UACM

Universidad Autónoma de la Ciudad de México

NADA HUMANO ME ES AJENO

COLEGIO DE HUMANIDADES y CIENCIAS SOCIALES

LICENCIATURA EN DERECHO

Análisis de la legislación en materia de los delitos cibernéticos en México

T E S I S

QUE PARA OBTENER EL TÍTULO DE

LICENCIADOS EN DERECHO

P R E S E N T A N

YOLLOCÁLLI CASTILLO MARTÍNEZ

FRANCISCO JAVIER RAMÍREZ GARCÍA

D I R E C T O R

DR. RUSLAN VIVALDI POSADAS VELÁZQUEZ

Ciudad de México, abril de 2025.

UACM
Universidad Autónoma de la Ciudad de México
Nada humano me es ajeno

CA Coordinación Académica

SISTEMA BIBLIOTECARIO DE INFORMACIÓN Y DOCUMENTACIÓN

UNIVERSIDAD AUTÓNOMA DE LA CIUDAD DE MÉXICO
COORDINACIÓN ACADÉMICA

RESTRICCIONES DE USO PARA LAS TESIS DIGITALES

DERECHOS RESERVADOS©

Agradecimientos:

A la Universidad Autónoma de la Ciudad de México por la oportunidad de acceder a la educación de calidad que tanto se necesita, por las herramientas en este camino y por la experiencia académica a lo largo de estos años.

A nuestra familia por el apoyo para llegar a este momento y concluir nuestros estudios.

A nuestro director el Dr. Ruslan Vivaldi Posadas Velázquez por el gran ser humano, que nos ha enseñado a seguir siempre adelante pese a la adversidad, por su apoyo incondicional, por su paciencia, por su comprensión ante cualquier situación, por su extraordinario conocimiento, por ser inspiración y ejemplo de que se puede ser excelente académico y persona al mismo tiempo; que sin él no sería posible esta tesis. Le agradecemos por haber estado en todo momento, expresarle nuestra admiración, respeto y aprecio.
Dar gracias a la vida por conocerlo y ponerlo en nuestro camino, expresarle de nuevo: gracias por ser parte de este sueño que perdurará en nuestra memoria por siempre.

A la Mtra. Ana Elisa Banderas Miranda por su disposición en todo momento, por ser una mujer que nos inspira, por la calidad como académica y persona, por ser un ejemplo real de estar siempre en pro de los y las estudiantes y por sumarse en esta tesis con la mejor actitud y conocimiento.

A la Dra. Adriana Terán Enríquez por haber estado con nosotros a lo largo de la carrera y los conocimientos a través de tanto tiempo siempre presente, por la formación académica de generaciones que con orgullo somos parte de esta casa de estudios.

Al Lic. Antonio Rabasa González de la Vega por su conocimiento, disposición y confianza en esta tesis, por estar a lo largo de nuestra formación académica y fomentar siempre una educación de calidad, donde el derecho debe ser apoyo y lucha contra las injusticias.

La tecnología es un sirviente útil, pero un jefe peligroso.

Christian Lous Lange.

Análisis de la legislación en materia de los delitos cibernéticos en México.

INDICE

INTRODUCCIÓN:

Las redes sociales han revolucionado la forma de comunicación, trabajo, difusión de noticias en tiempo real y sociabilización (acortando distancias e interactuando con otros continentes) sin embargo, también han sido un medio fácil para cometer delitos, intimidar y atacar a víctimas reales.

Este trabajo tiene como objetivo analizar el avance que se ha tenido en la legislación en México de los delitos cibernéticos, respecto a combatir, castigar y erradicar estos delitos, que lejos se han quedado en el avance tecnológico presente y tan acelerado, lo cual ha sido ferozmente impune por la falta de leyes para prevenir, combatir y erradicar, en un país donde aún falta mucho por educar, legislar y ofrecer mismas oportunidades a todos(as) incluyendo el acceso a la tecnología y conocimiento de la misma, que cuando falta esto ya existen otros delitos que las leyes aún no están listas ni cuentan con mecanismos para ello.

Es difícil la comprensión a víctimas y sobrevivientes cuando aún se siguen normalizando casos de maltrato y tortura hacia los animales, quienes su único delito fue vivir con personas (ya sea que están en la calle o en hogares) que justifican todo para dañar, entonces si no es posible respetar la vida de un ser vivo ¿cómo hacerlo hacia los seres humanos? ¿Cómo pueden las leyes (que se necesitan) aplicarse y no ser refugio en el *ciberespacio* para quienes encuentran el lugar perfecto para los crímenes aparentemente *inexistentes* que arropa a quienes la ética es impensable?

Esa pregunta refleja la base de tantos delitos que constantemente surgen desde la violencia que no termina, sino evoluciona mientras que la humanidad da pasos atrás, cuando la vida virtual se convierte en hogar de quienes cobardemente actúan desde la realidad creada por el hombre y que podría ser su destrucción, porque la tecnología se vuelve el *ciberespacio* para ir en contra de la misma especie.

