización a través de las acciones que surgen dentro de estos. Asimismo, todo usuario de internet o persona que tenga acceso a una red a través de los sistemas existentes, son potenciales víctimas.

Un ejemplo de víctimas de medios digitales son aquellas que han sido vulneradas a causa de la difusión de contenido de carácter personal, privado, íntimo y sexual, estas se encuentran bajo el resguardo de la Ley Olimpia, aprobada en el año 2020.

Dicha Ley surge de las reformas a la Ley General de Acceso de las Mujeres a una Vida Libre de Violencia y al Código Penal Federal. Busca reconocer la violencia digital y sancionar los delitos que violen la intimidad sexual de las personas a través de medios digitales. Su impulsora fue la activista Olimpia Corral M., después de ser víctima de la difusión de un video íntimo sin su consentimiento. Hasta el momento 28 entidades son las que la han aprobado, con las reformas a estas normas se busca que la violencia digital y la violencia en los medios de comunicación sean delitos sancionables en todo el país.

La Ley Olimpia contempla sanciones de tres a seis años de prisión para quienes realicen estas acciones y multas que van de 500 a 1,000 Unidades de Medida y Actualización (UMA). Ésta pretende resolver la problemática de difusión de contenidos íntimos de una persona a través de cualquier medio, lo que resulta ser violencia sexual y digital; ya que causa daño a la vida privada y los derechos humanos. Esta es una práctica normalizada, no regulada que inhibe el acceso a la justicia y pone en riesgo la vida de las personas.

La difusión sin consentimiento de imágenes de contenido íntimo o sexual a través de los medios digitales promueve un daño a la persona expuesta. Esto afecta principalmente a mujeres y adolescentes. La utilización de las diversas plataformas digitales en computadoras, laptops o teléfonos celulares, donde se publica información e imágenes sensibles y privadas, provocan una afectación en su vida emocional, psicológica y social.

3.4 Violencia digital y violencia mediática

La *violencia digital,* engloba actos de acoso, hostigamiento, amenazas, insultos, mensajes de odio, divulgación de datos o información privada realizados mediante el uso de tecnologías. Además, de la difusión de imágenes, audios y videos de contenido sexual de una persona sin su consentimiento.

Este tipo de violencia, igual que otros tipos de violencia mucho más visibilizados, puede causar daños emocionales, físicos, sexuales, invasión a la privacidad, miedo a la exposición pública, abandono del uso de medios digitales y redes sociales, entre otros.

La Organización No Gubernamental Luchadoras de México, ha identificado distintas formas de agresión de género relacionadas con las tecnologías. Estas agresiones tienen la capacidad de ejercer violencia psicológica, sexual e incitar a la violencia física. Algunos tipos de acciones digitales más comunes, son:

- Acceso y control no autorizado de cuentas (hackeo): implica reunir información no autorizada, el bloqueo de la cuenta de la víctima o la utilización de la cuenta para ejercer desprestigio y/o desacreditación del titular.
- Control y manipulación de la información: el robo de información implica una pérdida y manipulación de información.
- Difusión de fotos íntimas o información privada: consiste en compartir cualquier tipo de información, datos o contenido privado acerca de una persona, sin su consentimiento.
- Doxeo: investigar y difundir información de una persona sin su consentimiento, con fines de acoso.
- Vigilancia: monitoreo constante de las actividades de una persona, su vida diaria, información pública o privada.
- Uso de spyware: software para espiar y obtener información de otros dispositivos o acceso a cuentas sin el consentimiento del usuario.
- Uso de GPS u otros servicios de geolocalización para rastreo de movimientos.
- Robo de identidad/creación de perfiles falsos: el uso de la identidad de otra persona, la creación y divulgación de datos personales falsos, con la intención de dañar la reputación del titular.
- Distorsión de imágenes y/o vídeos: elaboración de contenido falso, manipulado o fuera de contexto y su divulgación con el fin de desprestigiar y dañar a una persona.

- Cyberbullying: acoso mediante el uso de medios digitales, a través de amenazas, mensajes ofensivos y/o peyorativos.
- Extorsión: forzar a una persona a actuar de acuerdo a la voluntad de otra a través de amenazas e intimidación.

Sin embargo, es pertinente mencionar que la violencia digital no se restringe a razones de género, ni se limita al ejercicio de violencia entre pares. Este tipo de violencia se refiere a cualquier mecanismo social, político, económico o tecnológico que aprovechando las plataformas digitales y los valores de la sociedad de la información, violenta y genera menoscabo en la integridad y dignidad de las personas.

Por otro lado, la *violencia mediática* se refiere a acciones realizadas a través de cualquier medio de comunicación que suscitan directa o indirectamente estereotipos sexuales, que justifican la violencia contra las mujeres y permiten la difusión de discursos de odio, la discriminación de género o desigualdad.
Considerando la violencia digital y la violencia mediática, podemos percatarnos de sus divergencias y similitudes que presentan, así como el papel que juegan los medios digitales para su evolución. Sin embargo, estos tipos de violencia se pueden prevenir o disminuir, si se les da el reconocimiento necesario dentro de los marcos normativos y en el diseño de política pública.

3.5 Derechos digitales

En cuanto a los *derechos digitales* y la importancia que estos tienen, es necesario mencionar, que en todo momento debe existir la protección a los derechos humanos. Al respecto, la sociedad civil se organiza en diversas agrupaciones que buscan lograr estos fines, entre ellas destaca en México: la Red en Defensa de los Derechos Digitales (R3D, 2021). Esta es una organización mexicana dedicada a la defensa de los derechos humanos en el entorno digital, la R3D utiliza diferentes herramientas legales y de comunicación para realizar investigaciones de políticas, litigio estratégico, incidencia pública y campañas con el objetivo de promover y hacer del conocimiento los derechos digitales en México, concentrándose en los derechos de

la libertad de expresión, la privacidad, el acceso a la información y conocimiento, así como a la cultura.

De acuerdo con información ofrecida en su propio sitio web (2021), esta organización comenzó tras la defensa de la privacidad en México a consecuencia de la discusión del Código Nacional de Procedimientos Penales (CNPP) a finales de 2013, el cual contemplaba la intervención de comunicaciones privadas, incluyendo la geolocalización, la recolección y acceso a metadatos. A partir de dicha labor, la R3D trabaja en diversas líneas estratégicas relacionadas a la privacidad en el entorno digital de los mexicanos.

La organización busca investigar, explorar y construir una estrategia alternativa de acceso universal al Internet de banda ancha, no solo en términos de confiabilidad, disponibilidad, continuidad y calidad, sino bajo una equidad y sin discriminación. Además, promueve la implementación de lineamientos que garanticen la neutralidad de la red, el uso libre, la no discriminación, la privacidad y el derecho a la libertad de expresión en línea. Defiende y promueve el derecho fundamental de todas las personas a expresar sus ideas en el mundo digital, así como la defensa jurídica y social contra intentos de censura, lleva a cabo monitoreos constantes de amenazas a la libertad de expresión en línea, y realiza incidencias legislativas para la defensa de este principio en las leyes mexicanas.

R3D busca que los intermediarios de Internet diseñen e implementen reglas y políticas respetuosas de los derechos humanos, donde se denote la existencia de mecanismos efectivos para impedir o minimizar los efectos del hostigamiento y la distorsión de conversaciones en línea, defiende el acceso al conocimiento de forma libre, compartible y modificable con el fin de obtener una mejor sociedad de la información, asimismo, busca que se garantice el derecho a las expresiones anónimas, que existan protecciones legales, herramientas tecnológicas y una cultura de la denuncia de interés público.

Por otro lado, en el contexto Mexicano se cuenta también con organismos defensores de los derechos digitales en el ámbito gubernamental, siendo el más importante a nivel nacional el *Instituto Nacional de Transparencia, Acceso a la*

Información y Protección de Datos Personales (INAI). Es el organismo constitucional autónomo que garantiza el cumplimiento del derecho de acceso a la información pública y el de protección de datos personales, es decir, que el primer derecho enunciado garantiza que cualquier autoridad en el ámbito federal, órganos autónomos, partidos políticos, sindicato o cualquier persona física o moral que reciba y ejerza recursos públicos o realice actos de autoridad, te entregue la información pública que se solicite. El segundo derecho, garantiza el uso adecuado de los datos personales, así como el ejercicio y tutela de los derechos de acceso, rectificación, cancelación y oposición que toda persona tiene con respecto a su información personal (INAI 2021).

En palabras de la propia institución, el INAI busca ser una Institución Nacional eficaz y eficiente en la consolidación de una cultura de transparencia, rendición de cuentas y debido tratamiento de datos personales para el fortalecimiento de una sociedad incluyente y participativa, promover el ejercicio de los derechos de acceso a la información y protección de datos personales como base para la participación democrática y un gobierno abierto.

3.6 Daño moral

Por otra parte, se debe considerar el daño moral y la reparación integral, debido a que las víctimas por medios digitales sufren este daño y deben ser acreedoras a una reparación del mismo.

De acuerdo con el Instituto de Investigaciones Jurídicas de la Universidad Nacional Autónoma de México (2014), los hermanos Mazeud, definen al *daño moral* como aquel que constituye un atentado contra un derecho extrapatrimonial, se refieren a la lesión a intereses morales, como el honor, la consideración social o la vida misma. Por su parte Volochinsky lo reconoce como el dolor, que causa a la víctima el hecho victimizante, aquello que perjudica a los sentimientos o creencias, y que puede tener afectaciones en el orden patrimonial.

Por otro lado y desde el punto de vista penal, el daño moral tiene carácter de pena pública a favor de la víctima u ofendido cuando se comete algún delito. Debe existir

una sentencia sobre el hecho delictivo; en consecuencia, se sanciona con el pago de una suma determinada de dinero por reparación al daño moral. Asimismo, el daño moral es aquel que sufre una persona a causa del hecho dañoso, en su honor, buena reputación o en su consideración social, resulta de la afectación o violación de los derechos de la personalidad.

De esta manera, se considera que las víctimas por medios digitales sufren de un daño moral, debido a que resultan afectaciones en su personalidad, sentimientos, valores, creencias, su esfera psicológica, entre otras. Este incluye perjuicios en la honra, el sufrimiento y el dolor, que se derivan de la violación a los derechos de la víctima, resultado de la humillación al que es sometida, del desconocimiento de su dignidad humana y derechos. Por lo tanto es necesario que se le brinde una reparación integral del daño sufrido.

En el sitio web de la Unidad para la Atención y Reparación Integral a las Víctimas del Gobierno de Colombia (2019) la *reparación integral* es un deber del Estado y es un derecho de las víctimas afectadas por la violación a sus Derechos Humanos, que han causado daños en sus vidas, integridad, patrimonio, sus proyectos de vida personales, familiares y profesionales. Comprende varias medidas, entre ellas; la restitución, indemnización, rehabilitación, medidas de satisfacción y garantías de no repetición. Sin embargo, no todas las víctimas acceden a todas las medidas de reparación, el acceso depende del tipo de hecho, del daño sufrido y de la voluntad de las víctimas para acceder a las mismas. Jorge F. Calderón (2015), menciona que la Corte Interamericana de Derechos Humanos, establece las medidas de reparación integral, que pueden ser individuales, colectivas, materiales, morales o simbólicas:

- Restitución: son las medidas que buscan el restablecimiento de los derechos y condiciones de las víctimas a la situación en que se encontraban antes de que ocurriera el hecho victimizante.
- Indemnización: Dependiendo del hecho victimizante, las víctimas recibirán una compensación económica por los daños sufridos, a título de indemnización administrativa.

- Rehabilitación: pretende reparar lo que concierne a las afectaciones físicas, psíquicas y morales que puedan ser objeto de atención médica o psicológica.
- Medidas de satisfacción: Estas medidas buscan proporcionar bienestar y contribuir a mitigar el dolor de las víctimas, tienen el objetivo de reintegrar su dignidad.
- Garantías de no repetición: El Estado debe implementar una serie de medidas con el fin de garantizar que no se repitan las violaciones a los derechos humanos, ni las infracciones al Derecho Internacional Humanitario que generaron la victimización.

IV. HIPÓTESIS

La sociedad de la información (con la tecnología, valores y dinámicas sociales que implica) produce nuevas formas de victimización que resultan en un aumento cuantitativo y cualitativo de víctimas, así como una constante normalización social.

V. OBJETIVOS

General

Identificar y describir las nuevas formas de victimización que surgen en la sociedad de la información, debido al uso del internet y de otras Tecnologías de la Información y Comunicación (TIC´S), con el objetivo de identificar categorías de análisis, características particulares y generales de las dinámicas de victimización.

Específicos

1. Conocer cómo es que lo digital ha pasado a formar parte de nuestro mundo en lo material, sensorial, social y su vinculación con la victimología.

2. Describir las formas de victimización presentes en la sociedad de la información e identificar categorías de agrupación.

3. Identificar las características comunes que comparten las dinámicas victimizantes de cada categoría.

4. Generar conclusiones útiles para la creación de futuras políticas públicas victimológicas.

Preguntas de investigación

1. ¿Cómo es que lo digital ha pasado a formar parte de nuestro mundo en lo material, sensorial, social y su vinculación con la victimología?

2. ¿Qué formas de victimización están presentes en la sociedad de la información? ¿Cómo y en qué categorías pueden agruparse?

3. ¿Qué características comparten las dinámicas de cada categoría identificada?

4. ¿Qué elementos son básicos en las propuestas de políticas públicas victimológicas en materia de victimización digital?

VI. METODOLOGÍA

Se emplea un enfoque cualitativo y se presenta un estudio de corte analítico explicativo, donde se busca el conocimiento detallado de fenómenos sociales específicos con el objetivo de identificar cómo ocurren los mismos y dar respuesta a las problemáticas que surgen de ellos. Este enfoque permite explorar los significados y las realidades del objeto de estudio por medio de la investigación documental, etnografía digital y revisión de casos.

En **primer lugar**, se realiza investigación documental que permite recabar datos y explorar distintos aspectos de la vida social de los usuarios en la red, cuyo objetivo es mostrar cómo se organizan a partir de la interacción y comunicación atravesada por las tecnologías de la información y la comunicación.

Ésta se caracteriza por el uso predominante de registros bibliográficos, archivos impresos o digitalizados que permiten el análisis del fenómeno social estudiado, en la que, a través de la técnica se aporte información de carácter descriptivo para la construcción de conocimientos.

Además, la revisión documental permite generar un primer acercamiento teórico a los elementos conceptuales de la sociedad de la información. Esto construye una base sólida de conocimiento a través de la cual se puede interpretar la realidad (en lo general) y la victimización (en lo particular).

En **segundo lugar,** durante la investigación se aplica etnografía digital para la recolección e interpretación de datos, ya que ésta es una forma de investigación cualitativa sumamente útil. De acuerdo con Karen O´Reilly (2005) se define a la etnografía digital como una investigación inductiva-iterativa, basada en una serie de métodos (...) que reconoce la función de la teoría y la del propio investigador y que considera que los seres humanos son en parte objetos y en parte sujetos. Por lo tanto, puede decirse que la etnografía digital consiste en establecer contacto con los participantes a través de los medios, de esta forma nos permite observar qué hacen siguiéndoles digitalmente.

En este sentido, la etnografía digital a menudo establece contacto con los participantes a través de los medios, un contacto “mediado”, más que a través de la presencia directa, (O´Reilly, 2005, pág. 19).

Las nuevas tecnologías ofrecen nuevas formas de participar e interactuar en los entornos de investigaciones emergentes. El sociólogo Dhiraj Murthy menciona que la etnografía digital se centra en “*sistemas de recopilación de datos que están intervenidos por la comunicación mediada por el ordenador*”, ya que a través de ella se pueden realizar notas de campo elaboradas digitalmente, la observación online participante, blogs/wikis con aportaciones de los respondientes y grupos focales online. (Pink,Sarah; Horst, H., 2019)

Asimismo al realizar un análisis de la vida social digital, se considera que los medios y las tecnologías digitales forman parte de los mundos cotidianos en el que habitan las personas, pues existe una normalización de la vida social digitalizada. En este sentido, los medios digitales forman parte de las relaciones humanas, donde existe una nueva forma de copresencia o de estar juntos, los bienes comunes creativos, las formas de participación y la colaboración digital pasan a ser formas de vivir y de relacionarse con los demás; es decir, parte de una cultura digital en donde se genera conocimiento y una actividad colaborativa.

En **tercer lugar,** se utiliza la revisión de casos; investigación que se realiza desde una perspectiva off-line para la obtención de información de casos en específico, sobre todo de categorías donde la información teórica es escasa. Esto para permitir un análisis de carácter descriptivo. Se busca a través de la revisión de casos: registrar y describir las conductas de las personas involucradas en los fenómenos sociales estudiados, permitiendo confirmar, cambiar, modificar y/o ampliar el conocimiento sobre el objeto de estudio.

Por último, tanto la identificación de las formas de victimización, como la elección de casos, respondieron a los siguientes criterios:

1) Se tratara de dinámicas victimizantes nuevas o bien, tradicionales pero con modalidades o mecanismos nuevos.

2) Hicieran uso y aprovechamiento de las plataformas digitales y sus características. En este sentido se descartaron otras que corresponden al aprovechamiento cibernético, electrónico, etc. en tanto no abarcaran el terreno digital.

3) Estuvieran relacionadas de manera directa con el producto central de la sociedad de la información: los datos y la información misma.

4) Respondieran a alguna de las siguientes dinámicas y relaciones:
    - Persona-persona.
    - Empresa-persona.
    - Estado-persona.

5) Haya producido o tenga potencial de producir victimización en un sentido amplio, no solo a víctimas de delitos y abuso de poder sino de la construcción misma de los sistemas y núcleos de poder.

VII. RESULTADOS Y DISCUSIÓN

Como se discutió anteriormente, la sociedad de la información encarna una serie de características que la hacen particularmente violenta para algunos. La transparencia, el culto por los datos y el riesgo generalizado hacen de esta época y de estas sociedades caldos de cultivo perfectos para la generación de nuevas formas de victimización.

Despliegues de conducta tales como el cyberbullying, acoso digital, difusión de contenido personal y sensible, fraudes, estafas, robo de datos, manipulación colectiva, hipervigilancia, entre otras, conforman el ecosistema de nuevas formas de victimización. Estos mecanismos pueden configurarse en tres rubros, de acuerdo con la dinámica que juegan la víctima y el victimario: persona-persona, empresa-persona y Estado-persona.

7.1 Dinámicas de victimización persona-persona.

En esta tipología encontramos formas de victimización que van de usuario a usuario, sea este individual o colectivo. Es decir, hablamos de la violencia ejercida entre personas o grupos de personas (colectivos, grupos sociales, comunidades). Estas formas de victimización son quizá las más evidentes y directas, son también aquellas cuyas consecuencias tienden a ser más perceptibles, favoreciendo la identificación de la víctima como tal.

7.1.1 Ciberacoso

El desarrollo de las TIC´S y el aumento de los medios digitales, han incrementado algunas ventajas para todos los usuarios, tales como la obtención de información, la facilidad de adquirirla, generación de conocimiento, entretenimiento, etc. Sin embargo, existen algunas desventajas tales como la exposición a actos o conductas que dañan a otros usuarios y que algunas veces se configuran como actos ilícitos, tal es el caso del ciberacoso.

Para comprender de una mejor manera este fenómeno, es necesario tener una definición clara del concepto fuera de los medios digitales; el acoso es la conducta de persecución física y/o psicológica que realiza un estudiante contra otro de forma negativa, continua e intencionada (UNICEF, 2019). Martínez-Otero V. (2017), cita a Castillo, Pulido (2011), donde menciona que en dicho fenómeno intervienen varios factores asociados con los orígenes, contexto sociocultural, entorno familiar y nivel socioeconómico de los sujetos involucrados y de la institución en la que se encuentran. En términos generales se puede decir que el acoso, consiste en perseguir a una persona de tal manera que la víctima se siente atemorizada y sufra graves desequilibrios emocionales.

Ahora bien, Martínez, Otero V. (2017) menciona que se puede distinguir una clasificación sobre los tipos de acoso:

- El acoso físico, que daña la integridad física de la persona. En este se encuentran dos modalidades: la manera directa, golpear, empujar, morder o indirecta se centra en objetos de la víctima.
- El acoso verbal, se produce por medio de las palabras; amenazar, burlarse, insultar, difamar, desprestigiar o desacreditar.
- El acoso social, que va enfocado a la exclusión social.
- El acoso psicológico, en el que su objetivo es debilitar o dañar emocionalmente a la persona.

Sin embargo, estos despliegues de violencia se han ido diversificando dependiendo del avance de la información y comunicación. Hoy en día ya no se requiere un espacio físico directo en donde el agresor tenga contacto con la víctima para que pueda darse la forma de intimidación, actualmente se podría considerar que el nuevo escenario es el ciberespacio, dentro del cual se configura el ciberacoso.

El ciberacoso es la agresión, intimidación, hostigamiento y victimización donde se hace uso de la información electrónica y medios digitales como las redes sociales, correos electrónicos, mensajes de texto, messenger, llamadas, videollamadas, teléfonos celulares, entre otros para acosar a una persona. Es una forma de maltrato intencional, persistente, en donde existe un desequilibrio de poder entre el

agresor y la víctima. (Martínez, Otero V., 2017) En dicho concepto se agrega además una característica esencial e importante, el anonimato.
Los medios digitales son utilizados por los mismos usuarios para ofender, hostigar, amenazar, insultar, ridiculizar a otras personas a través de la publicación de fotos, videos, difusión de los mismos, mensajes, llamadas. Por otro lado, las consecuencias son el daño a la integridad no solo física sino psicológica y emocional de la víctima.

Este tipo de violencia o agresión, del que los victimarios buscan obtener algún provecho, coloca a la víctima en un estado de indefensión y puede generar consecuencias negativas tales como ansiedad, depresión, baja autoestima, desconfianza, exclusión social, negación de la victimización o pensamientos suicidas.

En el ciberacoso destacan ciertas características que lo diferencian del acoso tradicional, Hernández y Solano (2007), citados por Martínez, Otero V., (2017) mencionan que estas son:

- El dominio y uso de las tecnologías y medios digitales.
- Acoso indirecto, no se necesita estar cara a cara víctima y victimario.
- Es un acto de violencia oculta, en la que los victimarios pueden ser conocidos o desconocidos.
- El desconocimiento del agresor aumenta el sentimiento de impotencia.
- Se desarrollan diversos tipos de acoso electrónico.
- La sensación o sentimiento de impotencia ante estas formas de acoso, se puede generar debido a que el material utilizado (imágenes, vídeos, mensajes) son difíciles de eliminar o retirar de la red.
- Puede existir un desamparo legal o la insuficiencia de marcos legales para la protección de la víctima.
- Invade la privacidad y seguridad del usuario, dejándolo en estado de indefensión.
- Se hace público, se extiende con rapidez.

Tras el avance de las nuevas tecnologías y el desarrollo de los medios digitales, las formas de victimización son más altas debido a las distintas formas de ocasionar un daño a las personas. Es necesario considerar que las víctimas que surgen a través de los medios digitales, muchas veces se quedan dentro de la cifra negra debido a que no denuncian, no solo por miedo al agresor, sino por la falta de marcos normativos o leyes que las protejan y respalden.

En este sentido, el periódico el Universal (2021), pública que, de la población usuaria de internet en México, 21% declaró haber vivido, entre octubre de 2019 y noviembre de 2020, alguna situación de acoso cibernético por las que se indagó, siendo mayor para mujeres (22.5%) que para los hombres (19.3%) informó el INEGI.

Los adolescentes y jóvenes son los más expuestos: 23.3% de los hombres de 20 a 29 años, y 29.2% de las mujeres de 12 a 19 años, señalaron haber vivido algún tipo de acoso cibernético, de acuerdo con los resultados del Módulo sobre Ciberacoso (MOCIBA 2020).

7.1.2 Extorsión por medio de las TIC’s

El Gobierno de México, explica que la extorsión telefónica dio inicios en el año 2000, cuando el acceso a la telefonía celular se amplió a un mayor número, haciendo más accesible la comunicación para todas las personas en cualquier sector.

La extorsión por medio del uso de teléfonos, es uno de los delitos más comunes en el que las personas siguen volviéndose víctimas. Sin embargo, también es fácil de prevenir, cuando la persona que está siendo "extorsionada" mantenga la calma, cuelgue o realice una serie de preguntas de carácter personal de las cuales no cualquier persona sepa la respuesta. La extorsión puede llevarse a cabo bajo el método de mensajes de texto o llamada telefónica dependiendo el modus operandi del estafador.

A través de la comunicación vía telefónica, los delincuentes, plantean supuestos escenarios que incluyen situaciones de riesgo para la posible víctima o familiares, tales como amenaza de daño físico, daño patrimonial, secuestros, detenciones de familiares a causa de un delito, etc. No obstante, también llevan a cabo otro tipo de dinámicas como discursos de premios obtenidos tras algún sorteo, campañas publicitarias e incluso, en ocasiones generan un diálogo previo con la víctima, para posteriormente presentarse como trabajadores de una institución bancaria, prestador de servicios de telefonía o de alguna institución u oficina de gobierno, ya que su objetivo es obtener información básica para luego utilizarla como parte de su estrategia de extorsión, ya sea de forma inmediata o postergando el uso de la misma. Todo esto como parte de sofisticadas técnicas de ingeniería social.

En la extorsión, la delincuencia utiliza la violencia psicológica para intimidar a las víctimas, utilizando agresiones verbales e incluyendo argumentos referentes al concepto de familia, pues en ocasiones se aprovechan de las personas para engañarlas. En la mayoría de los casos, los delincuentes eligen al azar a la víctima, utilizando directorios telefónicos, datos personales obtenidos a través de distintas vías y tomando la información publicada en el perfil de la persona a través de las redes sociales, observando imágenes publicadas en el perfil, lo que les permite conocer el nivel socioeconómico de la posible víctima y su familia. Posteriormente, obtienen el número del teléfono celular, utilizando argumentos relacionados con las actividades o intereses, o bien, ofertando una posición laboral a través de un anuncio y/o mensaje en las redes sociales.

Con datos generales, los extorsionadores tienen elementos para poder llevar a cabo sus actividades, ya sea con mensajes como "tenemos a tu hijo", “sé dónde trabajas”, "sabemos dónde vives" "estamos vigilando a tu familia", etc. Aunado a estos discursos y mediante la amenaza o engaño, los victimarios piden a las víctimas realizar depósitos de dinero a través de transferencias bancarias en cajeros u oxxos.

De acuerdo con el artículo 390 del Código Penal, la extorsión, la comete *“quien sin derecho obligue a otro a dar, hacer, dejar de hacer o tolerar algo, para obtener un lucro para sí o para otro, o causando a alguien un perjuicio patrimonial…”.* También

nos menciona que a quien cometa este delito, se le aplicarán penas de dos a ocho años de prisión y de cuarenta a ciento sesenta días de multa. Las penas aumentarán hasta un tanto más si se realiza por una asociación delictuosa, un servidor público, ex servidor público, miembro o ex miembro de alguna corporación policial o de las Fuerzas Armadas.

Núñez, J y Millan, A. (2004) identifican otra forma de extorsión que es el Spoofing. El término spoofing significa engaño, existen diversas técnicas informáticas basadas en falsear direcciones de correo electrónico, direcciones IP, direcciones MAC, servidores de nombres de dominio DNS, etc. Los peligros de este ataque son claros ya que atentan contra los principios de: privacidad (el SWS analiza y registra toda la información que circula entre la víctima y el servidor real), autenticidad e integridad (la información en ambos sentidos puede ser alterada) y réplica (repitiendo una acción de compra por Internet).

Un caso importante, es el documentado en el periódico El País por Rodríguez D, (2022). Este medio publicó una nota donde menciona cómo funciona el robo de cuentas de whatsapp, un modus operandi de los victimarios para realizar extorsión y se expone el caso de Daniel “N” quien fue víctima del secuestro de su cuenta conocida como *SIM swapping*. En este tipo de casos, cuando el número telefónico es clonado y utilizado para usurpar la identidad del propietario, robar contraseñas y vaciar cuentas bancarias. Los victimarios hacen uso de un mecanismo que se consigue en la red oscura (o *dark web*) por unos 200 dólares, o bien, mediante la ayuda de empleados corruptos de las compañías telefónicas que dejan al usuario sin servicio. En tan solo unos minutos, Daniel “N” fue víctima de varios delitos: suplantación de identidad, extorsión a sus contactos y también de la extracción de 2.000 pesos de su cuenta bancaria.

7.1.3 Difusión de pornografía intantil

El comportamiento humano, individual o colectivo se ha ido transformando a través del avance de las TIC's, pero no siempre son comportamientos adecuados. Tal es el

caso de la difusión de pornografía infantil, una práctica que va en aumento a la par del avance tecnológico en los últimos años.

De acuerdo con la Organización de las Naciones Unidas, en el artículo II del Protocolo Facultativo, la pornografía infantil fue definida como *toda representación, por cualquier medio, de un niño dedicado a actividades sexuales explícitas, reales o simuladas, o toda representación de las partes genitales de un niño con fines primordialmente sexuales (2021).* En este caso, la representación digital abarcaría aquellas cintas de video y las películas no reveladas, así como los datos almacenados en discos de ordenador o por medios electrónicos que puedan convertirse en imágenes visuales.

La pornografía infantil es un delito tipificado, no solo en México, sino que es un delito internacional. El Código Penal Federal, en el CAPÍTULO II, Pornografía de Personas Menores de Dieciocho Años de Edad o de Personas que no tienen Capacidad para comprender el Significado del Hecho o de Personas que no tienen Capacidad para Resistirlo; en su artículo 202 menciona que:

> *"Comete el delito, quien procure, obligue, facilite o induzca, por cualquier medio, a una o varias de estas personas a realizar actos sexuales o de exhibicionismo corporal con fines lascivos o sexuales, reales o simulados, con el objeto de video grabarlos, fotografiarlos, filmarlos, exhibirlos o describirlos a través de anuncios impresos, transmisión de archivos de datos en red pública o privada de telecomunicaciones, sistemas de cómputo, electrónicos o sucedáneos."*

De acuerdo con Najat M'jid Maala, relatora de la ONU (2009) sobre venta, prostitución y pornografía infantil:

> *"La pornografía infantil registra un constante aumento en Internet y otras plataformas como los teléfonos móviles. Se calculan que unos 750 mil pedófilos en el mundo están conectados permanentemente a la red y que existen 4 millones de sitios web con contenidos pornográficos que exponen niños (…) Se trata de un fenómeno que*

ha devenido una verdadera industria del delito, que genera miles de millones de dólares y que cada vez se extiende más debido al acceso generalizado a las nuevas tecnologías. Se cree que la producción y distribución de imágenes pornográficas criminales abusando de niños podrían representar un negocio de hasta 20.000 millones de dólares por año (…)".

La pornografía infantil y su difusión se ha extendido a través de los medios digitales, por la producción, tráfico, difusión y posesión de la misma. El poder del internet donde se tiene un fácil acceso, el carácter gratuito, el intercambio de información, la facilidad de ocultar la identidad, el anonimato; la velocidad y rapidez con la que se comparten contenidos, son ventajas de las cuales se aprovechan los consumidores y difusores de ese tipo de material.

Se tiene que dar la importancia necesaria a esta forma de victimización, ya que se desprenden más delitos como el comercio ilegal, uso de criptomonedas no reguladas por el Estado, difusión de material, explotación sexual de niños, entre otros. Las víctimas de esta acción son todas aquellas personas menores de 18 años que se encuentran en un estado de vulnerabilidad, no comprenden la gravedad del hecho o no pueden evitar estar en esa situación. Estas víctimas son violentadas en sus derechos, y su integridad, no solo física sino sexual y moral, ya que en muchas ocasiones dejan repercusiones biopsicosociales que pueden afectar a la persona en un alto grado con su percepción de sí mismos.

Un caso reciente, en México, fue el de Yosseline "N", una youtuber mexicana, quien fue acusada por el delito de pornografía infantil en agravio de una persona menor de edad.

En este sentido, en el Código Penal para el Distrito Federal, en su Capítulo III, Artículo 187, se menciona que:

Al que procure, promueva, obligue, publicite, gestione, facilite o induzca, por cualquier medio, a una persona menor de dieciocho años de edad o persona que no tenga la capacidad de comprender el significado del hecho o de

persona que no tiene capacidad de resistir la conducta, a realizar actos sexuales o de exhibicionismo corporal con fines lascivos o sexuales, reales o simulados, con el objeto de video grabarlos, audio grabarlos, fotografiarlos, filmarlos, exhibirlos o describirlos a través de anuncios impresos, sistemas de cómputo, electrónicos o sucedáneos; se le impondrá de siete a catorce años de prisión y de dos mil quinientos a cinco mil días multa, así como el decomiso de los objetos, instrumentos y productos del delito, incluyendo la destrucción de los materiales mencionados.

Además, en su cuarto párrafo señala que:

Se impondrán las mismas sanciones 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.

La youtuber fue partícipe de la reproducción, almacenamiento, publicación o exposición del material en el que se ve a una menor de edad, siendo abusada sexualmente por varios sujetos. Esto hace evidente dos cosas:

- La normalización de este tipo de violencia en internet, está tan generalizada que una figura pública no considero como negativo mostrar y viralizar material con contenido de pornografia infantil.
- La baja probabilidad de castigo y la impunidad, generan un caldo de cultivo adecuado para la proliferación de agresores. El caso de Yosseline “N”, demuestra que una figura pública puede difundir material indebido con casi ninguna consecuencia de por medio.

Es importante mencionar que el avance tecnológico y la difusión de la información tiene ventajas incomparables, sin embargo en muchas ocasiones suelen aprovechar ciertas características de los medios, lo que genera consecuencias negativas como el caso antes mencionado. Se debe tomar en cuenta que es una forma de victimización que va en crecimiento con el desarrollo de las TIC´S y que en definitiva, las víctimas deben ser escuchadas y respaldadas por un marco jurídico

que opere en favor y protección de las mismas, así como una reducción y prevención, no solo de la pornografía infantil, sino también de la difusión y el involucramiento de terceros ante tal delito.

Es importante mencionar que a diferencia de la difusión tradicional de pornografia infantil, los casos donde se ven involucrados los medios digitales y más aún figuras públicas y/o influencers con millones de seguidores, tienen un impacto mucho más grave y devastador para la víctima, pues el alcance de las imágenes se maximiza afectado no solamente los círculos inmediatos de la víctima sino todo su alrededor. En el caso antes discutido, por ejemplo, las imágenes fueron vistas por prácticamente todo el territorio mexicano.

7.1.4 Difusión de material sexual sin consentimiento

Como se mencionó en apartados anteriores, una de las principales características de la sociedad de la información es la hipercomunicación. Esto supone que la información puede ser compartida de manera rápida y sin contratiempos, además de la posibilidad de ser almacenada con relativa facilidad y en grandes volúmenes. Ello cobra especial relevancia en las dinámicas de difusión de material sensible, específicamente de órden sexual, ya que estos procesos tienden a ser rápidos, aprovechar las facilidades de almacenamiento y alcanzar a un mayor número de personas.

En los casos observados, se logra identificar la existencia de cuatro escenarios comunes: sexting o intercambio de contenido entre parejas, difusión de material por terceros, robo de contenido y recepción de material sin consentimiento.

1) Sexting: intercambio entre pareja sexual

De acuerdo con Mejía Soto, el término sexting, es la acción de enviar y recibir imágenes, videos o mensajes de índole sexual a través del uso de dispositivos móviles, computadoras o laptops, empleando las redes sociales como la principal fuente de intercambio de contenido. El sexting tiene como finalidad generar en el

receptor un deseo o atracción sexual, ya sea porque se tiene entre los actores una relación sexo afectiva estable o más o menos estable.

La práctica del sexting no genera interrogantes legales debido a que es una práctica voluntaria, mediante la que se comparte un aspecto de la propia intimidad con un tercero. La actividad en sí misma, de compartir contenido de índole sexual, no se considera un delito. Sin embargo, puede ser considerada una práctica de riesgo ya que el material audiovisual puede ser compartido sin el consentimiento o autorización del emisor.

2) Difusión de material por una persona diferente a la pareja

En este escenario, también existe una voluntad de ambas partes para enviar y recibir contenido audiovisual de tipo sexual (propio), sin embargo no media una relación sexoafectiva estable. El autor del contenido, al compartir a otra persona su material, ya no tiene control sobre el mismo, por lo que su difusión a otras personas resulta fácil.

La exposición de la intimidad que se presenta al llevar a cabo el intercambio sitúa al emisor en una situación de gran riesgo, pues afecta su privacidad y pone en riesgo su intimidad e imagen social, en la medida de los mensajes enviados, ya que estos pueden ser reenviados o reproducidos de forma indiscriminada por el receptor o una persona distinta a él, en redes sociales o medios de comunicación como lo son Whatsapp, Telegram, Hangouts, Instagram, Snapchat, etc.

3) Robo de contenido sexual, hackeado o en persona.

Existe la posibilidad de que una persona sea expuesta y violentada al difundir fotos o videos íntimos sexuales, a través del hackeo de cuentas o robo de contenido directamente de sus dispositivos móviles. Los victimarios se encargan de tener acceso fácil al dispositivo móvil empleando formas cómo “solicitar una llamada”, “tomar una foto”, “consultar una información”, etc, donde al tener acceso, aprovechan para enviar información o contenido sexual al cual tienen acceso al

disponer del móvil de la otra persona, en consecuencia el autor de las imágenes pierde el control de las mismas.

4) Recibir material sin consentimiento

En una dinámica contraria, se encuentra recibir imágenes, fotos o vídeos de contenido sexual a través de los medios digitales o redes sociales, sin consentimiento, es otra forma de ser victimizado, ya que no existe una autorización y aceptación del contenido, por la persona afectada. Esta situación se puede dar con mayor facilidad a través de las redes sociales, donde los usuarios (incluso con cuentas falsas), violentan a otros usuarios al compartir contenido íntimo sexual, generando así violencia digital.

Como respuesta a este tipo de casos, en México se instrumentó la Ley Olimpia. Dicho ordenamiento es un conjunto de reformas a la Ley General de Acceso de las Mujeres a una Vida Libre de Violencia y al Código Penal Federal, que buscan reconocer la violencia digital y sancionar los delitos que violen la intimidad sexual de las personas a través de medios digitales. En esta ley se menciona que *"difundir contenidos íntimos de una persona a través de cualquier medio es Violencia Sexual y Digital; daña la vida privada, los derechos humanos, y puede causar hasta la muerte, esta es una práctica normalizada, no regulada que inhibe el acceso a la justicia y pone en riesgo la vida de las personas".*

Las tecnologías de la información y comunicación están siendo utilizadas mayormente para difusión de información, ventas, etc., pero también, para causar daño principalmente se ha observado que es encaminada hacia mujeres y niñas, se considera que todo esto es por la falta de controles legales, sociales, medidas de seguridad, marcos jurídicos y sistema de justicia que faciliten la persecución del delito en las redes sociales.

La difusión de imágenes de contenido íntimo, erótico o sexual, sin consentimiento, a través de los medios digitalizados promueve un daño a la persona expuesta, dañando su intimidad, integridad física, moral y psicológica. Esto, se ve reforzado por el hecho de que los escenarios digitales se han convertido en extensiones de

nuestra vida psíquica y social. Al respecto, la iniciativa que dio vida a la ley Olimpia se menciona que "*acorde con cifras de la empresa informática Google México, 30.5 millones de personas cuentan con un teléfono de los llamados inteligentes (Smartphone), y pasan tres horas del día conectados a través de estos dispositivos, estos teléfonos son la pantalla donde más interactúan las personas con 40%, seguido por las computadoras con 29%, la televisión con 23% y tableta con 8%, lo que significa que la interconectividad es una extensión de la vida humana y lo que pasa en ella debe ser vista también como un medio comisivo."* (Dip. Rosales I, 2019)

El Congreso de la Ciudad de México, menciona que existen varios actores involucrados en este delito, no solo es la persona que lo difunde sino todos los que son partícipes tales como:

- Los creadores y administradores de páginas en las redes sociales que permiten este tipo de contenido y su difusión para una comercialización o exposición de las víctimas, ofertando el consumismo sexual y compilando los contenidos no autorizados.
- Los autores y productores directos de los videos e imágenes, que son los que se encargan de producir contenido sexual directamente con o sin consentimiento de la persona o en otras ocasiones existen productores ajenos a las parejas y estos actúan a través de cámaras escondidas en hoteles, moteles, baños públicos, videos por "debajo de la falda".
- Los que hacen públicas las imágenes o videos y todas aquellas personas que por algún motivo tienen material sexual en sus manos donde de manera dolosa hacen pública esta información, reproduciendo su viralización.
- Los cómplices y clientes de estas páginas, los que a través de su demanda, hacen que se genere todo tipo de contenido sexual, todos aquellos que frecuentan los medios, que forman parte de la cadena de delitos y del consumismo.

Por tanto, se puede concluir la relación entre estas acciones al tratarse de diferentes fenómenos sociales que de forma implícita tienen en común la difusión sin autorización de contenido de carácter sexual, causando un daño mayor a la víctima

en distintos ámbitos de su vida personal. Sin embargo, las legislaciones y reformas aún no contemplan formas de protección a quienes reciben imágenes de tipo sexual, no solicitadas.

8.1.5 Ciber-suicidios

En su sitio web, la Organización Panamericana de la Salud (OPS) considera al suicidio un problema de salud pública importante y a menudo descuidado. Cada caso de suicidio es una tragedia que afecta gravemente no solo a los individuos, sino también a las familias y las comunidades, el impacto que se genera tras el fenómeno, es muy alto debido a la cantidad de víctimas que ocasiona (primarias, secundarias y terciarias).

De acuerdo con Susana Olivares P. (2018), quien a su vez cita a la Organización Mundial de la Salud (OMS) define al suicidio como *"el acto deliberado de quitarse la vida", y* menciona que *"es un acto de violencia, la cual genera para los individuos, las familias, las comunidades y los países, graves consecuencias, tanto a corto como a largo plazo, provocando efectos perjudiciales en los servicios de atención de salud".* Existen distintos factores de riesgo por los cuales vulneran o incitan a que las personas cometan suicidio, estos factores van desde lo personal, económico, social o familiar.

Por otra parte, el cibersuicidio se refiere a la influencia de la información masiva que circula en los medios digitales y que puede sobrepasar al sujeto, así como la incitación que hay para ejercer actos suicidas. Se han documentado casos donde la acción de quitarse la vida se encuentra motivada por la influencia de los llamados chatsroom, páginas web pro-suicidas, redes sociales, entre otros, (Paredes, 2014). Para Olivares P. (2018) el cibersuicida se manifiesta y retroalimenta a través de la información otorgada en la red, ya que esta induce a los usuarios por medio de juegos, chistes y música a llevar a cabo tal acción. La influencia del internet, como forma de compartir y expandir información, se vuelve negativa, ya que el cibersuicidio es una problemática real hoy en día.

El uso del internet aumenta las posibilidades de comunicación en línea, pero también dificulta el control de lo que pasa en la red. Los usos indebidos o deshumanizados que pueden llegar a determinar, provocar o influenciar un acto suicida.

A través de diversos buscadores, se obtiene información, así como sitios web en donde se detallan formas o maneras de suicidio con contenido gráfico. En dichas páginas, los usuarios postean o publican notas, comentarios o pensamientos suicidas; otros comentan de manera anónima sus intenciones, las formas más “eficaces”, o incluso a través de tendencias sociales, incitan a actividades como juegos, retos, que deben ser videograbados o incluso en vivo para que más usuarios puedan verlos.

En la legislación mexicana, se encuentra tipificada la conducta de motivación e induccion al suicidio en el art. 312 del Código Penal Federal, Libro Segundo, Título Decimonoveno - Delitos contra la Vida y la Integridad Corporal en el Capítulo III - Reglas Comunes para Lesiones y Homicidio, el cual dice lo siguiente:

> *Artículo 312. El que prestare auxilio o indujere a otro para que se suicide, será castigado con la pena de uno a cinco años de prisión; si se lo prestare hasta el punto de ejecutar él mismo la muerte, la prisión será de cuatro a doce años.*

Algunas dinámicas que facilitan los ciber suicidios, son los grupos o páginas en las redes sociales, donde se comparte contenido, tales como; foros informativos, de contenido gráfico, tácticas de manipulación para la incitación al suicidio, influencia de otros usuarios, así como tendencias sociales,etc. Esto ocasiona que muchos usuarios, en su mayoría jóvenes, tengan un sentido de pertenencia y formen parte de estos grupos, como sucedió con el famoso caso de la ballena azul.

En 2017, un "juego suicida" se viralizó rápidamente por internet. El reto de la "Ballena azul", dirigido a adolescentes, establecía 50 tareas para realizar en 50 días. El desafío estuvo vinculado, presuntamente, con numerosas muertes en todo el mundo. Sin embargo, nada sobre el juego es lo que parece.

Las primeras tareas que planteaba eran relativamente inofensivas: levantarse en la mitad de la noche, o mirar una película de terror. Pero, día a día, las propuestas se iban tornando más fuertes: "párate en el borde de un precipicio", "tállate una ballena azul en el brazo".

El 22 de noviembre de 2015, Rina Palenkova, una adolescente que vivía en el sureste de Rusia, publicó un *selfie.* En la foto se la ve al aire libre, con una bufanda negra cubriéndose la boca y la nariz, y haciendo un gesto obsceno con su mano (mostrando el dedo del medio). La foto va acompañada de una leyenda en la que dice adiós. Al día siguiente, Palenkova se quitó la vida, (BBC MUNDO, 2019).

7.1.6 Ciber-secuestros

El secuestro es una acción o conducta tipificada que recibe una pena a quien participe o sea autor principal de este hecho. Si bien, es necesario resaltar el concepto de secuestro en sí mismo, se define como el apoderamiento y retención que se realiza a una persona con el fin de solicitar un rescate en dinero o en especie, en donde se adquiere un beneficio propio. El secuestro es generalmente llevado a cabo con el fin de obtener un rescate monetario, pero también puede ser por propósitos políticos u otros.

El artículo 364 del Código Penal Federal menciona que se impondrá de seis meses a tres años de prisión y de veinticinco a cien días multa:

> *Al particular que prive a otro de su libertad. Si la privación de la libertad excede de veinticuatro horas, la pena de prisión se incrementará de un mes más por cada día.*
>
> *La pena de prisión se aumentará hasta en una mitad, cuando la privación de la libertad se realice con violencia, cuando la víctima sea menor de dieciséis o mayor de sesenta años de edad, o cuando por cualquier circunstancia, la víctima esté en situación de inferioridad física o mental respecto de quien la ejecuta.*

Por otro lado, el Código Penal del Estado de Querétaro, en su artículo 150, recalca que:

> *Al que prive de la libertad a otro, se le aplicará prisión de seis a treinta y cinco años, si el hecho se realiza con el propósito de:*
> *I.- Obtener un rescate, un derecho o el cumplimiento de cualquier condición;*
> *II.- Que la autoridad realice o deje de hacer un acto de cualquier índole*
> *III.- Causar daño o perjuicio en la persona del secuestrado o en persona distinta relacionada con él.*

El cibersecuestro, es una modalidad nueva del concepto tradicional y de delitos cibernéticos, debido a las circunstancias y factores por los cuales se lleva a cabo. Las personas que se dedican a realizar estos delitos obtienen información de sus víctimas de diferentes maneras, entre ellas, se obtiene a partir de un chat o conversaciones con la víctima. Otra manera muy común en la web, es ingresar a las listas de correo y agregarse al llamado messenger, algunas víctimas pueden llegar a proporcionar sus datos o información de manera voluntaria, así los victimarios se pueden aprovechar de esta información ya sea para “fingir” el secuestro o en los casos más extremos, para realizar un encuentro con la víctima y después secuestrarla a través de “citas a ciegas”.

Otra modalidad, consiste en el cibersecuestro de datos o *ransomware*. De acuerdo con el sitio web de Expansión, Zamora E. (2021), menciona que a diferencia de otros tipos de extorsiones, los ciberdelincuentes amenazan la información, datos financieros o cualquier otro activo de valor que se encuentre guardado en un equipo, dispositivo o plataforma digital. El *ransomware*, es un tipo de software malicioso que tiene como objetivo apoderarse de la información que reside en la computadora de la víctima, solicitando un pago de rescate a cambio de liberarla. La técnica utilizada por el ransomware es encriptar la información de la computadora de la víctima, volviéndola inaccesible. Tras el pago del rescate, que es típicamente en criptomonedas, la víctima podría recibir la clave para desencriptar la información. Muchas veces los cibercriminales también recurren a la extorsión al amenazar con publicar la información robada.

Un ejemplo de este último es el ciberataque de Revil a una firma de herramientas de software, mismo que afectó a alrededor de 1,500 empresas. Algunos informes hablan de que los atacantes exigían un rescate de 50,000 dólares para organizaciones pequeñas y hasta 5 millones de dólares para corporativos más grandes.

El secuestro de información cambia la dinámica de los secuestros convencionales, no solo porque los medios empleados son digitales sino porque el objetivo del secuestro no es una persona, sino paquetes de información. Esto, ya que en la sociedad de la información los datos (no solo personales sino también industriales y comerciales) se convierten en el activo más importante.

7.1.7 Amenazas

Las amenazas son un fenómeno causado por el ser humano que puede poner en peligro a una persona, grupo de personas, sus cosas o su ambiente, cuando no son precavidos con sus acciones. De acuerdo a la RAE, la amenaza se define como el *"anuncio de un mal dirigido a otro, que puede realizarse de forma oral, escrita, o con actos, y con entidad suficiente para infundir miedo y temor".*

Las amenazas, están motivadas por varios escenarios, van desde la exigencia de dinero o cualquier otra condición como allanamiento de morada, sabotaje, robo, fraude o algún otro delito, lo que puede ser grave cuando es efectuada de forma seria, real y persistente atentando contra la salud o vida de la víctima (consumando el homicidio) o sus familiares.

Existen diferentes tipos de amenazas, dentro de las más comunes destacan:

- Revelar secretos de otro: Cuando alguien exige de otro una cantidad para no difundir hechos referentes a su vida privada, laboral o relaciones familiares que no sean públicamente conocidas y puedan afectar su reputación, crédito o interés.

- Contra la pareja: Cuando de modo intencionado se afecte a quien sea o haya sido su cónyuge, o bien, que esté o haya estado relacionado al ofensor por una relación de afectividad, aún sin convivencia.
- Con armas o instrumentos peligrosos: Es el uso de armas u objetos peligrosos con el fin de obtener un beneficio o bien material de la víctima.

Los medios para cometer las amenazas en contra de las personas se pueden distinguir en:

- Presenciales: Aquellos que emplean el uso de armas o instrumentos peligrosos en contra de la víctima.
- Indirectos o no presenciales: Los que se realizan a través de medios escritos, digitales o auditivos en contra de las víctimas.

Actualmente, cualquier persona puede acceder a un medio digital, debido a la rapidez en la que viaja la información, coloca a las redes sociales como un medio no solo digital, sino de divulgación de información, es decir, en una herramienta que se emplea para dar a conocer datos personales, desprestigiar o amenazar a cualquier individuo. En la actualidad las Redes Sociales más populares son Facebook, Twitter, Instagram, Pinterest, Youtube, SnapChat, TikTok, y Whatsapp como la principal fuente de comunicación y difusión de información personal.

En el caso de las aplicaciones consideradas de “conquista” como lo son Tinder, Badoo o Lovoo, se emplea el uso del sistema de geolocalización del smartphone para mostrar al otro usuario el lugar aproximado en el que se encuentra la otra persona y la distancia que existe entre ambos, lo que representa uno de los principales riesgos de seguridad. Muchas de las amenazas que ocurren en estas aplicaciones no son tomadas en cuenta por sus receptores, o no les dan ninguna importancia por no ver en ellas ningún tipo de veracidad y peligro. No obstante, existen personas que se pueden sentir intimidadas y que buscan tomar las medidas necesarias para restablecer su seguridad.

Dentro del Código Penal Federal, en el artículo 282, se enuncia lo siguiente:

Se aplicará sanción de tres días a un año de prisión o de 180 a 360 días multa:

I.- Al que de cualquier modo amenace a otro con causarle un mal en su persona, en sus bienes, en su honor o en sus derechos, o en la persona, honor, bienes o derechos de alguien con quien esté ligado con algún vínculo, y

II.- Al que por medio de amenazas de cualquier género trate de impedir que otro ejecute lo que tiene derecho a hacer.

Los ejercicios de amenazas a terceros adquieren, en la sociedad de la información, dos características esenciales: 1) Diversificación de los mecanismos para enviar las amenazas (correo electrónico, mensajería instantánea, redes sociales, videojuegos, etc.). 2) Aumento de información accesible y aprovechable para el diseño de las amenazas. 3) Amenazas dirigidas a personas, activos virtuales y reputación digital.

7.1.8 Discriminación y discursos de odio.

La discriminación surge cuando a una persona se le trata de forma desigual, por condiciones raciales, políticas, sociales y religiosas, entre otras. De acuerdo con Jesús Rodríguez Zepeda *"La discriminación es una conducta, culturalmente fundada, sistemática y socialmente extendida, de desprecio contra una persona o grupo de personas sobre la base de un prejuicio negativo o un estigma relacionado con una desventaja inmerecida, y que tiene por efecto (intencional o no) dañar sus derechos y libertades fundamentales".*

La discriminación no solo se realiza de manera física, sino también digital. Por lo tanto, la discriminación digital se refiere a toda expresión y acción desigual realizada a través de medios y plataformas digitales. Esta se manifiesta a través de acciones como la manipulación de información y contenido de carácter personal, la violencia dirigida a una persona o grupo de personas, de modo que el ciberacoso o cyberbullying forman parte de estas acciones de manera implícita y a consecuencia generan un daño psicológico y violación a sus derechos personales.

Actualmente, las redes sociales son un medio por el cual los usuarios comparten intereses, actividades, experiencias y relaciones interpersonales. En muchas ocasiones publican formas de expresión a través de imágenes, textos, videos, lo que conlleva una forma distinta de socialización e interacción. Sin embargo, no todas las acciones son de manera positiva, ya que existen otras que son expresiones peyorativas que van dirigidas a alguien en específico, por cuestiones de género, raza, condiciones sociales, etc.

La discriminación puede expresarse de manera directa e indirecta. La primera surge cuando el propio usuario crea o publica contenido que afecta a otros usuarios; y la discriminación indirecta es cuando el usuario acepta contenido discriminatorio y ayuda a su difusión mediante sus acciones (compartir, comentar a favor, dar "me gusta" a la publicación, etc.).

La discriminación en medios digitales, ha caido en una conducta normalizada debido a la difusión de contenidos peyorativos que traen consigo altos márgenes de discriminación, violencia, estigmatización y etiquetamiento social, debido a la cotidianidad en la que estos se comparten, la mayoría de los usuarios quienes son parte de esta forma victimización, no son concientes del trasfondo de estos contenidos y las consecuencias que ellos mismos generan.

El ejercicio de discriminación a través de medios digitales, se diferencia de las figuras tradicionales ya que puede alcanzar a un mayor número de usuarios en tiempos relativamente reducidos (por no decir inmediatos). En este sentido, el número de víctimas se amplía ya que el acto puede resultar dañino, indirectamente, para otras personas en mismas condiciones que la víctima directa.

Por otra parte, se encuentran los discursos de odio, mecanismos de violencia que no paran en la negación de derechos sino que se extienden y pretenden la erradicación de personas y colectivos por considerarlos metáforas recurrentes del mal. De acuerdo con Ángela Sierra González *"el siglo XXI se está caracterizando por la legitimación del odio, desde el poder establecido y como estrategia política"* (2007).

Esto, permea en las relaciones entre individuos formando una retórica constante de enemigo y víctima. De acuerdo con UNESCO (2021), entre enero y marzo de 2021, YouTube eliminó 85 247 vídeos que violaban su política relativa al discurso de odio. En ese mismo trimestre, Facebook denunció un total de 25,2 millones de elementos de contenido en relación con los cuales había tomado alguna medida, y en el caso de Instagram fueron 6,3 millones.

En cuanto a la dinámica de los discursos de odio a través de mecanismos convencionales (fuera de línea) y aquellos difundidos a través de medios digitales (en línea), esta misma organización afirma que:

> *El discurso de odio en línea no es muy diferente del que tiene lugar fuera de línea. Su diferencia reside en las interacciones en las que sucede/se lleva a cabo, así como en el uso y la difusión de palabras, acusaciones y teorías conspiratorias específicas que pueden evolucionar, alcanzar máxima popularidad y desvanecerse muy rápidamente. Los mensajes de odio pueden hacerse virales en horas, incluso en minutos* (UNESCO, 2021, p.4).

La propagación de discursos de odio en medios digitales, además de ser rápida también implica un bajo coste y tiene la posibilidad de volver a aparecer después de un tiempo en caso de ser borrado.

7.1.9 Características generales de las formas de victimización entre personas.

Los fenómenos descritos en páginas anteriores comparten una serie de características que les identifican y diferencian de otras formas de victimización, así como de las dinámicas que se revisarán más adelante. Estas son:

- Se desarrollan entre pares o iguales, ya sea individuos o grupos.
- La víctima y el victimario se encuentran claramente diferenciados.

- Son conductas ilícitas convencionales pero los mecanismos de ejecución tienden a ser más sofisticados y hacer uso de las tecnologías de información y comunicación, así como de las plataformas e infraestructura digital.
- Los victimarios pueden ser agentes conocidos o desconocidos.
- Los victimarios aprovechan el aparente anonimato, y facilidad para ocultar la identidad, que brindan las plataformas digitales.
- La brecha digital facilita su proliferación.
- Las conductas son casi siempre dirigidas hacia usuarios específicos.
- Empleo recurrente de ingeniería social como una de las principales herramientas para la obtención de información personal.
- Masificación de potenciales víctimas.
- Generan daños a la intimidad, integridad física, moral y psicológica.

7.2 Dinámicas de victimización empresa-persona.

Las dinámicas de victimización, que se dan en la sociedad de la información, no sólo ocurren entre individuos, en algunos casos incluyen también agentes privados, tal es el caso de empresas proveedoras de servicios, fabricantes de tecnología, proveedores de internet, motores de búsqueda, organizaciones criminales, etc. Estas dinámicas de victimización se encuentran ancladas a delitos informáticos, en tanto que estos se configuran como actos ilícitos que emergen mediante el uso malintencionado de las TIC's. Sin embargo, las conductas tipificadas no son las únicas que generan victimización, existen otras conductas de órden antisocial que aún no son concebidas como dañinas para la sociedad y los individuos pero que en términos objetivos sí generan daño.

Estos ejercicios de victimización pueden agruparse en tres categorías de acuerdo con las características del victimario y la víctima:

A. Organizaciones criminales ejecutan actos victimizantes contra individuos y empresas.
B. Empresas ejecutan actos victimizantes contra individuos y otras empresas.
C. Individuos ejecutan actos victimizantes contra empresas.

A continuación se agrupan las dinámicas de victimización que se exploran en este apartado, de acuerdo con la clasificación anterior.

Tabla 2. Sub-categorías victimización empresa-persona.

A Organizaciones criminales	B Empresas lícitas	C Individuos
- Robo y venta ilegal de datos. - Fraudes. - Estafa. - Ciberataques. - Robo de identidad. - Virus informáticos. - Fabricación de discursos de verdad y fake news. - Uso indebido de activos digitales.	- Robo y venta ilegal de datos. - Uso indebido de datos personales. - Fraudes. - Estafa. - Fabricación de discursos de verdad y fake news. -Uso de datos biométricos con los bancos. - Uso indebido de activos digitales. -Mercadotecnia emocional. -Ataques contra la neutralidad de la red.	- Robo y venta ilegal de datos. - Fraudes. - Estafa. - Ciberataques. - Virus informáticos. - Fabricación de discursos de verdad y fake news.

Fuente: Elaboración propia.

7.2.1 Robo y venta ilegal de datos.

Como habitantes de la sociedad de la información, generamos en todo momento rastros digitales que van construyendo nuestra huella digital. Estos rastros digitales pueden ser de orden consciente e inconsciente. El primero se refiere a toda aquella información que los usuarios comparten de manera directa en publicaciones de redes sociales, formularios, expedientes digitales con terceros, etc. En tanto, los rastros inconscientes se refieren a todos aquellos datos que son recolectados sin

que el usuario tenga conciencia de ello, por ejemplo geolocalización, tendencias de consumo, orientación política, etc.

Lo anterior sin contar la información compartida en páginas web o aplicaciones que forman parte de estratégias de victimización. Actualmente, existe una gran variedad de contenidos como bibliotecas virtuales, chats, correos electrónicos, videoconferencias, firmas electrónicas, foros, blogs, etc., que facilitan cualquier tipo de interacción y obtención de datos, aspectos a los que hay que sumar temas como la edad, género o condiciones socioeconómicas. En este sentido, es pieza clave brindar seguridad a los datos personales alojados tanto en redes sociales, en cuentas de correo electrónico como en aplicaciones de carácter social y financiero, en la medida en que pueden facilitar información a terceros para el acceso no autorizado a cuentas bancarias y comerciales.

Según Amado López (2017), la información viaja de manera codificada entre computadoras, pero depende del nivel de seguridad que se tenga en los dispositivos y las condiciones que los usuarios aceptan al transferir o publicar su información, lo que genera el nivel de seguridad con la que se navega en internet. Si la información es sensible y privada como las contraseñas de cuentas de correos, de redes sociales, de cuentas bancarias, información privilegiada entre empresas o gobiernos, resulta grave que usuarios no autorizados tengan acceso a estos datos, ya que podrían hacer un uso inadecuado y malintencionado para la comisión de delitos.

Un ejemplo es el robo, desvío o fraude bancario que realizan los hackers por medio del robo de datos, de información importante o virus informáticos (Malware) instalados comúnmente en aplicaciones de uso particular.

Para prevenir ser víctima de estos delitos, se recomienda que mientras se navegue en internet:

- Evitar descargar fotos o música o dar clic en ligas de internet que lleguen a correos, redes sociales, o programas de mensajería instantánea que no provengan de un usuario confiable o no se haya solicitado ese tipo de información.

- Evitar descargar cualquier programa que resulte de un anuncio.
- Eliminar programas o aplicaciones que no utilice.
- Proteger los dispositivos o cuentas de internet mediante contraseñas largas que combinen letras, números y símbolos.
- Evitar utilizar la misma contraseña para ingresar a distintos dispositivos o cuentas de correo o bancarias.
- Evitar dar acceso a información personal a las aplicaciones que se instalen en los dispositivos cuando esto no sea necesario.
- Evitar deshabilitar el antivirus o cualquier programa que provea de seguridad al dispositivo.
- Evitar dar clic en el botón de aceptar sobre anuncios que aparezcan mientras se navega en internet.
- Navegar en páginas en cuya dirección al inicio se muestre “https://”.
- Cuidar la información personal que se publique en internet.

De acuerdo con ello, se identifican como principales factores de riesgo: la calidad de contraseñas personales, hábitos de navegación, descarga de aplicaciones no verificadas y brecha digital (específicamente la relacionada con el dominio y conocimiento de la tecnología).

Los delitos que surgen a través de los medios digitales, promueven la comisión de un acto ilícito que atenta contra la información privada de miembros de la sociedad, las organizaciones y el Estado en general. Diariamente los delitos informáticos van en aumento, y esto comúnmente se debe al descuido y la baja protección de la data por parte de los usuarios. De esta manera, los victimarios encuentran oportunidades para extraer información que atenta con la integridad y con la estabilidad de los dueños de la información. Es necesario mencionar que, como usuarios, se tiene la responsabilidad de asegurar que la información proporcionada llegue a su destino y que sea utilizada de manera correcta o para el fin que fueron dados.

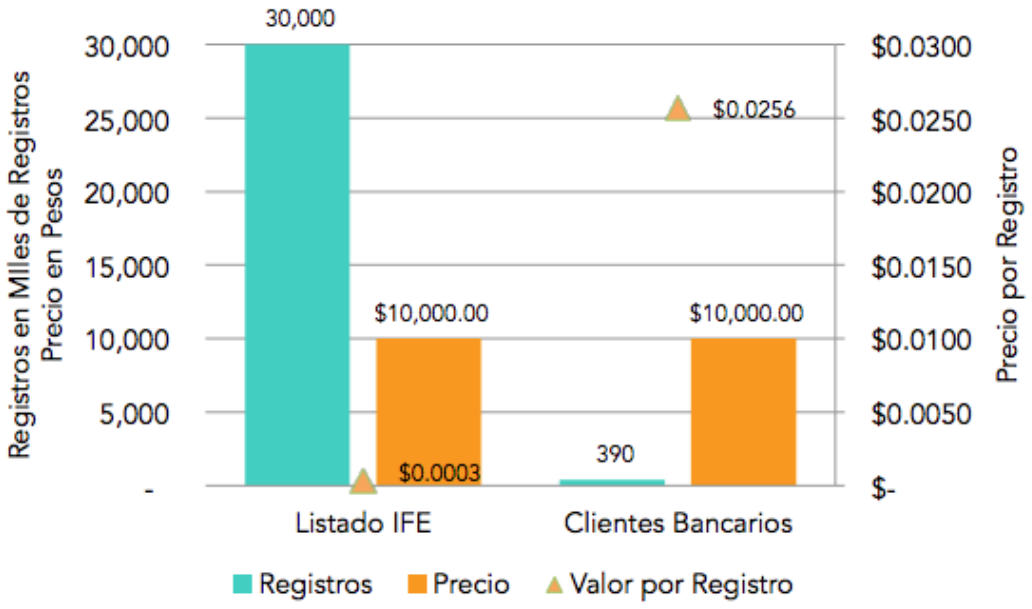
El Reglamento General de Protección de Datos (RGPD) restringirá aún más el uso de datos, para intentar evitar un nuevo caso de Cambridge Analytica, la sociedad de análisis que explotó en su propio beneficio los datos de casi 90 millones de usuarios de Facebook, al que acusaron de negligencia, así como Grindr, la aplicación de

encuentros homosexuales que dejó que empresas terceras accedieron a datos sensibles de sus usuarios, incluyendo datos sobre el virus VIH.

La empresa de seguridad informática Hold Security afirmó en agosto de 2014 que un grupo de piratas rusos habían robado 1.200 millones de contraseñas en 420.000 páginas web del mundo. Según esta misma empresa, el grupo de hackers, apodado CyberVor, habría podido tener acceso a 500 millones de cuentas de correo electrónico. Un anuncio que no tuvo mayores consecuencias.

En México, existe un creciente mercado negro de datos personales generado *"tanto por dependencias del sector público como por empresas privadas, especialmente del sector financiero" (AMIPCI, 2016. p.44).* Por ejemplo, se ha detectado que un listado de 30,000 registros del Instituto Nacional Electoral (antes Instituto Federal Electoral) es vendido en el mercado negro en tan solo $10,000 pesos mexicanos (Tal como se observa en el Gráfico 1). Esto quiere decir que por tan solo 33 centavos de peso mexicano se estaría exponiendo nombre, dirección, fecha de nacimiento, ocupación y clave electoral de una persona.

Gráfico 1. Estimado de precios de datos personales en mercados ilegales en México.



Fuente: AMIPCI, 2016. p.44

7.2.2 Uso indebido de datos personales.

De acuerdo con el INAI, el uso indebido de datos personales se refiere al acto ilícito, la divulgación no permitida o el almacenamiento excesivo y desproporcionado de los datos personales, que lleve a cabo el responsable de su protección, en medio físico o electrónico.

De acuerdo con la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, Capítulo XI, las conductas indebidas en materia del tratamiento de datos personales, son las siguientes:

- *Artículo 67.- Se impondrán de tres meses a tres años de prisión al que estando autorizado para tratar datos personales, con ánimo de lucro, provoque una vulneración de seguridad a las bases de datos bajo su custodia.*
- *Artículo 68.- Se sancionará con prisión de seis meses a cinco años al que, con el fin de alcanzar un lucro indebido, trate datos personales mediante el engaño, aprovechándose del error en que se encuentre el titular o la persona autorizada para transmitirlos.*
- *Artículo 69.- Tratándose de datos personales sensibles, las penas a que se refiere este Capítulo se duplicarán.*

Cuando se habla de datos personales, se hace referencia a la información que hace identificable a la persona como el nombre, su voz, la imagen, el número de tarjeta de crédito y teléfono, los intereses, los gustos y las opiniones, etc. Este derecho incluye a los niños, niñas y adolescentes y posee protección en el entorno virtual.

Es importante mencionar que dentro de los datos personales, existe un subgrupo importante: los datos sensibles. Estos se refieren a datos personales que requieren mayor protección que los demás, ya que revelan información sobre etnia, orientación

sexual, opiniones políticas o religiosas, información referente a la salud o cualquier otra, cuyo conocimiento pueda generar un trato discriminatorio o poner en riesgo la seguridad e integridad del titular de los datos. Por lo tanto, se debe tener especial atención y cuidado en el levantamiento, procesamiento y almacenamiento de este tipo de información.

Si bien, el descuido de los datos sensibles representa mayor riesgo para el usuario, no debe permitirse que ningún tipo de dato personal sea empleado de manera indebida.

Por otra parte, en México el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI) es el organismo que garantiza el cumplimiento del derecho de acceso a la información pública y el de protección de datos personales. Es decir, garantiza el uso adecuado de los datos personales, así como el ejercicio y tutela de los derechos de acceso, rectificación, cancelación y oposición que toda persona tiene con respecto a su información personal y que se consideran esenciales en la autodeterminación informativa.

Un caso relevante en el tratamiento indebido de datos personales es el que involucró a Grupo Meta, de Mark Zuckerberg, y a Cambridge Analytica. En 2016, la empresa británica recogió detalles de más de 87 millones de usuarios de Facebook datos de comportamiento, psicológicos, de preferencias y más minucias que después servirían para manipular las elecciones presidenciales de ese año en las que el candidato presidencial de ese entonces, Donald Trump, se vio involucrado.

La dinámica de recolección siguió una ruta general en todos los casos: en primer lugar, aparecía al usuario publicidad para realizar un test psicológico (en Facebook); una vez que el usuario accedía al test daba consentimiento a Facebook para acceder de manera secundaria a la totalidad de sus datos personales. Es justo este elemento el diferenciador entre el uso indebido de datos personales y el robo y venta ilegal de datos.

En caso del robo y venta ilegal de datos, el titular de los datos personales no da ningún tipo de consentimiento para que un tercero acceda a su información, por lo

que el victimario aprovecha vulnerabilidades y brechas de seguridad para tener control. Por el contrario, en el uso indebido la ocurre alguno, o varios, de los siguientes supuestos:

1) El consentimiento del titular de los datos se obtiene mediante estratégias fraudulentas.
2) Los datos recogidos no guardan proporcionalidad con los fines del procesamiento.
3) Los datos recogidos son empleados para fines distintos a los declarados por el responsable del tratamiento.
4) Los datos son compartidos con terceros no autorizados.

7.2.3 Fraude y estafa.

La Tecnología de la Información y la Comunicación (TIC) está generando una evolución, ya que el ciberespacio se está convirtiendo en un punto de acceso para millones de personas, debido a su flexibilidad en el uso y a la gran cantidad de información disponible para los usuarios.

La modernización ha ocasionado que la información se maneje a través de procesadores informáticos, que almacenan grandes cantidades de información, a la que se puede acceder de manera rápida y efectiva. Esta puede ser de cualquier tipo; personal, empresarial, financiera-bancaria, etc.

Uno de los delitos más frecuentes en la red, es el fraude, el cual amenaza y está presente en la mayoría de las empresas a través de los medios digitales y tiene la característica de ser favorecido por el desarrollo y avance de la tecnología, lo que ocasiona un grave problema para la sociedad actual.

Conforme al Código Penal Federal, en el Capítulo III, hace mención del delito de fraude, enunciando el siguiente artículo:

Artículo 386.

- Comete el delito de fraude el que engañando a uno o aprovechándose del error en que este se halla se hace ilícitamente de alguna cosa o alcanza un lucro indebido.

El delito de fraude se castigará con las penas siguientes:

I.- Con prisión de 3 días a 6 meses o de 30 a 180 días multa, cuando el valor de lo defraudado no exceda de diez veces el salario;

II.- Con prisión de 6 meses a 3 años y multa de 10 a 100 veces el salario, cuando el valor de lo defraudado excediera de 10, pero no de 500 veces el salario;

III.- Con prisión de tres a doce años y multa hasta de ciento veinte veces el salario, si el valor de lo defraudado fuere mayor de quinientas veces el salario.

Algunos factores que conllevan la realización del fraude son las siguientes:

1. Presión: se da por el aspecto económico y la necesidad urgente de pagar o comprar algo, como las tarjetas de crédito, deudas, adicciones, etc.
2. Oportunidad: la facilidad que favorece la comisión del fraude sin ser detectado.
3. Raciocinio: la persona analiza cuál será su plan de acción, este comúnmente se da cuando el delito se comete por primera vez.
4. Capacidad: tener las aptitudes necesarias para llevar a cabo la comisión.

Gabaldon, Luis G, (2006), define el fraude electrónico como la conducta dirigida a la obtención de un provecho económico mediante la apropiación, la falsificación, la interferencia y la reproducción de códigos, instrucciones o programas incorporados a sistemas de procesamiento de datos, que permiten el acceso a dinero en efectivo, bienes y cuentas bancarias.

Existen distintas maneras de realizar los fraudes, estas se dan por medio de las estafas.

De acuerdo con un artículo de Forbes, la Comisión Federal de Comercio de los Estados Unidos (FTC) en 2021, declaró que el 45% de los informes de dinero perdido por estafas en las redes en 2021 fueron sobre compras en línea y en casi el

70% de estos informes, las personas dijeron que hicieron un pedido, generalmente después de ver un anuncio, pero que nunca recibieron la mercancía.

Algunos informes incluso describieron anuncios que se hacían pasar por minoristas en línea reales que conducían a las personas a sitios web similares. Cuando las personas identificaron una plataforma de redes sociales específica en sus informes de productos no entregados, casi 9 de cada 10 mencionaron Facebook o Instagram.

Por otra parte, y de acuerdo con el Código Penal Español, la estafa consiste en engañar a otro con ánimo de lucro, induciéndolo a realizar un acto de disposición en perjuicio propio o ajeno.

Las estafas en Internet son otra forma de victimización y estas son diferentes metodologías de fraude que pueden ocurrir de distintas maneras, por medio de correos electrónicos de suplantación de identidad (phishing), redes sociales, mensajes SMS, llamadas telefónicas falsas, información consultada en el sitio web Norton.. Los objetivos de las estafas van desde el robo de tarjetas de crédito, robo de datos, de información, de contraseñas, dinero, entre otros.

Entre los tipos más comunes de estafas en línea, se encuentran los siguientes:

-Estafas en redes sociales

Estas se presentan a través de diferentes noticias que aparecen en el inicio de cada perfil de los usuarios, favoreciendo la visibilidad de las mismas, todo esto con el objetivo de lograr que se dé clic en los vínculos de dichas noticias, las cuales en la mayoría de los casos contienen virus.

-Phishing

La estafa en línea más difundida es el “phishing”. Esta modalidad se opera con correos electrónicos, en los que se engaña al usuario para que crea que está ingresando a un sitio web de confianza con el que normalmente opera. Esto podría ser un banco, su cuenta de redes sociales, un sitio web de compras en Internet, empresas de transporte, empresas de almacenamiento en la nube, etc.

La finalidad del phishing es la de apoderación de información personal de un usuario de Internet, para acceder a sus cuentas de correo o de redes sociales y obtener sus datos personales o de sus contactos virtuales, a fin de comercializar ilícitamente la información obtenida a un tercero (mula), o bien, conseguir claves de “e-banking” para ingresar a las cuentas bancarias de los titulares y disponer del dinero que en ellas se encuentra.

-Antivirus falsos

Scareware, estos dan comienzo con una advertencia emergente que dice que el usuario tiene virus en su dispositivo digital (celular, ipad, laptop, computadora, etc.). Después, la ventana emergente sugiere al usuario hacer clic en un vínculo que se despliega a la par del anuncio del virus, dicho link promete realizar una limpieza del virus detectado.

Los delincuentes informáticos aprovechan la necesidad de los usuarios para conseguir un “Antivirus gratuito”, para así poder implantar un mal software en el dispositivo de la víctima.

Las estratégias fraudulentas y de estafa son múltiples, muchas de ellas aprovechan la brecha digital de corte generacional y otras tantas explotan los atributos de la ingeniería social.

7.2.5 Ciberataques.

La historia de los ciberataques está marcada, en sus inicios, por dos eventos relevantes. El primer evento tuvo lugar en diciembre de 2005, parte de Ucrania no tuvo energía eléctrica por aproximadamente seis horas, a causa de un ciberataque contra la compañía nacional de energía, producido por un malware que tuvo la capacidad de proporcionar el control a un usuario ajeno a los equipos de cómputo de la compañía y con ello lograr desactivar sus sistemas y borrar archivos de sus computadoras. El segundo ocurrió en 2007 en Estonia, donde se presentó un ciberataque dirigido en contra de su infraestructura política y económica (parlamento y bancos).

Estos eventos son considerados de gran importancia ya que, actualmente, los ciberataques considerados como más graves, son aquellos que involucran infraestructura crítica, apoderamiento de información de alto grado de importancia, privación de servicios básicos, interrupción de comercio electrónico, exposición de secretos de Estado, interferencia en líneas telefónicas, etc.

De acuerdo con el Consejo de Investigación de Instituciones Financieras de los Estados Unidos de Norteamérica (FFIEC por sus siglas en inglés), un ciberataque es:

> *El intento de dañar, interrumpir u obtener acceso no autorizado a una computadora, sistema informático o red de comunicaciones electrónicas. Es un ataque a través del ciberespacio, dirigido a una institución con el propósito de interrumpir, deshabilitar, destruir o controlar maliciosamente un entorno/infraestructura de computación, o bien destruir la integridad de los datos o robar la información controlada* (FFIEC, 2022).

Estos fenómenos cibernéticos se caracterizan por cuatro elementos básicos: 1) bajo costo, 2) ubicuidad y fácil ejecución, 3) efectividad e impacto y, 4) reducido riesgo para el atacante.

Por otra parte, de acuerdo con Frieiro (2017), se pueden identificar a los principales agentes atacantes de acuerdo con la motivación y objetivos que persiguen:

- Estados: buscan una posición estratégica y/o geopolítica.
- Organizaciones criminales: buscan un beneficio económico.
- Ciber terroristas y Ciberyihadistas: buscan atemorizar e influir en las decisiones políticas.
- Ciber activistas: motivación ideológica.
- Ciber vándalos: buscan evidenciar vulnerabilidades, explotar la piratería, diversión, reto.
- Organizaciones privadas: buscan información de valor o secretos profesionales de la competencia.
- Agentes internos: buscan venganza o beneficio económico.

Estos agentes atacantes operan, según INCIBE, *al acecho de nuevas formas con las que atacarnos a los usuarios aprovechándose de nuestro desconocimiento o vulnerabilidades en nuestras defensas. Sus objetivos son muchos y pueden tener distintas consecuencias para el usuario* (INCIBE, SD, p.3). Estos ataques se dividen en cuatro tipos: ataques a contraseñas, ataques por ingeniería social, ataques a las conexiones y ataques por malware. A su vez, cada una de estas categorías contiene subtipos de ciberataques (Ver tabla 3).

Tabla 3. Tipos de ciberataques.

Tipo de ciberataque	**Subtipos de ciberataque**
Ataques a contraseñas	• Fuerza bruta. • Ataque por diccionario.
Ataques por ingeniería social	• Phishing, Vishing y Smishing. • Baiting o Gancho. • Shoulder surfing o mirando por encima del hombro. • Dumpster Diving o rebuscando en la basura. • Spam o correo no deseado. • Fraudes online.
Ataques a las conexiones	• Redes trampa (Wifi falsas). • Spoofing o suplantación. - IP Spoofing . - Web Spoofing. - Email Spoofing. - DNS Spoofing. • Ataques a Cookies. • Ataques DDoS. • Inyección SQL. • Escaneo de puertos. • Man in the middle o ataque de intermediario. • Sniffing
Ataques por malware	• Virus. • Adware o anuncios maliciosos. • Spyware o software espía. • Troyanos. - Backdoors. - Keyloggers. - Stealers. - Ransomware. • Gusano.

	● Rootkit. ● Botnets o redes zombi. ● Rogueware o falso antivirus. ● Criptojacking. ● Apps maliciosas

Elaboración propia con información de INCIBE.

Si bien, no es objetivo de esta investigación profundizar en las características y dinámicas de cada uno, sí es importante dimensionar la importancia de estos eventos. La encuesta sobre la percepción de riesgos globales del World Economic Forum 2017-2018, tanto los ataques cibernéticos como el fraude masivo de datos aparecen en tercer y cuarto lugar, respectivamente, de la lista de principales riesgos globales según la probabilidad percibida. Por otro lado, en términos de impacto, el daño por ciberataques ocupa el sexto lugar, sólo por debajo de los riesgos asociados al clima o la naturaleza y de armas de destrucción masiva.

Por otra parte, también es necesario hacer una diferenciación entre los ciberataques de órden delincuencial y los de origen terrorista. En este sentido, el ciberterrorismo va más allá de la ciberdelincuencia. Este es la conjunción del ciberespacio y el terrorismo, es decir, la forma en la que el terrorismo utiliza las TIC'S para atemorizar, coaccionar o causar daños a grupos sociales con fines políticos y religiosos. Esto modifica las formas en las que se ha llevado el terrorismo comúnmente, dando pauta a la utilización de las redes y medios digitales para llevar acabo sus ataques de carácter político y religioso, contra un grupo, Estado o nación.

Algunas de las actividades que desarrollan los ciberterroristas en el internet son:

a) Financiación: esto se desarrolla por medio de la extorsión a grupos financieros, transferencias de dinero, transferencias financieras a través de bancos offshore, lavado de dinero, uso de dinero electrónico (bitcoin), ventas falsas de productos, etc.

b) Guerra psicológica: se exhibe información falsa a través de las redes, así como de los medios sin censura, así mismo, se exponen amenazas y comparten imágenes de sus atentados.

c) Reclutamiento: a través de los medios digitales reclutan a usuarios para que formen parte de su organización, ya que reúnen información sobre los usuarios para elegir a los más adecuados para trabajar con ellos.

d) Interconexión y comunicación: los correos electrónicos encriptados fungen como su herramienta principal de comunicación. A través de la comunicación se coordinan para llevar a cabo sus acciones.

f) Fuente de información y entretenimiento: el internet ofrece a los ciberterroristas la facilidad de adquirir información para su beneficio, tales como mapas, localizaciones, datos personales, fotografías, visitas virtuales, creación de armas y bombas, entre otras.

Un ejemplo, reciente, que sirve para dimensionar este tipo de fenómenos es el de SolarWinds (empresa fabricante de Orion), un software utilizado por miles de empresas, entre ellas las que integran la lista de Fortune 500 y organizaciones gubernamentales de Estados Unidos como la NASA, las fuerzas aéreas o el Pentágono.

Según el periodico Forbes, Forbes Staff, (2021), la compañía dedicada al software recibió un ataque con malware el cual contaminó una de sus actualizaciones, de esta forma los ciberdelincuentes recopilaron grandes cantidades de información de sus clientes. Más de 18,000 organizaciones entre las que destacan varias agencias gubernamentales y del sector privado de EE.UU. se vieron afectadas en este ataque que duró meses antes de ser descubierto a finales de 2020.

7.2.6 Suplantación de identidad.

En primer lugar, es importante mencionar que, esta dinámica de victimización no se encuentra en el apartado de Persona-persona, ya que si bien existen muchos ejercicios de suplantación que se dan entre particulares, la mayor proporción de casos se realizan en un ejercicio originado desde organizaciones criminales que ejecutan estos mecanismos no como fines en sí mismos sino como herramientas para la comisión de conductas delictivas quizá más graves, por ejemplo la trata de personas.

Ahora bien, de acuerdo con la Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros (CONDUSEF), la suplantación de identidad es un método de fraude en donde una persona obtiene, utiliza y se apropia de manera ilícita de los datos personales de otra, sin su autorización y con el propósito de cometer un fraude o delito implicando al sujeto en cuestión. Sin embargo, se han registrado casos en que la suplantación se da con el mero fin de apropiarse de "bienes digitales" (juegos, música, etc.), o bien de gozar de los beneficios sociales y de popularidad que posee el titular de los datos personales.

Para entender este fenómeno, es necesario comprender que la identidad abarca todos los datos personales, tales como: nombre, domicilio, teléfono, fotografías, en algunos casos las huellas dactilares, la información financiera, información médica, credenciales de identificación, las licencias y tarjetas de crédito o débito que maneje la persona, así como cualquier otro dato que nos brinde información sobre el sujeto y que permite dar personalidad jurídica, moral y física a la persona.

En este sentido, dentro de los objetivos principales de los victimarios se destaca el apropiarse ilegalmente de estos datos para obtener productos y servicios financieros, transferir recursos de las cuentas a nombre de la víctima a un tercero, o también para hacer compras, con la ventaja de que estos no sean rastreados. Un modus operandi muy común es hacerse pasar por personal de una institución bancaria y solicitar datos por vía telefónica, ya sea en llamada o mensaje de texto, correo e incluso redes sociales, engañando y haciendo creer que se es acreedor de algún tipo de premio o beneficio, o para querer validar una operación que supuestamente se realizó en alguna institución bancaria. En consecuencia, solicitan proporcionar datos como el nombre, dirección, números de tarjetas de crédito, nip´s, cuentas bancarias, nombres de usuarios, contraseñas, entre otros, permitiendo la detección de patrones o tendencias de comportamiento.

Además de las técnicas recién descritas, también se aprovecha como instrumento para la suplantación la minería de datos, o datamining por su nombre en inglés, mediante la cual se permite una exploración automática o semiautomática de

grandes cantidades de datos personales, entre los que figuran: direcciones, rutas de tránsito, nombres, preferencias de búsqueda y consumo, etc.

Como ejemplo, de cómo este tipo de mecanismos operan en la realidad se presentan datos del caso mexicano: tan sólo en el primer semestre de 2021, el Infonavit había registrado 40 casos de robo de identidad en compra de vivienda por un monto global de 59 millones 425 mil 426 pesos. Valle de México con 8 casos; Jalisco, con 6 casos; así como Tabasco, Chiapas y Veracruz con 4, cada uno.

Estos datos dejan ver que uno de los principales campos afectados a causa de la suplantación de identidad es el económico, sin embargo, el potencial de daño puede ser aún más profundo. De acuerdo con Giménez *la identidad puede definirse como un proceso subjetivo (y frecuentemente auto-reflexivo) por el que los sujetos definen su diferencia de otros sujetos (y de su entorno social) mediante la auto-asignación de un repertorio de atributos culturales frecuentemente valorizados y relativamente estables en el tiempo* (2010, p.4). En cuanto se ejecutan procesos para suplantar la identidad de las personas, la diferenciación con otros sujetos se rompe toda vez que pueden existir dos o más personas presumiendo ser la misma y demandando reconocimiento. Además la suplantación de identidad fragmenta también la auto-asignación de atributos en tanto que quien ha logrado la suplantación puede adjudicarse nuevas características incluso antagónicas, esto representa afectaciones no solo a la esfera económica sino también psíquica del individuo.

Por otra parte, cuando la suplantación de identidad se realiza con la finalidad de generar otro tipo de victimización, las consecuencias pueden trascender de lo económico y psicológico al terreno sexual e incluso representar la pérdida de la vida misma.

7.2.7 Construcción de discursos de verdad y Fake news

Castillo V. y Hermosilla P. (2021) afirman que las noticias falsas (fake news) se pueden entender como una alteración intencionada de un hecho real o la invención de un hecho ficticio con el fin de confundir o desinformar a las personas,

generalmente se presentan en formatos que igualan a la noticia tradicional. Estas noticias tienen distintos propósitos como favorecer intereses políticos, influir en algún debate político, obtener ganancias económicas, generar dudas y controversias con el fin de conseguir beneficios económicos o ideológicos, entre otras.

Las fake news no son un fenómeno reciente, sin embargo su aumento se debe al impacto y crecimiento acelerado del internet, de los medios digitales así como los usuarios que cada día incrementan y forman parte de las audiencias de las redes sociales. Estas últimas son espacios que facilitan y promueven que las noticias e información en general se hagan virales en tiempo real. Dichas plataformas forman parte de las principales fuentes de información de los usuarios, debido a que su acceso es abierto y todo tipo de persona puede ingresar a estas redes y por lo tanto de distribuir información no necesariamente verídica. En consecuencia, la difusión de fake news y rumores pueden generar incertidumbre en la sociedad, aumentar la desconfianza hacia las instituciones y gobiernos, e incluso poner en riesgo la vida e integridad de las personas.

El aumento de las noticias falsas que se presentan como información verídica y comprobada, facilitan la manipulación de la información que se genera a partir de bases, referencias falsas o erróneas, generando que al usuario le sea complicado identificar si se trata de un discurso cierto o falso.

La hipercomunicación, propia de la era digital facilita la rápida generación y réplica de información, además de facilitar entornos de posverdad donde prima la tendencia a valorar más las emociones y las creencias personales que los hechos objetivos al momento de formar una opinión o tomar una decisión. Al respecto, Daniel Innerarity argumenta que en la sociedad actual, caracterizada por la abundancia de información y la complejidad de los problemas, incluso los discursos científicos pueden caer en este tipo de dinámicas:

> Nunca el conocimiento había sido tan importante y a la vez tan sospechoso; nunca lo habíamos necesitado tanto y desconfiado al mismo tiempo de él; nunca habíamos depositado tantas esperanzas

> en el conocimiento como solución mientras se convertía él mismo en un problema (2022, p. 9).

En este sentido, la construcción malintencionada de discursos de verdad, así como las fake news, construyen y refuerzan un panorama de post verdad. Ésta a su vez consiste en la *relativización de la veracidad, en la banalización de la objetividad de los datos y en la supremacía del discurso emotivo* (Zarzalejos, 2017).

En síntesis, la manipulación de información y la falta de veracidad de las noticias falsas pueden afectar la percepción de la realidad y la toma de decisiones, además de generar polarización y conflictos sociales.

8.2.8 Mercadotecnia emocional

Pablo Sevilla (2015) define al marketing como el conjunto de técnicas o estrategias que se utilizan para estudiar el comportamiento de los mercados, la gestión comercial de las empresas y las necesidades de los consumidores. Frecuentemente, el marketing engloba acciones que se relacionan con la publicidad, estratégias que se desarrollan de forma planificada y abarcan una multitud de aplicaciones más allá de la publicidad.

Actualmente los términos como social media marketing, marketing móvil, email marketing, marketing directo, son cada día más populares y se encuentran con más facilidad. En general, todas estas herramientas, tienen como objetivo principal satisfacer las necesidades de las empresas y, en menor medida, cubrir las necesidades de los consumidores. El marketing hace referencia a todas aquellas actividades, estrategias o técnicas que tienen como fin u objetivo mejorar y facilitar el proceso de venta. No obstante, no se refiere solamente a la publicidad del producto para aumentar su compra, sino también identificar las necesidades de los clientes. identificar qué necesitan, por qué, cómo o por qué lo necesitan.

Es por ello, que el marketing no se dedica solo a la mejora de venta, sino que abarca todo lo relacionado con mejorar el proceso de venta de un producto o servicio, abarca el estudio de la necesidad que va a cubrir, el segmento de mercado al que va dirigido, su producción, su formato de venta, su logística, su comercialización y el servicio post-venta.

Ahora bien, de acuerdo con el sitio de internet acumbamail, el marketing emocional es un tipo de marketing que se enfoca en la utilización de las emociones de los clientes para crear un vínculo con el producto, se trata de movilizar a las personas a través de sus sensaciones, emociones y sentimientos. El consumidor se deja guiar por sus emociones para evaluar un producto o servicio, ya que a través de comentarios en redes sociales comparte su punto de vista e incluso da o publicidad gratuita al servicio o producto adquirido. Asimismo, las empresas aprovechan la oportunidad que brindan las nuevas tecnologías para dar una atención al público en las distintas plataformas virtuales.

El marketing emocional se plantea estrategias que buscan lograr un vínculo afectivo-emocional con mensajes que lleguen a los sentimientos del consumidor y así lograr el objetivo de la adquisición. Sin embargo, la mercadotecnia no solo se enfoca en sentimientos positivos sino también en los negativos como la pena, la culpa o la injusticia. Además puede emplear herramientas como las descritas en el apartado anterior, referentes a la creación de discursos de verdad y noticias o contenido falso.

En este sentido, puede hablarse del marketing emocional como proceso victimizante cuando se utiliza de manera manipuladora o engañosa para inducir a los consumidores a realizar una compra o tomar una decisión que no beneficia sus intereses. En este sentido, algunos de los problemas asociados son: manipulación emocional, creación de necesidades artificiales, fomento de la cultura consumista y creación de estereotipos.

En el caso de este último, el marketing emocional tiene el potencial de perpetuar estereotipos de género, raza, edad, apariencia corporal, entre otros, a través de la creación de imágenes y mensajes estereotipados.

7.2.9 Bancos de datos biométricos.

Cortes Osorio, Medina Aguirre y Francisco A (2010) describen que el concepto biometría viene de las palabras bio (vida) y metría (medida), el cual consiste en técnicas que miden e identifican las características físicas únicas de organismos vivos o patrones de su comportamiento, que permiten identificar los diferentes individuos. Debido a esto, los sistemas de seguridad basados en biometría son un medio eficaz y eficiente para las empresas en cuanto al reconocimiento del ser humano. Dentro de estos, se destaca: el reconocimiento facial o de rostro, el reconocimiento de la voz, el análisis del patrón del iris, el reconocimiento de huellas dactilares, el análisis del mapa de la retina del ojo, el análisis de la forma del oído, el análisis de la forma de la mano, la geometría de los dedos, la forma de la cabeza, entre otros.

La biometría se encuentra vinculada también al área de la criptografía y seguridad informática, de forma que puede considerarse para un sistema de seguridad aplicando tecnologías biométricas en las organizaciones. Así, los sistemas biométricos tienen dos objetivos:

- El primero es para identificar, es decir, reconocer al individuo, por lo que su funcionamiento está basado en utilizar un dato y compararlo con una lista o base de datos.
- El segundo es para autenticar, es decir, verificar la identidad del individuo, por lo que su funcionamiento está basado en la utilización de un dato comparándolo con el mismo dato almacenado previamente (Díaz, 2012).

Estas características han popularizado el usos de sistemas basados en biometría en entornos de seguridad, producción, tránsito, corporativos, escolares, etc. Sin embargo, en tanto estos bancos crecen, es cada vez más difícil protegerlos, dado que la información se encuentra no solo en dispositivos estáticos (servidores, computadores) sino en dispositivos móviles (USB, laptop, ipad, celulares, etc.) y

plataformas digitales (cloud computing) que pueden almacenar información muy valiosa. En este sentido, se enfrentan distintos retos y desventajas:

1. Costes. Es necesario hacer una inversión significativa en biometría para seguridad
2. Violación de datos. Las bases de datos biométricas pueden ser hackeadas
3. Monitorización y datos. Los dispositivos biométricos, como los sistemas de reconocimiento facial, pueden limitar la privacidad de los usuarios
4. Sesgo. El aprendizaje automático y los algoritmos tienen que ser muy avanzados para minimizar el sesgo demográfico biométrico
5. Positivos falsos e imprecisiones. Es posible que ocurran falsos rechazos y falsas aceptaciones que impidan a los usuarios acceder al sistema (Mitek Systems, 2021).

Costes

Hace referencia al aumento gastos e inversión que requiere elaborar e implementar un servicio de seguridad biométrico, el cual varía dependiendo el tipo de seguridad que se quiera llevar a cabo.

Violación de datos

Si una contraseña o PIN han estado expuestos, siempre existe la posibilidad de cambiarlos, algo que no se puede implementar con los datos biométricos conductuales o fisiológicos de una persona. Por lo que el robo de estos datos puede ser posible por medio de un hacker.

Monitorización y datos

A medida que la vigilancia aumenta, los datos biométricos pueden usarse para monitorizar a las personas, con o sin su conocimiento.

Sesgo

Sin una solución verificada para la comprobación de identidad basada en documentos de identificación, el desempeño demográfico cruzado puede ser poco

fiable, lo que a su vez limitaría el acceso de los clientes a servicios como créditos y servicios digitales.

Falsos positivos e imprecisiones

Los métodos de autenticación biométrica más comunes dependen de información parcial para autenticar la identidad del usuario, un dispositivo móvil biométrico puede escanear una huella digital completa durante la fase de registro y convertirla en datos.

En sentido general, además de los costos, potencial violación y monitorización de datos, sesgos y falsos positivos, estas dinámicas de generación exacerbada y generalizada de los bancos de datos biométricos, tienen alto potencia vicitmizante debido a los siguientes puntos:

- Los registros biométricos son reforzados a través de discursos de securitización no necesariamente confiables, ni verdaderos.
- Las empresas restringen cada vez más los accesos físicos y digitales, poniendo de por medio controles biométricos. Esto se convierte en imposiciones para los sujetos; de negarse a ceder sus datos, el servicio es negado.
- Los datos biométricos no cambian, ni caducan con el tiempo por lo que una vez recolectados, estos pueden ser usados en el momento necesario y en más de una ocasión.
- Son mecanismos intrusivos para los derechos y libertades fundamentales de los individuos.
- Los datos biométricos y otros datos recopilados facilitan el perfilamiento digital.

Si bien, los bancos de datos biométricos no constituyen en sí mismos procesos de victimización, sí colocan a los usuarios en posiciones vulnerables, y expuestos al uso indebido de datos que sí pueden constituir victimización. Además, se considera que la generación exacerbada de estos, así como la condicionante de ceder los datos biométricos para poder acceder a determinados derechos o servicios sí constituye en sí misma una dinámica de victimización.

7.2.10 Uso indebido de activos digitales.

Los nuevos avances tecnológicos también han modificado la economía y los agentes en que ésta se mueve con la sociedad y los mercados. Cortes Ordoñez (2018), ejemplifica la forma en que se realizan transacciones utilizando las nuevas tecnologías: hoy en día, gran parte de las transacciones, pagos, compras y transferencias se realizan a través de internet, de aplicaciones bancarias; y términos como dinero virtual, comercio electrónico, negocio electrónico, entre otros, son cada vez más frecuentes.

Esta nueva moneda virtual tiene una característica importante y es que no depende de la regulación de un país porque su uso es anónimo, que permite pagos nacionales e internacionales y fáciles mediante un cuenta bancaria virtual que se encuentra en la nube o en la computadora de un cliente.

Las criptomonedas hacen posible el Internet del Valor o el llamado Internet del Dinero, que son aplicaciones de Internet que facilitan y posibilitan el intercambio de valor en la forma de criptomonedas. Este valor puede ir desde contratos, propiedades intelectuales, acciones o cualquier propiedad en general que contenga algún valor. Anteriormente, las cosas de valor se podían pagar a través de sistemas de pago como Paypal, que es un servicio donde te permite pagar, enviar dinero y aceptar pagos sin tener que introducir tus datos financieros continuamente; sin embargo la diferencia entre pagar con Paypal y criptomonedas es que en la primera se requiere que el pago se haga a través de redes privadas como tarjetas de crédito o cuentas bancarias, mientras que en las criptomonedas no hay intermediarios.

Como menciona López Rodríguez (2020), el uso de las criptomonedas en la actualidad ha generado la posibilidad de satisfacer necesidades a la sociedad a través de la disminución de costos, riesgos y tiempos en las transacciones financieras y más aún tomando en cuenta que el uso de las criptomonedas es un

fenómeno que atrae la atención de medios de comunicación, empresas, industrias financieras, instituciones gubernamentales, etc.

Sin embargo, se debe tomar en cuenta que como toda ventaja también hay desventajas y en el uso de criptomonedas no hay excepción. Estas desventajas consisten en que no son moneda de curso legal, debido a que en muchos casos no están respaldadas por los bancos centrales; la imposibilidad de revertir una operación realizada en criptomoneda ya ejecutada; el inestable valor de las criptomonedas; así como los riesgos tecnológicos, cibernéticos y fraudes electrónicos inherentes al uso de las criptomonedas (Alanis, 2019).

Los medios de digitales, las redes sociales, el internet, etc, han generado en torno a las criptomonedas un impulso frente a sus beneficios y ganancias, sin embargo los riesgos financieros, la confianza del mercado, la credibilidad y sobretodo la ausencia de marcos normativos que respaldan su uso y crecimiento, limitan su potencial como moneda útil dentro del sistema monetario internacional. Si bien, las criptomonedas siguen creciendo y desarrollándose de manera imparable como un producto en un mercado de movimientos económicos, se debe considerar y analizar los impactos sociales que pueden generar a la población y a los usuarios.

Al respecto de los activos virtuales, específicamente del Bitcoin, la Comisión Nacional de la Protección y Defensa de los Usuarios de Servicios Financieros (CONDUSEF, 2022) afirma que al no estar reguladas por las autoridades financieras, las operaciones son irrevocables y no existe forma en que los usuarios puedan reclamar en caso de que sospechen que han sido víctimas de alguna conducta. Así mismo, describe que las autoridades no pueden responder por algún cambio en su valor y que este tipo de activos han sido señalados en operaciones ilícitas como lavado de dinero y fraude.

7.2.11 Ataques contra la neutralidad de la red

De acuerdo con la Red en Defensa de los derechos Digitales R3D (2015), la neutralidad de la red, es un principio identificado con una serie de políticas sobre

Internet encaminadas a generar un régimen de no discriminación por parte de los proveedores de acceso a Internet (ISP), a fin de mantener una forma de competencia en la oferta de aplicaciones, contenidos o servicios.

La Comisión Interamericana de los Derechos Humanos, CIDH, en su informe de 2013 Libertad de Expresión en Internet, señala que "La protección de la neutralidad de la red es fundamental para garantizar la pluralidad y diversidad del flujo informativo". Por su parte, el principio 5 de la Declaración de Principios dispone que *"las restricciones en la circulación libre de ideas y opiniones, como así también la imposición arbitraria de información y la creación de obstáculos al libre flujo informativo, violan el derecho a la libertad de expresión".*

En tanto la legislación mexicana, a través de la Ley Federal de Telecomunicaciones y Radiodifusión (LFTR) Art. 145, aborda la neutralidad de la red especificando que los concesionarios y autorizados que presten el servicio de acceso a internet deberán sujetarse a determinados lineamientos. Entre estos lineamientos destaca el de la libre elección, mismo que se refiere a:

> *Los usuarios de los servicios de acceso a internet podrán acceder a cualquier contenido, aplicación o servicio ofrecido por los concesionarios o por los autorizados a comercializar, dentro del marco legal aplicable, sin limitar, degradar, restringir o discriminar el acceso a los mismos.*
> *No podrá limitar el derecho de los usuarios del servicio de acceso a internet a incorporar o utilizar cualquier clase de instrumentos, dispositivos o aparatos que se conecten a su red, siempre y cuando éstos se encuentren homologados* (LFTR, Art. 145).

En este sentido, un ataque contra la neutralidad de la red podría entenderse como cualquier acción que vaya en contra del principio de tratar todos los contenidos y servicios en internet de manera igualitaria, sin discriminación o preferencia por parte de los proveedores de servicios de internet. Estos ataques pueden adoptar distintas formas y dinámicas, por ejemplo:

1. Bloqueo o limitación del acceso a ciertos contenidos o servicios online, en función de intereses particulares (Comerciales, económicos, políticos, etc).
2. Reducción de la velocidad de acceso a ciertos contenidos, servicios o usuarios, favoreciendo a otros.
3. Priorización de tráfico: ralentizar o bloquear el acceso a ciertos servicios para favorecer a otros o bien para solicitar pagos extra a cambio de una velocidad normal.

R3D comparte la postura de la Relatoría Especial para la Libertad de Expresión de la CIDH, en tanto no debe haber discriminación, restricción, bloqueo o interferencia en la transmisión de Internet, a menos que sea estrictamente necesario y proporcional para preservar la integridad y seguridad de la red; para prevenir la transmisión de contenidos no deseados por el usuario; y para gestionar temporal y excepcionalmente la red.

Un caso importante fue documentado en 2017 por BBC Mundo: La Comisión Federal de Comunicaciones de Estados Unidos (FCC) revocó la normativa de 2015 que protegía la neutralidad de la red y aseguraba el acceso igualitario a internet de todos los individuos y compañías. Con ello las empresas que suministran el servicio tienen la libertad de experimentar con nuevos precios, priorizar o bloquear contenido, sin tener que rendir cuentas.

De acuerdo Singel, especialista de la Universidad de Stanford, uno de los primeros efectos será una subida en los precios de conexión, Netflix, por ejemplo, se volverá más cara. Cómo tendrán que pagar tarifas más altas por utilizar internet de mejor calidad para ofrecer sus servicios, necesitarán cobrar más también a sus usuarios para mantenerlo. Así que veremos que Internet se volverá mucho más caro en los servicios por los que se paga.

En este sentido, los ataques contra la neutralidad de la red son graves ya que amenazan la igualdad de acceso a la información y libertad de expresión. Además, abren la puerta para que los proveedores de servicios de internet gestionen los contenidos o servicios en línea en función de intereses comerciales o políticos,

generando barreras artificiales para el acceso a la información, topes a la creatividad e innovación en línea, así como desigualdad en el acceso a información.

7.2.12 Características generales de las formas de victimización entre empresas y personas.

Los fenómenos descritos en páginas anteriores comparten una serie de características que les identifican y diferencian de otras formas de victimización, así como de las dinámicas que se revisarán más adelante. Estas son:

- Sustentadas en la obtención de datos personales de usuarios y comercio ilegal de información.
- Exposición de información personal, laboral, académica, y financiera.
- Creación de perfiles individuales y colectivos con potencial de predicción conductual.
- Manipulación digital-emocional con motivaciones comerciales y políticas.
- Estrategias de bajo costo.
- Ubicuidad y fácil ejecución.
- Alta efectividad e impacto sobre grandes masas de población.
- Reducido riesgo para el atacante.
- Victimario difícilmente identificable.
- Las víctimas no siempre son conscientes de los eventos victimizantes y no siempre se asimilan a sí mismas como tal.
- Riesgos globales: tanto percibidos como reales.
- Riesgo para la democracia, el acceso a la información y la libertad de expresión.
- Favorecen y amplían las asimetrías y desigualdades sociales.
- Conductas no siempre dirigidas a individuos particulares sino destinadas a afectar grandes masas, casi siempre de manera fortuita.
- No siempre son reconocidos como delitos, abuso de poder o hechos victimizantes. Sin embargo, al tener potencial de daño y de restringir el desarrollo pleno del sujeto lo son.

7.3 Formas de victimización desde el Estado

En esta tipología se encuentran formas de victimización que se generan desde el Estado, mismo que su ejercicio de poder y a través de sus estructuras produce nuevas formas de victimización.

7.3.1 Sistemas de control e hipervigilancia

Dos de las características más distintivas de la era digital son la hipervigilancia y la transparencia, mismas que se sustentan en la vigilancia multifocal a través de miles de dispositivos conectados a la red y que recolectan datos en todo momento (Han, 2012). Estos dispositivos levantan información a través de sensores y lentes, siendo las cámaras de videovigilancia y los sistemas de inteligencia artificial (IA) los principales elementos operativos.

En este sentido, Henry Arguello Fuentes (2011), explica que actualmente es posible generar estas pautas de hipervigilancia a través de diversas fuentes; imágenes de las huellas digitales, iris de los ojos, palma de la mano, el rostro, la voz o firma manual, la principal ventaja de esta técnica es la facilidad de implementación y el bajo coste computacional, por lo cual permite la creación dichos sistemas.

Según Cortés Osorio, Medina Aguirre y Francisco Alejandro (2010), el reconocimiento del rostro presenta ventajas sobre otros sistemas biométricos, debido a que es una técnica no invasiva y puede ser utilizada tanto en aplicaciones públicas gratuitas como apps privadas, sin embargo, algunos elementos vuelven complejo el proceso de reconocimiento de rostro, ya sea por las distintas fuentes de iluminación, las sombras, el cambio en la textura de la piel, el cabello, los maquillajes y el envejecimiento prematuro.

Por otra parte, Daniela M (2016), menciona que los sistemas de video vigilancia inteligente se convirtieron en un tema importante de investigación ya que apoya el sector de la seguridad, estos elementos en conjunto proporcionan un sistema completo para la identificación de personas en espacios operados con videovigilancia, así como en entornos multi-cámara. La videovigilancia resulta muy importante para el gobierno, ya que ayuda a dar cuenta del cumplimiento de la ley, mantener el control social, asimismo reconocer y monitorear amenazas, prevenir o investigar delitos captados en video.

Al tipo de datos biométricos captados en cámaras de videovigilancia se les reconoce como soft-biométricos, ya que son de gran ayuda para definir la identidad de las personas captadas en video, a pesar de no contarse con una definición completa y minuciosa del rostro y físico del sujeto. Dentro de estas características que nos permiten identificar los datos soft-biométricos están el color de piel, de cabello, la ropa, la altura, la forma de andar, cicatrices, tatuajes, etcétera.

Como puede notarse, los sistemas de control e hipervigilancia como mecanismos victimizantes trascienden a lo revisado en 'bancos de datos biométricos' en el apartado de dinámicas empresa-persona. Si bien, los sistemas de control emplean como método de apoyo la recolección de datos biométricos, la dinámica de hipervigilancia exige que estos datos sean más extensivos en cuanto a cantidad y cualidad, además hace uso de tecnologías de inteligencia artificial dirigidas al reconocimiento inteligente y la predicción de comportamientos.

Un tema particular de estos sistemas es el reconocimiento facial, mismo que es utilizado como una poderosa herramienta de control, vigilancia, acceso, etc. (ver tabla (X). Este tipo de sistemas se encuentra conformados, de manera básica, por: el usuario a identificar (persona), el dispositivo de adquisición digital de imágenes (cámara), el dispositivo de almacenamiento (computadora), y por último la base de datos para el almacenamiento de la información.

Tabla 4. Aplicaciones con reconocimiento facial

ÁREA	APLICACIONES ESPECÍFICAS
BIOMETRÍA	Licencias de conducir, programas de derecho, inmigraciòn, pasaportes, registro de votantes, fraude, teléfonos inteligentes, acceso a instalaciones restringidas
SEGURIDAD DE LA INFORMACIÓN	Inicio de sesión, seguridad en aplicaciones, seguridad en bases de datos, cifrado de informaciòn, seguridad en internet, acceso a internet, registros médicos, terminales de comercio seguro, cajeros automáticos
CUMPLIMIENTO DE LA LEY Y VIGILANCIA	Video vigilancia avanzada, control portal, análisis pos-evento, hurto, seguimiento de sospechosos, investigación.
TARJETAS INTELIGENTES	Valor almacenado, autenticación de usuarios.
CONTROL DE ACCESO	Acceso a instalaciones, acceso a vehículos.

Fuente: Elaboración propia con información de Castro, 2016.

Sin embargo, los sistemas de reconocimiento facial en particular, y los sistemas de hipervigilancia en general, se potencializan a través de paquetes algorítmicos e inteligencia artificial (IA). Sin embargo, presentan también importantes críticas que pueden transformarse en pautas de victimización constante y sistemática:

- Inexactitud: puede conducir a la identificación errónea de personas inocentes, lo que tendría consecuencias graves como acoso policial, detenciones injustas, criminalización, revictimización, etc. Por ejemplo, las tecnologías de reconocimiento facial presentan tasas de error que oscilan entre el 92.3% y el 95.4% al momento de identificar a alguien (R3D, 2022).
- Sesgos.
- Levantamiento de datos sin conocimiento de los sujetos observados.
- Discursos de seguridad sustentados en la vigilancia masiva, constante y multifocal.

En el contexto mexicano, esto se ve plasmado en el caso del Fan ID. Este sistema de reconocimiento facial es impulsado por la Federación Mexicana de Futbol. la liga Mx y los equipos Santos y Atlas, como respuesta a los actos de violencia ocurridos, el 5 de marzo de 2022, en el Estadio Corregidora de Querétaro donde supuestas barras de aficionados se enfrentaron dejando personas lesionadas.

Dicha estratégia responde a un registro de datos de personas que asistirán a los partidos de fútbol, así como la instalación de cámaras provistas con tecnología de reconocimiento facial en los estadios. Esto resulta un problema debido a la exposición de datos biométricos y personales de miles de personas que asisten a un partido de fútbol. Las razones son: La creación de una base de datos masiva y centralizada de datos personales; No se respeta el principio de consentimiento libre, ya que no hay alternativa; Incrementa la vulnerabilidad de la afición frente a delitos como la extorsión, el fraude y el secuestro.

Además de las consecuencias desplegadas del levantamiento de estos datos, la potencial vulneración de los mismos, la inexactitud y sesgos cometidos por dicha tecnología, la hipervigilancia resulta potencialmente victimizante debido al impacto que estas pueden tener en la autonomía y la psique de los sujetos y colectivos sociales.

7.3.2 Espionaje informático

Aunque el espionaje informático se encuentra íntimamente relacionado con el apartado anterior (sistemas de control e hipervigilancia), merece un lugar aparte ya que los anteriores se realizan casi siempre bajo dinámicas de masividad, donde no hay blancos específicos sino que se pretende vigilar y controlar a todos. En cambio, el espionaje informático está usualmente dirigido a sujetos particulares.

Ahora bien, María Gabriela Acosta (2020), menciona que se entiende por espionaje informático la adquisición y transferencia de información cibernética, de carácter confidencial, comercial y sin autorización del propietario de la información, con el fin de causar pérdidas económicas o de obtener algún beneficio propio.

En el contexto estatal este espionaje suele ejecutarse a través de de las mismas técnicas de hipervigilancia colectiva por una parte, y del uso de malware y spyware por la otra. Esto implica una alta intrusión a la vida privada de los sujetos y una amenaza importante para derechos como la libertad de expresión.

Uno de los casos mejor documentados es el uso del spyware Pegasus, de acuerdo con la organización Forbidden en colaboración con el Laboratorio de Seguridad de Amnistía Internacional (2022), este es un producto de la firma NSO Group que tiene altas capacidades como software espía ya que se puede instalar de manera remota en un teléfono inteligente sin requerir ninguna acción por parte de su propietario. Además, una vez instalado, permite a los clientes tomar el control del dispositivo, encender cámara y micrófono e incluso acceder a las aplicaciones de mensajería encriptada como WhatsApp y Signal.

Además se han detectado al menos 180 objetivos en países como México, India, Marruecos, Francia y Hungría entre los que destacan defensores de derechos humanos, académicos, líderes sindicales, periodistas, políticos y algunos jefes de estado. Para el caso Mexicano, The Citizen Lab de la Universidad de Toronto junto con R3D, SocialTic y Artículo 19 publicaron en 2017 ocho informes sobre la focalización de Pegasus en el país que resultó en el escrutinio de las prácticas de vigilancia de las autoridades mexicanas. Posteriormente, R3D y Citizen Lab detectaron que periodistas y un defensor de derechos humanos habían sido infectados con el spyware entre 2019 y 2021 e identificaron los siguientes hallazgos:

- Se validaron las infecciones de Pegasus 2019-2021 mediante análisis forense de artefactos recopilados de dispositivos.
- Las infecciones de 2019-2021 aprovecharon los ataques de clic cero: no se requirió engaño para engañar a las víctimas para que hicieran clic. Los informes anteriores de Citizen Lab sobre casos mexicanos encontraron mensajes de texto maliciosos diseñados para engañar a los objetivos para que hicieran clic en un enlace que desencadenaría una infección.
- El defensor de derechos humanos Raymundo Ramos fue hackeado con Pegasus al menos tres veces entre agosto y septiembre de 2020.
- El periodista y autor Ricardo Raphael fue pirateado con Pegasus al menos tres veces en octubre y diciembre de 2019, y nuevamente en diciembre de 2020. Anteriormente también fue atacado e infectado en 2016 y atacado en 2017 (Scott-Railton et. al, 2022).

Si bien, la validación técnica de los artefactos forenses recopilados de los dispositivos de las víctimas confirma que fueron pirateadas por el software Pegasus,

estos datos técnicos no permiten atribuir la piratería a un cliente específico de NSO Group. Sin embargo, las víctimas representan gran interés para las dependencias del gobierno mexicano y en algunos casos para los cárteles de la droga en México (Scott-Railton et. al, 2022). Además, en la propia página web de esta firma se describe que los servicios prestados están dirigidos a agencias gubernamentales.

Esto representa no solo un riesgo para la privacidad y las garantías de protección de datos personales, sino que representa una amenaza y vulneración de otros derechos humanos y libertades fundamentales, tal es el caso de la libertad de expresión, el libre acceso a la información, etc. Por otra parte, este tipo de espionaje estatal genera un clima social de miedo, autocensura, incertidumbre jurídica,

7.3.3 Votaciones digitales

De acuerdo con Julio Téllez Valdez (2010) el creciente desarrollo y avance de las tecnologías, han permitido el desarrollo de nuevas formas de votación, entre las cuales se erigen la votación electrónica y la votación digital. Si bien, este procedimiento en sí mismo no es constitutivo de victimización, si representa campos importantes de oportunidad para vulnerar los derechos de las personas, así como un riesgo para la democracia.

Hasta ahora, en México, este ejercicio consiste en expresar el sufragio a través del Sistema para el Voto Electrónico por Internet para las y los mexicanos que residen en el extranjero, sistema que afirma garantizar la confidencialidad del voto durante su emisión, transmisión y almacenamiento. De acuerdo con el artículo 329 de la Ley General de Instituciones y Procedimientos Electorales (LGIPE), los ciudadanos que residan en el extranjero podrán ejercer su derecho al voto.

Además, en el Libro Sexto del Voto de los Mexicanos Residentes en el Extranjero, en el Capítulo Único, artículo 329, manifiesta que:

> *1. Los ciudadanos que residan en el extranjero podrán ejercer su derecho al voto para la elección de Presidente de los Estados Unidos Mexicanos y senadores, así como de Gobernadores de las entidades federativas y del Jefe*

de Gobierno del Distrito Federal, siempre que así lo determinen las Constituciones de los Estados o el Estatuto de Gobierno del Distrito Federal.

2. El ejercicio del voto de los mexicanos residentes en el extranjero podrá realizarse por correo, mediante entrega de la boleta en forma personal en los módulos que se instalen en las embajadas o consulados o, en su caso, por vía electrónica, de conformidad con esta Ley y en los términos que determine el Instituto.

3. El voto por vía electrónica sólo podrá realizarse conforme a los lineamientos que emita el Instituto en términos de esta Ley, mismos que deberán asegurar total certidumbre y seguridad comprobada a los mexicanos residentes en el extranjero, para el efectivo ejercicio de su derecho de votar en las elecciones populares.

El voto electrónico tiene variedad de ventajas como lo son la eficacia y rapidez para su conteo, una mayor precisión en los resultados, posibilidad de aumento de la participación de votantes, voto para los que residen en el extranjero, entre otras. La primera implementación del voto se llevó a cabo en las elecciones de 2021 en entidades como Baja California Sur, Chihuahua, Ciudad de México, Colima, Guerrero, Jalisco, Michoacán, Nayarit, Querétaro, San Luis Potosí y Zacatecas.

Sin embargo, se debe tomar en cuenta las desventajas del uso del voto electrónico como la desconfianza en las autoridades administrativas electorales, la autenticidad de un procedimiento transparente, la posibilidad de violar la privacidad y el voto secreto. Derivado de estas incertidumbres es que se tiene que aumentar la confianza en las autoridades administrativas, evitar fraudes electorales por el uso de datos biométricos como huellas dactilares, el reconocimiento facial, el reconocimiento de voz, la firma electrónica, la comprobación del iris, la clave de seguridad, etc.

De acuerdo con Chorny, el problema del voto por internet es amplio ya que *“si una lección es manipulada, es muy difícil o incluso imposible saberlo (...) porque la tecnología y la naturaleza de los software que se usan para votar permite manipular una elección (en el caso de se hackeada) sin dejar rastros; los fraudes electorales en internet pueden ser invisibles”* (2020, p.6).

Así es que el voto por internet, además de tener todos los riesgos de las elecciones tradiciones, advierte riesgos más específicos:

- El voto o la información de los votantes pueden ser robados o manipulados.
- Se corre el riesgo de que el espacio desde el cuál se vota no sea privado y esto facilite la coerción.
- Los dispositivos empleados para registrar, transmitir y almacenar la información relacionada con el procedimiento puede ser objeto de hackeo a través de software malicioso.
- El sentido del voto puede ser cambiado sin que el votante se de cuenta.
- Una sola persona puede manipular la elección completa.
- Las elecciones pueden ser secuestradas por agentes internos o externos con fines políticos o económicos.
- Es imposible asegurar la secrecía del voto ya que este va acompañado de microdatos de conexión, ubicación e identificación.

Ante estos riesgos, países como Alemania, Estonia y Estados Unidos de América han decidido abandonar los intentos de implementar este tipo de esquemas. Incluso, agencias de seguridad tales como el FBI, *"advirtieron a los Estados que votar por internet era altamente peligroso y debían abstenerse de hacerlo"* (2020, p.8).

Como bien se mencionó, las dinámicas de voto por internet pueden resultar victimizantes, además de tener la particularidad de generar víctimas colectivas y causar grave daño a las estructuras políticas de los estados nación.

7.3.4 Características generales de las formas de victimización desde el estado.

- Desamparo legal e insuficiencia de marcos legales para la protección de las víctimas.
- Revictimización por parte de las autoridades e instituciones.
- Baja probabilidad de castigo y alta tasa de impunidad.
- Falta de controles legales, sociales, medidas de seguridad, marco jurídico y sistema de justicia..
- Sistemas que ponen en riesgo la seguridad de datos biométricos.

- Deshumanización en los procesos.
- Fracaso de expectativas frente a la realidad del trato institucional.
- Victimario difícilmente identificable.
- Mezcla de conductas dirigidas y no dirigidas.
- Amenazas contra la democracia.

VIII. CONCLUSIONES

La sociedad de información implica no solo desarrollo tecnológico e hiperproducción de datos sino también cambios en las estructuras sociales, caracterizados por la transparencia y la comunicación constante. Esto genera oportunidades en donde el flujo de información juega un papel muy importante ya que a través de este se crea una conexión globalizada donde miles de usuarios pueden estar en contacto al mismo tiempo, sin embargo ello puede desencadenar actividades ilícitas, nocivas o dañinas que afectan a otras personas dejando un nuevo tipo de víctimas.

Como primera conclusión del presente trabajo, destaca la necesidad de contar con una conceptualización más amplia de la víctima. Tal como se mencionó, la víctima no se reduce a aquella que ha experimentado las consecuencias del delito o la vulneración de los derechos humanos, se trata también de personas y sectores que de manera silenciosa viven los aspectos negativos de la construcción sistemática del sistema mundo capitalista.

Dicha redefinición de la víctima debe incorporar a los sujetos que resultan invisibles para el poder político y económico, así como aquellos que experimentan consecuencias negativas a causa de elementos, tales como la tecnología, que generan consecuencias negativas, sin que esto represente necesariamente la comisión de un delito o la vulneración de un derecho humano reconocido.

Además, como segunda conclusión, y después de haber descrito y analizado las distintas dinámicas de victimización de la sociedad digital, se propone una primera clasificación de estas:

1. Persona - persona: formas de victimización que van de usuario a usuario, sea este individual o colectivo. Es decir, violencia ejercida entre personas o grupos de personas (colectivos, grupos sociales, comunidades). Estas formas de victimización son quizá las más evidentes y directas, son también aquellas cuyas consecuencias tienden a ser más perceptibles, favoreciendo la identificación de la víctima como tal.

2. Empresa - persona: estas dinámicas de victimización incorporan a agentes privados, tal es el caso de empresas proveedoras de servicios, fabricantes de tecnología, proveedores de internet, motores de búsqueda, organizaciones criminales, etc. De acuerdo con las características del victimario, pueden detectarse a su vez, tres subtipos:
    A. Organizaciones criminales ejecutan actos victimizantes contra individuos y empresas.
    B. Empresas ejecutan actos victimizantes contra individuos y otras empresas.
    C. Individuos ejecutan actos victimizantes contra empresas.
3. Estado - persona: formas de victimización caracterizadas por la implicación de los órganos del estado como victimarios.

Esta división se construye en razón de las relaciones que guardan las víctimas y victimarios e intenta incorporar como víctimas a todos aquellos individuos que experimentan alguna consecuencia negativa de la masificación de datos e hipercomunicación propios de la sociedad de la información.

Como tercera conclusión, se presentan en la siguiente tabla las características comunes de las dinámicas de victimización, mismas que las agrupan como categoría y distinguen a cada tipo de los otros.

Tabla 5. Características generales por tipología.

Tipología	Características
Persona - persona	● Se desarrollan entre pares o iguales, ya sea individuos o grupos. ● La víctima y el victimario se encuentran claramente diferenciados. ● Son conductas ilícitas convencionales pero los mecanismos de ejecución tienden a ser más sofisticados y hacer uso de las tecnologías de información y

	comunicación, así como de las plataformas e infraestructura digital. ● Los victimarios pueden ser agentes conocidos o desconocidos. ● Los victimarios aprovechan el aparente anonimato, y facilidad para ocultar la identidad, que brindan las plataformas digitales. ● La brecha digital facilita su proliferación. ● Las conductas son casi siempre dirigidas hacia usuarios específicos. ● Empleo recurrente de ingeniería social como una de las principales herramientas para la obtención de información personal. ● Masificación de potenciales víctimas. ● Generan daños a la intimidad, integridad física, moral y psicológica.
Empresa - persona	● Sustentadas en la obtención de datos personales de usuarios y comercio ilegal de información. ● Exposición de información personal, laboral, académica, y financiera. ● Creación de perfiles individuales y colectivos con potencial de predicción conductual. ● Manipulación digital-emocional con motivaciones comerciales y políticas. ● Estrategias de bajo costo. ● Ubicuidad y fácil ejecución. ● Alta efectividad e impacto sobre grandes masas de población. ● Reducido riesgo para el atacante. ● Victimario difícilmente identificable.

	● Las víctimas no siempre son conscientes de los eventos victimizantes y no siempre se asimilan a sí mismas como tal. ● Riesgos globales: tanto percibidos como reales. ● Riesgo para la democracia, el acceso a la información y la libertad de expresión. ● Conductas no siempre dirigidas a individuos particulares sino destinadas a afectar grandes masas, casi siempre de manera fortuita. ● No siempre son reconocidos como delitos, abuso de poder o hechos victimizantes. Sin embargo, al tener potencial de daño y de restringir el desarrollo pleno del sujeto lo son.
Estado - persona	● Desamparo legal e insuficiencia de marcos legales para la protección de las víctimas. ● Revictimización por parte de las autoridades e instituciones. ● Baja probabilidad de castigo y alta tasa de impunidad. ● Falta de controles legales, sociales, medidas de seguridad, marco jurídico y sistema de justicia.. ● Sistemas que ponen en riesgo la seguridad de datos biométricos. ● Deshumanización en los procesos. ● Fracaso de expectativas frente a la realidad del trato institucional. ● Victimario difícilmente identificable. ● Mezcla de conductas dirigidas y no dirigidas. ● Amenazas contra la democracia.

Fuente: Elaboración propia.

Por último, la inexistencia de una política pública victimológica que atienda a las víctimas que surgen de los medios digitales, propicia el aumento de las nuevas formas de victimización provocando una evolución en cada una y a su vez reduciendo la importancia que se les debe dar. Es por ello que la creación e implementación de una política pública victimológica específica para víctimas de medios digitales podría generar un impacto positivo en la sociedad de la información, así como la disminución de la cibervictimización.

En este sentido, se proponen pautas de diseño de políticas públicas en materia victimológica que se puedan tomar en consideración en un futuro, para la creación de esta política que englobe los temas de gran relevancia como los mencionados en el presente trabajo, para su intervención, disminución y prevención, así como la atención a las víctimas que surgen a través de los medios digitales y las nuevas tecnologías. En este sentido, las pautas propuestas se presentan a continuación:

- Realizar estudios profundos sobre cada una de las dinámicas expuestas en el presente trabajo, con la intención de identificar factores de riesgo específicos para cada categoría.
- Concentrarse en la brecha digital, sobre todo aquella relacionada con el conocimiento y uso adecuado de la tecnología con la finalidad de comenzar generar herramientas de protección para las potenciales víctimas.
- Fomentar la profesionalización de la comunidad victimológica en materia de tecnologías y las dinámicas de victimización relacionadas con la sociedad de la información.
- Fomentar la profesionalización y sensibilización de autoridades e instituciones gubernamentales que tienen contacto directo e indirecto con víctimas digitales.
- Fomentar la gobernanza en internet, incorporando como actores clave a organismos gubernamentales, usuarios, empresas y organizaciones de la sociedad civil.
- Actualización de marcos normativos que respondan a las necesidades de la sociedad digital e incorporen el uso correcto de conceptos.
- Reforzar la regulación de derechos ARCO (acceso, rectificación, cancelación y oposición) de los datos personales.

- Prevención de la victimización desde el diseño, es decir desde el diseño e implementación de procesos las empresas y organismos deben asegurar que en sentido amplio no se generarán dinámicas de victimización.
- Contribución intencional en materia de diseño y operación de leyes y políticas públicas. Esto considerando que la victimización digital no atiende a lógicas convencionales de tiempo y territorio.
- Desarrollo de medidas de protección física, tecnológica y administrativa a nivel individual y colectivo.
- Generación de mecanismos y procesos que permitan a la población tener conocimiento de cuándo han sido víctimas.
- Procesos claros que permitan a los usuarios conocer y reclamar sus derechos digitales.
- Incorporar el perfil del victimologo en el diseño de programas específicos con la intención de dirigir los esfuerzos en la protección de las víctimas y no de intereses políticos y económicos.

IX. REFERENCIAS

Acosta, María Gabriela. (2020). *Delitos informáticos: Impunidad organizacional y su complejidad en el mundo de los negocios.* Universidad del Zulia; Venezuela. Consulado en https://www.redalyc.org/journal/290/29062641023/29062641023.pdf, el 08 de Septiembre de 2021 a las 15:00 hrs.

Agudo, A. & Monge, Y. (2012). *Humillada en la Red, humillada en la calle*. Publicado en el sitio del período El País. Consultada en https://elpais.com/sociedad/2012/10/18/actualidad/1350587479_648426.html, el 16 de febrero de 2022 a las 14:00 hrs.

Alanis, G. (2019). Evaluemos el riesgo en el uso de criptomonedas. EGADE Business School, Tecnológico de Monterrey.

Amaro L, José Antonio & Rodriguez R., Citlalli R. (2016). *Seguridad en internet.* Universidad de Guadalajara; México. Consultado en https://www.redalyc.org/pdf/4990/499054323006.pdf, el 01 de Septiembre de 2021 a las 16:30 hrs.

Amescua, C, Cristina. (2010). *El secuestro virtual en el continuum de la violencia Visibilizar lo que se oscurece.* Trace. Centro de Estudios Mexicanos y Centroamericanos Distrito Federal; México. Consultado en https://www.redalyc.org/pdf/4238/423839515008.pdf, el 06 de Agosto de 2021 a las 13:00 hrs.

Andrada, A. M (2021). *El reto de la privacidad digital.* Universidad Americana de Europa. Consultado en https://unade.edu.mx/privacidad-digital/, el 28 de octubre de 2021 a las 16:39 hrs.

Ant, Adeane (2019). *La verdadera historia del reto suicida de la "Ballena Azul" que se hizo viral en internet*. Portal del periodico BBC. Mundo. Consultado en

https://www.bbc.com/mundo/noticias-46974250, el 5 de marzo de 2022 a las 12:11 hrs.

Ardevol, E; Bertrán M.; Callen M., & Pérez C. (2003). *Etnografía virtualizada; la observación participante y la entrevista semiestructurada en línea.* Universidad Oberta de Catalunya. Consultada en https://ddd.uab.cat/pub/athdig/15788946n3/15788946n3a5.pdf, el 02 de marzo de 2021 a las 19:45 hrs.

Arguello Fuentes, Henry. (2011). *Sistemas de reconocimiento basados en la imagen facial.* Universidad Nacional de Colombia; Colombia. Consultado en https://www.redalyc.org/pdf/1331/133122679021.pdf, el 20 de octubre de 2021 a las 18:13 hrs.

Arredondo Rubio, Celina. (2020). *La red social Facebook como dispositivo de control. Una mirada desde la filosofía de Foucault.* Universidad de Guadalajara; México. Consultado en https://www.redalyc.org/journal/5138/513862147008/513862147008.pdf, el 06 de noviembre de 2021 a las 11:00 hrs.

Arturi G. (2022) *Usuarios de las redes sociales perdieron 'al menos' 770 mdd por estafas en 2021*. Recuperado del sitio de Forbes. Consultado en https://www.forbes.com.mx/mundo-usuarios-de-las-redes-sociales-perdieron-al-menos-770-mdd-por-estafas-en-2021/, el 5 de marzo de 2022 a las 17:22 hrs.

Asociación Mexicana de Internet A.C (AMIPCI). (2016). *Estudio sobre el valor económico de los datos personales*; México. Consultado en https://clustertic.org/wpcontent/uploads/2016/06/valor_eco_Datospersonales_FINAL.pdf, el 8 de junio de 2021 a las 20:00 hrs.

AYUDALEY. (2021). *Principales ejemplos de fake news*. Consultado en https://ayudaleyprotecciondatos.es/2021/06/24/ejemplos-fake-news/, el 5 de marzo de 2022 a las 17:24 hrs.

BBC. Mundo (2018). *5 claves para entender el escándalo de Cambridge Analytica que hizo que Facebook perdiera US$37.000 millones en un día*. Portal del periodico BBC. Mundo. Consultado en https://www.bbc.com/mundo/noticias-43472797, el 8 de enero de 2022 a las 19:45 hrs.

BBC Mundo.(2017). *Qué consecuencias tendrá el fin de la neutralidad de internet en Estados Unidos (y cómo afectará al resto del mundo*). Portal del periodico BBC Mundo. Consultado en https://www.bbc.com/mundo/noticias-internacional-42315967, el 20 de junio de 2022, a las 21:36 hrs.

Bedecarratz, F. (2018). *Riesgos delictivos de las monedas virtuales: Nuevos desafíos para el derecho penal.* Universidad Autónoma de Chile; Chile. Consultado en https://www.scielo.cl/scielo.php?script=sci_arttext&pid=S0719-25842018000100079, el 8 de junio de 2021 a las 18:39 hrs.

Bujan, Javier A.; Carri P.; Trerotola D. (s.f.). *Si discrimina #NoDaCompartir.* Instituto Nacional contra la Discriminación, la Xenofobia y el Racismo INADI, UNICEF. Consultado en https://www.unicef.org/argentina/media/1581/file/Si%20discrimina%20no%20da%20compartir.pdf, el 28 de Agosto de 2021 a las 20:49 hrs.

Calderón G, J. (2015). *La Evolución de la "Reparación Integral" en la Jurisprudencia en la Corte Interamericana de los Derechos Humanos;* México. Consultado en http://appweb.cndh.org.mx/biblioteca/archivos/pdfs/fas_CSIDH_EvolucionReparacionIntegral-1aReimpr.pdf, el 29 de Mayo de 2021 a las 23:45 hrs.

Canes F, Dulce María. (2011). *Acerca de los virus informáticos: una amenaza persistente.* Centro Provincial de Información de Ciencias Médicas de Camagüey; Cuba. Consultado en https://www.redalyc.org/pdf/3684/368445227018.pdf, el 28 de Septiembre de 2021 a las 22:00 hrs.

Carrión J. (s.f.). *Diferencia entre dato, información y conocimiento.* Consultado en http://iibi.unam.mx/voutssasmt/documentos/dato%20informacion%20conocimiento.pdf, el 19 de Mayo de 2021 a las 10:23 hrs.

Castillo-Pulido L. E. (2011). *El acoso escolar. De las causas, origen y manifestaciones a la pregunta por el sentido que le otorgan los actores.* Pontificia Universidad Javeriana; Colombia. Consultado en https://www.redalyc.org/pdf/2810/281021722009.pdf, el 30 de junio de 2021 a las 15:37 hrs.

Castillo R., Victor; Hermosilla U., P; Poblete T., J.P; Durán A., C. (2021). *Noticias falsas y creencias infundadas en la era de la posverdad.* Universidad Politécnica Salesiana. Consultado en https://www.redalyc.org/journal/4761/476165932004/html/, el 12 de octubre de 2021 a las 19:49 hrs.

Castro Arias, R. Daniel.(2016). *"Sistema de control de acceso al personal de la lavadora de jeans fashion mediante reconocimiento facial".* Universidad Técnica de Ambato; Ecuador. Consultado en https://repositorio.uta.edu.ec/bitstream/123456789/20347/1/Tesis_t1107ec.pdf, el 24 de octubre de 2021 a las 21:56 hrs.

Cejudo G., Michel C. (2016). *Coherencia y políticas públicas: Metas, instrumentos y poblaciones objetivo*. Centro de Investigación y Docencia Económicas, A.C. Distrito Federal; México. Consultado en https://www.redalyc.org/pdf/133/13343543001.pdf, el 8 de junio de 2022 a las 14:32 hrs.

Congreso de la Ciudad de México. Código Penal para el Distrito Federal (última reforma 2020). Consultado en https://www.congresocdmx.gob.mx/media/documentos/9cd0cdef5d5adba1c8e25b34751cccfdcca80e2c.pdf, el 07 de Julio de 2021 a las 12:34 hrs.

Código Penal Federal. (s.f). *Código Penal Federal*. Cámara de diputados del H. Congreso de la Unión. Consultado en

http://www.diputados.gob.mx/LeyesBiblio/pdf_mov/Codigo_Penal_Federal.pdf , el 05 de Julio de 2021 a las 11:58 hrs.

Código Penal Federal.(s.f.). *Artículo 282.* Conceptos jurídicos. Consultado en https://www.conceptosjuridicos.com/mx/codigo-penal-articulo-282/, el (09 de Agosto de 2021 a las 17:45 hrs.

Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros, CONDUSEF (s.f). Consultado en https://www.gob.mx/condusef/que-hacemos , el 14 de mayo de 2022 a las 7:00 hrs.

Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros (s.f.). Alerta CONDUSEF sobre el uso del BITCOIN como medio de pago. Consultado en https://www.condusef.gob.mx/?p=contenido&idc=833&idcat=1 el 16 de junio de 2022 a las 13:23 hrs.

Comisión Nacional de Seguros y Finanzas (2019) Riesgo Cibernético y Ciberseguridad. Secretaria de Hacienda y Credito Público. México. Consultado en https://www.gob.mx/cms/uploads/attachment/file/478193/181.-_Riesgo_Cibern_tico_y_Ciberseguridad_2019.pdf , el 20 de mayo de 2022 a las 13:00 hrs.

Concepto (2013) *Privacidad digital*. Enciclopedia Concepto, Editorial Etecé. Consultado en https://concepto.de/privacidad-digital/, el 14 de mayo de 2022 a las 9:45 hrs.

CONDUCEF, 2022. Alerta CONDUSEF sobre el uso del BITCOIN como medio de pago. Consultado en https://www.condusef.gob.mx/?p=contenido&idc=833&idcat=1#:~:text=Por%20ello%2C%20CONDUSEF%20alerta%20que,volatilidad%20y%20posibles%20p%C3%A9rdidas%20monetarias el 22 de noviembre de 2022.

Correa Medina, Juan Gabriel; Carlos Pérez, Héctor de Jesús; Velarde Martínez, Apolinar (2006). *Virus informáticos.* Instituto Tecnológico de Aguascalientes; México.

Consultado en https://www.redalyc.org/pdf/944/94403112.pdf, el 25 de Septiembre de 2021 a las 15:00 hrs.

Cortés O, Jimy Alexander; Medina A., Francisco Alejandro; Muriel E., José A (2010). *Sistemas de seguridad basados en Biometría.* Universidad Tecnológica de Pereira; Colombia. Consultado en https://www.redalyc.org/pdf/849/84920977016.pdf, el 15 de octubre de 2021 a las 15:44 hrs.

Cortez O, Alexandra & Tulcanaza P. Ana B (2018). *Bitcoin: su influencia en el mundo global y su relación con el mercado de valores.* Universidad Politécnica de Cataluña, España. Consultado en https://www.redalyc.org/journal/5717/571763394004/, el 18 de octubre de 2021 a las 21:00 hrs.

Crovi D, Delia.(2002) *Sociedad de la información y el conocimiento. Entre el optimismo y la desesperanza.*Universidad Nacional Autónoma de México; México. Consultado en https://www.redalyc.org/pdf/421/42118502.pdf, el 15 de enero de 2021 a las 16:02 hrs.

Delgadillo G, A. (2017) *Televisión y narcocultura. Cuando los narcos se ponen de moda.* Universidad de Colima; México. Consultado en http://ww.ucol.mx/interpretextos/pdfs/964_inpret1710.pdf, el 01 de junio de 2021 a las 13:20 hrs.

Díaz, V.. (2013). Sistemas biométricos en materia criminal: un estudio comparado. *Revista IUS*, *7*(31), 28-47. Recuperado en 13 de diciembre de 2022, de http://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S1870-21472013000100003&lng=es&tlng=es.

Dueñas David; Pontón, Paloma; Belzunegui, Ángel; Pastor, Inma (2016). *Expresiones discriminatorias, jóvenes y redes sociales: la influencia del género.* Grupo Comunicar; España. Consultado en https://www.redalyc.org/pdf/158/15847441007.pdf, el 15 de agosto de 2021 a las 23:00 hrs.

Estrada-Cuzcano, Alonso; Alfaro-Mendives, Karen; Saavedra-Vásquez, Valeria (2020). *Desinformación y Misinformación, Posverdad y Fake News.* Universidad de Buenos Aires; Argentina. Consultado en https://www.redalyc.org/journal/2630/263062301010/263062301010.pdf, el 15 de octubre de 2021 a las 12:15 hrs.

Estudillo García, J (2001). *Surgimiento de la sociedad de la información.* Universidad Nacional Autónoma de México; México. Consultado en https://www.redalyc.org/pdf/285/28540203.pdf, el 13 de Noviembre de 2020 a las 16: 40 hrs.

Expansión política. (2021). *La youtuber 'YosStop' es detenida en la CDMX por pornografía infantil.* Portal del periodico Expansión Política. Consultado en https://politica.expansion.mx/mexico/2021/06/30/yosstop-detenida-por-pornografia-infantil-denuncia-youtuber, el 07 de Julio de 2021 a las 21:00 hrs.

EXPANSIÓN. (2011). *Un joven mexicano que secuestraba usando las redes sociales es detenido*. Portal del periodico Expansión. Consultado en https://expansion.mx/nacional/2011/01/15/un-joven-que-secuestraba-haciendo-uso-de-redes-sociales-es-capturado, el 5 de marzo de 2022 a las 22:10 hrs.

Forbes (2021) Seis ciberataques que marcaron el 2021. Portal del periodico Forbes. Consultado en https://forbescentroamerica.com/2021/12/15/seis-ciberataques-que-marcaron-el-2021/, el 3 de abril de 2022 a las 00:00 hrs.

Gabaldón, Luis Gerardo. (2006). *Fraude electrónico y cultura corporativa.* Universidade Federal da Bahia; Brasil. Consultado en https://www.redalyc.org/pdf/3476/347632169004.pdf, el 10 de Septiembre de 2021 a las 21:13 hrs.

Gabriel R., Ana (2019). *Ciberacoso: "Pasé de ser la 'gordibuena' del video sexual que criticaba todo el pueblo a que 11 estados de México aprobaran una ley con mi*

nombre". Portal del periodico BBC.Mundo. Consultado en https://www.google.com/amp/s/www.bbc.com/mundo/noticias-america-latina-49763560.amp, el 2 de marzo de 2022 a las 13:28 hrs.

Gamboa M, Claudia & Valdés R. Sandra. (2008). *Delito de secuestro: (Primera Parte). Estudio Teórico Conceptual, Antecedentes Legislativos, Referencia de las Iniciativas presentadas en esta LX Legislatura.* Centro de Documentación, Información y Análisis; México. Consultado en http://www.diputados.gob.mx/sedia/sia/spi/SPI-ISS-27-08.pdf, el 08 de Agosto de 2021 a las 22:22 hrs.

Garmendia, M. Jiménez, E., Casado, M.A. & Mascheroni, G. (2016). Net Children Go Mobile: *Riesgos y oportunidades en internet y el uso de dispositivos móviles entre menores españoles (2010-2015).* Universidad del País Vasco; Madrid. Consultado en https://netchildrengomobile.eu/ncgm/wp-content/uploads/2013/07/Net-Children-Go-Mobile-Spain.pdf, el 17 de abril de 2021 a las 19:20 hrs.

García N, Isabel. (2014). *Pornografía infantil en internet: principales aspectos de la transposición de la directiva.* Universitat Oberta de Catalunya; España. Consultado en https://www.redalyc.org/pdf/788/78835370009.pdf, el 06 de julio de 2021 a las 17:35 hrs.

Gímenez, G. (2010). Cultura, identidad y procesos de individualización. Universidad Nacional Autónoma de México, México.

Ginner A, César. (s.f). *Aproximación psicológica de la victimología.* Consultado en http://repositorio.ucam.edu/bitstream/handle/10952/573/Aproximaci%C3%B3n%20psicol%C3%B3gica%20%20a%20la%20victimolog%C3%ADa.%20C%C3%A9sar%20Augusto%20G%C3%ADner%20Alegr%C3%ADa%20.pdf?sequence=1, el 02 de diciembre de 2020 a las 11:37 hrs.

Grupo BIT. (2018). *¿Cuántos datos se producen en un minuto?.* Portal de Grupo BIT. Business analytics. Consultado en

https://business-intelligence.grupobit.net/blog/cuantos-datos-se-producen-en-un-minuto, el 19 de Mayo de 2021 a las 16:11 hrs.

Guardiola, Elia. (). *Marketing emocional, ¿Qué es el marketing emocional?*. Acumbamail. Consultado en https://acumbamail.com/glosario/marketing-emocional/, el 24 de octubre de 2021 a las 21:39 hrs.

Gutierrez de Piñeres Botero, Carolina; Coronel, Elisa y Perez Calos Andres (2009) *Revisión teórica del concepto de victimización secundaria*.Universidad Cooperativa de Colombia; Colombia. Consultado en http://www.scielo.org.pe/scielo.php?script=sci_arttext&pid=S1729-48272009000100006, el 28 de Noviembre de 2021 a las 22:49 hrs.

Hernández T, Y. (2020). *Una mirada al tema de la Victimología y la Justicia Restaurativa desde un Estado del Arte.* Universidad Cooperativa de Colombia; Colombia. Consultado en https://repository.ucc.edu.co/bitstream/20.500.12494/17524/4/2020_victimologia_justicia.pdf, el 18 de abril de 2021 a las 14:00 hrs.

Homs, Ricardo (2020). *Redes sociales, manipulación y libertad de prensa.* El Universal. Consultado en https://www.eluniversal.com.mx/opinion/ricardo-homs/redes-sociales-manipulacion-y-libertad-de-prensa, el 10 de noviembre de 2021 a las 18:30 hrs.

Informatix Servicios Informáticos (2021) *Los 10 virus más letales de la historia (para los ordenadores)*. INFORMATIX. Consultado en https://informatix.es/10-virus-mas-letales-de-la-historia/, el 5 de marzo de 2022 a las 17:56 hrs.

Innerarity, D. (2022). La sociedad del desconocimiento. Barcelona, Ed. Galaxia Gutenberg.

Instituto Federal de Telecomunicaciones (2020). *En México hay 80.6 millones de usuarios de internet y 86.5 millones de usuarios de teléfonos celulares: ENDUTIH*

2019. Instituto Federal de Telecomunicaciones. Consultado en http://www.ift.org.mx/comunicacion-y-medios/comunicados-ift/es/en-mexico-hay-806-millones-de-usuarios-de-internet-y-865-millones-de-usuarios-de-telefonos-celulares#:~:text=Seg%C3%BAn%20la%20ENDUTIH%202019%2C%20se,puntos%20porcentuales%20respecto%20de%202015, el 03 de junio de 2021a las 09:50 hrs.

Instituto Nacional Electoral (2020) *Concepto de víctima y sus tipos*. Igualdad de Género y no Discriminación, Guía para la Prevención, Atención y Sanción de la Violencia Política Contra las Mujeres por Razón de Género del Instituto Nacional Electoral. Consultado en https://igualdad.ine.mx/wp-content/uploads/2020/07/Guia_Prevencion_Violencia_Politica_Texto_9.pdf, el 18 de enero de 2021 a las 14:00 hrs.

Instituto Nacional Electoral. (s.f). *Voto electrónico por internet.* Instituto Nacional Electoral. Consultado en https://www.votoextranjero.mx/web/vmre/voto-por-internet-2020-2021, el 21 de octubre de 2021 a las 23:58 hrs.

Islas O. (2021). *Internet en 2021.* El Universal. Consultado en https://www.eluniversal.com.mx/opinion/octavio-islas/internet-en-2021, el 12 de abril de 2021 a las 19;45 hrs.

José L. Núñez; Alejandro Millán; Paulino Ruiz de Clavijo; David Guerrero; Enrique Ostúa; Manuel J. Bellido & Jorge Juan (2004) *Seguridad en Internet: Web Spoofing.* Universidad de Sevilla,España; España. Consultado en https://www.researchgate.net/publication/228699085_Seguridad_en_Internet_Web_Spoofing, el 6 de junio de 2021 a las 00:20 hrs.

León Unger, Juan (2015). *Víctimas y revictimización. Reflexiones en torno a la finalidad del proceso penal.* Universidad de Buenos Aires; Argentina. Consultado en https://cdsa.aacademica.org/000-061/1185.pdf, el 28 de octubre de 2021 a las 17:00 hrs.

Ley Federal de Protección de Datos Personales en Posesión de los Particulares (2010) Cámara de Diputados del H. Congreso de la Unión; México. Consultado en http://iibi.unam.mx/archivistica/ley_federal_datos_personales.pdf, el 20 de septiembre de 2021 a las 23:00 hrs.

Ley General de Víctimas. (última reforma 2022). Cámara de Diputados del H. Congreso de la Unión; México. Consultado en https://www.diputados.gob.mx/LeyesBiblio/pdf/LGV.pdf , el 10 de diciembre de 2020 a las 21:00 hrs.

Ley Olimpia (2019). Congreso de la Ciudad de México I Legislatura. Consultado en https://congresocdmx.gob.mx/archivos/parlamentarios/IN_215_10_12_09_2019.pdf, el 30 de Mayo de 2021 a las 19:10 hrs.

López-Rodriguez, Campo E; Lopez-Ordoñez, Diego A; Poveda A., A; Lancheros P, LJ (2020). *Las criptomonedas como medios de transacción financiera: perspectivas en la población de Bogotá, Colombia.* Revista Espacios. https://www.revistaespacios.com/a20v41n34/a20v41n34p02.pdf, el 20 de octubre de 2021 a las 16:40 hrs.

Lucumi J.P. (2022) *Mark Zuckerberg, demandado por la Fiscalía de Washington por el caso 'Cambridge Analytica'* . Portal del sitio France 24. Consultado en https://www.france24.com/es/am%C3%A9ricas/20220523-facebook-mark-zuckerberg-demanda-fiscal%C3%ADa-cambridge-analytica, el 4 de junio de 2022 a las 11:10 hrs.

Mantilla, Saida. (2015). *La revictimización como causal de silencio de la víctima.* Revista de ciencias forenses Honduras. Consultado en http://www.bvs.hn/RCFH/pdf/2015/pdf/RCFH1-2-2015-4.pdf, el 03 de noviembre de 2021 a las 22:23 hrs.

Mata Villalpando- Becerra, Isaac; Guevara-Juárez, Oscar Antonio (2010). *Virus informáticos, todo un caso pero no perdido*. Universidad Autónoma de Tamaulipas;

México. Consultado en https://www.redalyc.org/pdf/4419/441942920010.pdf, el 10 de octubre de 2021 a las 13:07 hrs.

Marketing (2018) *¿Qué es el marketing? la respuesta que deberían saber todas las Pymes.* Puro Marketing. Consultado en https://www.puromarketing.com/44/30910/marketing-respuesta-deberian-saber-contestar-todas-pymes , el 24 de octubre de 2021 a las 17:00 hrs.

Martín Montilla, Ariadna; Pazos Gómez, María; Montilla Coronado, María del Valle Cecilia; Romero Oliva, Cristina (2016). *Una modalidad actual de violencia de género en parejas de jóvenes: las redes sociales.* Universidad Nacional de Educación a Distancia Madrid; España. Consultado en https://www.redalyc.org/pdf/706/70645811017.pdf, el 12 de agosto de 2021 a las 17:57 hrs.

Martinez O. Juan M (2013). *La difusión de sexting sin consentimiento del protagonista: un análisis jurídico.* Nueva Época: Derecom. Dialnet. Consultado en https://dialnet.unirioja.es/servlet/articulo?codigo=4330495, el 17 de julio de 2021 a las 15:03 hrs.

Martínez-Otero P, V. (2017). *Acoso y ciberacoso en una muestra de alumnos de educación secundaria*. Universidad de Granada; España. Consultado en https://www.redalyc.org/pdf/567/56752489014.pdf, el 01 de Julio de 2021 a las 21:45 hrs.

Mejía S, Guillermina (2014). *Sexting: una modalidad cada vez más extendida de violencia sexual entre jóvenes.* Ciudad de México. Consultado en http://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S0187-53372014000400007, el 10 de Julio de 2021 a las 20:18 hrs.

Mendoza M, Luciana A (2014). *La acción civil del daño moral.* Universidad Nacional Autónoma de México; México. Consultado en https://archivos.juridicas.unam.mx/www/bjv/libros/8/3636/10.pdf, el 28 de Mayo de 2021 a las 22:35 hrs.

Meza, A. (2021) *Cuatro preguntas clave sobre el escándalo del espionaje*. Revista Digital. Consultado en https://www.france24.com/es/programas/revista-digital/20210728-pegasus-escandalo-espionaje-internet-software, el 2 de febrero de 2022 a las 07:00 hrs.

Migueles R. (2021) *Víctimas de ciberacoso uno de cada cinco usuarios de internet en México: Inegi*. El Universal. Consultado en https://www.eluniversal.com.mx/cartera/victimas-de-ciberacoso-uno-de-cada-cinco-usuarios-de-internet-en-mexico-inegi, el 8 de febrero de 2022 a las 22:00 hrs.

Miró Llinares, Fernando (s.f). *La cibervíctima: perfiles de victimización y riesgo real de la amenaza del cibercrimen.* Información Jurídica Inteligente. Consultado en *https*://libros-revistas-derecho.vlex.es/vid/cibervictima-perfiles-victimizacion-riesgo-695997205., el 01 de junio de 2021 a las 23:39 hrs.

Mitek Systems, 2021. Ventajas y desventajas de la biometría digital.

Moctezuma O, Daniela Alejandra. (2016). *Re-identificación de personas a través de sus características soft-biométricas en un entorno multi-cámara de video-vigilancia.* Universidad Nacional Autónoma de México; México. Consultado en https://www.redalyc.org/pdf/404/40445803010.pdf, el 21 de octubre de 2021 a las 21:17 hrs.

Norton (2021) *Cómo evitar las estafas en línea*. Norton. Consultado en https://mx.norton.com/internetsecurity-online-scams.html, el 18 de Septiembre de 2021 a las 20:21 hrs.

Observatorio de Violencia de Género en Medios de Comunicación. (s.f). *Violencia mediática.* Consultado en https://ovigem.org/violencia-de-genero-en-los-medios-de-comunicacion/, el 01 de junio de 2021 a las 22:30 hrs.

Olivares P, Susana. (2019). *El uso de internet y conductas suicidas en adolescentes de 14 a 18 años en México*. Visión Criminológica- Criminalística. Consultado en .http://revista.cleu.edu.mx/new/descargas/1804/articulos/Articulo06_uso_de_internet_y-conductas_suicidas_en_adolescentes_de_14_18_mexico.pdf, el 05 de Marzo de 2021 a las 11:46 hrs.

Organización de las Naciones Unidas (s.f) *Protocolo facultativo de la Convención sobre los Derechos del Niño relativo a la venta de niños, la prostitución infantil y la utilización de niños en la pornografía.* ONU. Consultado en https://childrenandarmedconflict.un.org/keydocuments/spanish/crcoptionalproto20.html, el 05 de julio de 2021 a las 17:00 hrs.

Oxman Nicolás (2013). *Estafas informáticas a través de internet. Acerca de la imputación penal del phishing y el pharming.* Universidad Santo Tomás, Santiago de Chile; Chile. Consultado en https://www.redalyc.org/pdf/1736/173629692007.pdf, el 01 de Septiembre de 2021 a las 21:00 hrs.

O´Reilly, Karen (2005). *Ethnographic methods*. Londres: Ed. Routledge.

Paredes M, Sara R. (2014) El cibersuicidio a través de las TIC: un nuevo concepto. Dialnet. Consultado en https://dialnet.unirioja.es/servlet/articulo?codigo=5470249#:~:text=El%20suicidio%20es%20un%20fen%C3%B3meno,la%20sociedad%20a%20nivel%20mundial, el 25 de julio de 2018 a las 17:39 hrs.

Pérez C, María M. (2007). *Infancia y violencia en medios de comunicación. Aproximación a un aspecto de la educación informal*. Universidad Nacional Autónoma de México UNAM: México. Consultado en https://revistas.juridicas.unam.mx/index.php/derecho-comparado/article/view/3966/5032, el 01 de Junio de 2021 a las 22:01 hrs.

Pink, Sara (2019) *Etnografía digital: principios y práctica*. España: Ed. Morata.

Policía Federal (s.f) *¿Qué es la extorsión?.* Portal del Gobierno de México. Consultado en https://www.gob.mx/policiafederal/articulos/que-es-la-extorsion?idiom=es, el 12 de julio de 2021 a las 07:54 hrs.

Portal Único del Estado Colombiano (2019) *¿En qué consisten las medidas de reparación?.* Unidad de víctimas. Gobierno de Colombia; Colombia. Consultado en https://www.unidadvictimas.gov.co/es/en-que-consisten-las-medidas-de-reparacion/44460, el 05 de junio de 2021 a las 08:00 hrs.

Portal Único del Estado Colombiano (2019). *Reparación integral individual*. Unidad de víctimas. Gobierno de Colombia; Colombia. Consultado en https://www.unidadvictimas.gov.co/es/reparacion-integral-individual/286, el 05 de junio de 2021 a las 08:18 hrs.

Portal GESTIÓN. (2019) *Los principales casos de robo de datos personales*; Lima. Consultado en https://gestion.pe/mundo/principales-casos-robo-datos-personales-266922-noticia/, el 10 de marzo de 2022 a las 23:00 hrs.

Procuraduría Federal del Consumidor (2021) *La Ley Olimpia y el combate a la violencia digital.* Gobierno de México. Consultado en https://www.gob.mx/profeco/es/articulos/la-ley-olimpia-y-el-combate-a-la-violencia-digital?idiom=es, el 01 de junio de 2021 a las 09:05 hrs.

Pro Luzmila; González, Juan Carlos; Contreras Walter; Yañez Carlos (2009) *Tecnologías Biométricas aplicadas a la seguridad en las organizaciones.* Universidad Nacional Mayor de San Marcos; Perú. Consultado en https://sisbib.unmsm.edu.pe/BibVirtual/Publicaciones/risi/2009_n2/v6n2/a07v6n2.pdf, el 16 de octubre de 2021 a las 08:27 hrs.

Rebolledo R. (2017) Los 5 casos de espionaje del gobierno mexicano. Portal del periodico El Economista. Consultado en

https://www.eleconomista.com.mx/politica/Los-5-casos-de-espionaje-del-gobierno-mexicano-20170620-0101.html, el 2 de junio de 2022 a las 11:01 hrs.

Red en Defensa de los Derechos Digitales (R3D) (2022). *Inai no debe validar Fan ID de forma opaca y precipitada*. Red en Defensa de los Derechos Digitales R3D. Consultado en https://r3d.mx/2022/06/13/inai-no-debe-validar-el-fan-id-de-forma-opaca-y-precipitada/, el 15 de agosto de 2022 a las 23:00 hrs.

Report, Junior. (2019). *Manipular a través de las redes.* Portal del periodico La Vanguardia. Consultado en https://www.lavanguardia.com/vida/junior-report/20180326/441964145003/manipular-datos-personales-usuarios.html, el 04 de noviembre de 2021 a las 23:09 hrs.

Rincón de Parra, H. Cecilia. (2007). *Economía digital: ¿se requieren nuevos fundamentos teóricos que la definan?.* Universidade do Vale do Rio dos Sinos; Brasil. Consultado en https://www.redalyc.org/pdf/3372/337228632009.pdf, el 18 de octubre de 2021 a las 08:51 hrs.

Rodriguez D. (2022). *Cómo funciona el robo de cuentas de WhatsApp y qué hacer para evitarlo*. Portal de periodico El País. Consultado en https://elpais.com/mexico/2022-01-06/como-funciona-el-robo-de-cuentas-de-whatsapp-y-que-hacer-para-evitarlo.html, el 3 de marzo de 2022 a las 09:11 hrs.

Rodriguez, Juan C. (2021). *Plataformas Digitales y su Regulación Fiscal a Partir del 2020*. PGA Perez Gongora y Asociados. Consultado en https://perezgongora.com/plataformas-digitales-y-su-regulacion-fiscal-a-partir-del-2020/, el 10 de junio de 2021 a las 20:56 hrs.

Rodríguez Z, Jesús. (2005). *Definición y concepto de la no discriminación.* Universidad Autónoma Metropolitana Unidad Azcapotzalco; México. Consultado en https://www.redalyc.org/pdf/325/32513404.pdf, el 16 de agosto de 2021 a las 18:45 hrs.

Rubí, M. (2022). *Roban identidad a 2,088 trabajadores para gestionar créditos fraudulentos*.Portal de Mexicanos contra la corrupción y la impunidad. Consultado en https://contralacorrupcion.mx/roban-identidad-a-2088-trabajadores-para-gestionar-creditos-fraudulentos/#:~:text=Tan%20s%C3%B3lo%20en%20el%20primer,encabezaron%20la%20lista%20de%20fraudes, el 5 de marzo de 2022 a las 12:00 hrs.

Salas, Javier (2017). *La oscura utilización de Facebook y Twitter como armas de manipulación política.* El país. Consultado en https://elpais.com/tecnologia/2017/10/19/actualidad/1508426945_013246.html, el 04 de noviembre de 2021 a las 13:41 hrs.

Sánchez M, Gema. (2012). *Ciberespacio y el crimen organizado. Los nuevos desafíos del siglo XXI.* Universidad Central de Chile; Chile. Consultado en https://www.redalyc.org/pdf/960/96024266004.pdf, el 18 de Septiembre de 2021 a las 18:02 hrs.

Sánchez T, JM; González Z, M Patricia; Sánchez M, María Paloma (2012). *La Sociedad de la Información: Génesis, Iniciativas, Concepto y su Relación con las Tic.* Universidad Industrial de Santander; Colombia. Consultado en https://www.redalyc.org/pdf/5537/553756873001.pdf, el 15 de Febrero de 2021 a las 21:00 hrs.

Scott-Railton J, Marczak B, Razzak B, Anstis S, Herrero P & Deibert R. (2022). Nuevos abusos del Spyware Pegasus identificados en México. Consultado en https://citizenlab.ca/2022/10/new-pegasus-spyware-abuses-identified-in-mexico/ el 2 de febrero de 2022 a las 16:00 hrs

Secretaría de prevención, atención y seguridad universitaria. (s.f). *Protocolo ante amenaza por red social.* Consultado en http://www.serviciosalacomunidad.unam.mx/index_htm_files/Protocolo_de_amenaza_por_red_social.pdf, el 12 de gosto de 2021 a las 15:34 hrs.

Serrano-Barquín, Rocío del C; Ruiz Serrano, Emilio (2013). *Violencia simbólica en internet.* Universidad Autónoma Indígena de México; México. Consultado en https://www.redalyc.org/pdf/461/46128387007.pdf, el 15 de Agosto de 2021 a las 07:51 hrs.

Sevilla Arias, Pablo (s.f) *Marketing / Mercadotecnia.* Economipedia. Consultado en https://economipedia.com/definiciones/mercadotecnia-marketing.html, el 28 de octubre de 2021 a las 11:11 hrs.

Suárez K. (2022). *Cobro por derecho de piso, robo de identidad y amenazas telefónicas: las extorsiones en México alcanzan cifras récord en 2021*. El País. Consultado en https://elpais.com/mexico/2022-02-03/cobro-por-derecho-de-piso-robo-de-identidad-y-amenazas-telefonicas-las-extorsiones-en-mexico-alcanzan-cifras-record-en-2021.html#:~:text=En%202021%20el%20pa%C3%ADs%20registr%C3%B3%20una%20cifra%20r%C3%A9cord%20de%209.407,de%20Seguridad%20P%C3%BAblica%20(SESNSP), el 16 de febrero de 2022 a las 08:00 hrs.

Synnex Westcon- Comstor. (2016). *El lado negativo de la identificación Biométrica.* TD Sinnex. Consultado en https://digital.la.synnex.com/el-lado-negativo-de-la-identificacion-biometrica, el 16 de octubre de 2021 a las 13:28 hrs.

Tavarez M. M & Góngora M. J.J (2021) *Moderación de contenidos en plataformas digitales: derechos humanos y regulación frente a la decisión Trump del Oversight Board*. Portal del Centro de Estudios Constitucionales SCJN. Consultado en https://www.sitios.scjn.gob.mx/cec/blog-cec/moderacion-de-contenidos-en-plataformas-digitales-derechos-humanos-y-regulacion-frente-la, el 8 de enero de 2022 a las 22:34 hrs.

Tellez V, Julio. (2015). *Ciberacoso*. Universidad Nacional Autónoma de México. Consultado en . https://revistas.juridicas.unam.mx/index.php/derecho-privado/article/download/10446/12590, el 30 de junio de 2021 a las 11:00 hrs.

Tidy J. (2021) *Las verdaderas víctimas de los masivos robos cibernéticos de criptomonedas*. Portal del periodico BBC Mundo. Consultado en https://www.bbc.com/mundo/noticias-58344057, el 12 de marzo de 2022 a las 21:09 hrs.

TN. Sociedad. (2016) *seis casos en el que el sexting terminó en tragedia*. TN Sociedad. Consultado en https://tn.com.ar/sociedad/seis-casos-en-el-que-el-sexting-termino-en-tragedia_657925/, el 4 de febrero de 2022 a las 21:00 hrs.

Torres-Melo,J.; Santander J. (2013). Introducción a las políticas públicas. conceptos y herramientas desde la relación entre Estado y Ciudadania. IEMP Ediciones; Colombia. Consultado en https://www.funcionpublica.gov.co/eva/admon/files/empresas/ZW1wcmVzYV83Ng==/imgproductos/1450056996_ce38e6d218235ac89d6c8a14907a5a9c.pdf, el 9 de junio de 2022 a las 20:01 hrs.

Torres, Rosa M., (2005). *Sociedad de la información/sociedad del conocimiento.* Consultado en http://www.ub.edu/prometheus21/articulos/obsciberprome/socinfsoccon.pdf, el 11 de febrero de 2021 a las 12:00 hrs.

Tudela, S; Barrón A. (2017). *Redes sociales: del ciberacoso a los grupos de apoyo online con víctimas de acoso escolar.* Redalyc. Consultado en https://www.redalyc.org/jatsRepo/2710/271053857004/html/index.html, el 08 de Abril de 2021 a las 17:09 hrs.

Trujano Ruiz, Patricia; Dorantes Segura, Jessica; Tovilla Quesada, Vania (2009) *Violencia en internet: nuevas víctimas, nuevos retos.* Universidad de San Martín de Porres; Perú. Consultado en https://www.redalyc.org/pdf/686/68611923002.pdf, el 08 de agosto de 2021 a las 21:00 hrs.

Vargas C. (2007) *Análisis de las Políticas Públicas*. Redalyc. Universidad Católica Boliviana San Pablo; Bolivia. Consultado en https://www.redalyc.org/pdf/4259/425942453011.pdf, el 8 de junio de 2022 a las 09:00 hrs.

Vazquez A, Gregorio. (2019). *Evaluemos el riesgo en el uso de criptomonedas.* El Economista. Consultado en https://www.eleconomista.com.mx/opinion/Evaluemos-el-riesgo-en-el-uso-de-criptomonedas-20190825-0114.html, el 18 de octubre de 2021 a las 11:04 hrs.

Violencia digital (s.f). *Violencia digital*. Consultado en https://violenciadigital.tedic.org/, el 08 de junio de 2021 a las 00:18 hrs.