Este trabajo cuenta con tres capítulos, en los cuales se analizará la legislación de los delitos *cibernéticos* en México. En el primer capítulo se abordará la descripción jurídica de los delitos *cibernéticos*, esto mediante los antecedentes y tipos de la violencia digital, así como los tipos de *ciberviolencia*.

En el segundo capítulo se hará un análisis de la legislación en materia de delitos *cibernéticos* en México porque es necesario que las leyes que se han dado en algunos Estados, se apliquen en todo el país con el fin de que esto se vuelva universal.

Finalmente, en el tercer capítulo, se dará una visión hacia una reclasificación de las penas en materia de delitos *cibernéticos*, desde el ámbito nacional e internacional y una propuesta hacia salud mental, repercusiones, alcances y límites de los riesgos de los avances tecnológicos.

CAPÍTULO 1. DESCRIPCIÓN JURÍDICA DE LOS DELITOS CIBERNÉTICOS.

1.1.-ANTECEDENTES HISTÓRICO- JURÍDICOS DE LA VIOLENCIA DIGITAL.

Hablar de violencia y sobre todo en México, un país donde se han *normalizado* acciones, expresiones, justificaciones por tradición, costumbre y cultura para que se perciba como parte de una forma de ser de los habitantes la violencia, es muy benéfico para quienes intentan hacer de la agresión a través de la tecnología un delito del que la ley tiene muchos vacíos, como el *ciberacoso* o el *ciberbullying*, donde todos estamos expuestos, que si bien puede abarcar desde cualquier edad, género, clase social o cualquier forma en la que se vea afectada la vida de una persona; lo cierto es que el ataque en redes es una situación en la que el mundo debe poner atención.

> La vinculación entre tecnología y delito no comenzó con el desarrollo de las computadoras. Con el surgimiento del telégrafo durante el siglo XIX se interceptaban comunicaciones para la transmisión de información falsa con fines económicos. Ya con la irrupción del teléfono, durante la década del 60, diferentes programadores informáticos o especialistas en sistemas intentaban boicotear el financiamiento gubernamental a la guerra de Vietnam mediante el uso gratuito del servicio. Los phreakers (neologismo proveniente de las palabras en inglés "freak", de rareza; "phone", de teléfono; y "free", gratis) utilizaban unas blue boxes o cajas azules que reproducían tonos de llamadas similares a los utilizados por la Bell Corporation, y la ATT establecía comunicaciones gratuitas de larga distancia. En cuanto a la utilización de computadoras, la principal preocupación estaba dada por el manejo de la información a partir del almacenamiento y procesamiento de datos personales producto de obras de ficción como 1984 de Orwell.[1]

Con la pandemia por COVID-19 la tecnología dio un salto significativo para *vivir dentro de una nueva normalidad* que en ese momento la incertidumbre constante sirvió para que dentro de esa nueva realidad (virtual) las personas continuaran adelante con su vida, trabajo (lo que trae consigo remuneración) escuela, incluso distracción (como plataformas de *TikTok*) pero todo esto avanzó a tal escala que surgieron reuniones virtuales grupales, entrevistas de trabajo y *clases en línea* que

[1] *Gustavo Sain, Cibercrimen y Delitos Informáticos. Los nuevos tipos penales en la era de internet*, ERREIUS, Dirección Nacional del Derecho de Autor. Hecho el depósito que marca la ley 11723, ISBN 978-987-4405-56-2, p.7, 2018, de:
https://www.pensamientopenal.com.ar/system/files/2018/09/doctrina46963.pdf

llevaron al mundo a plantearse si estábamos listos para ese despegue tan acelerado, pero sin regulación jurídica de por medio.

Si bien la tecnología *cibernética* ayudó a conectar al mundo y en el caso de las escuelas a seguir con clases, también se volvió una herramienta que al terminar (aunque con incertidumbre de cómo acabaría y cuándo) la pandemia, la vida no sería igual, ni la forma de pensar, de comunicarnos porque todo lo digital se volviera una herramienta indispensable y que en otro años podría haber sonado impensable o que quizá no lo viviríamos (por ejemplo, caricaturas como *los supersónicos* se veía impensable llegar a una situación como la que se planteaba en esa serie infantil).

> Las conductas delictivas han estado presentes y evolucionado en la historia de la humanidad; y en las sociedades del siglo XXI con la acelerada revolución tecnológica han surgido y crecido exponencialmente los ciberdelitos o delitos informáticos. Su conceptualización, características y legislación aplicable, han sido temas del debate jurídico en los últimos años, y en México es un tema pendiente, por lo que se considera importante analizarlos y determinar si su reconocimiento explícito en los ordenamientos penales contribuye a la denuncia, investigación, persecución, prevención y disminución.
>
> Los primeros delitos informáticos comenzaron en los años sesenta con la recopilación de información personal sin consentimiento; pero el uso de computadoras en el sector comercial supuso que los más comunes fuesen el fraude informático, la manipulación de datos o el espionaje empresarial. En los ochenta y noventa, la generalización de computadoras en la población originó infracciones masivas contra la propiedad intelectual como la piratería del *software*, en productos audiovisuales, la música y el cine. Con internet en el siglo XXI, se crearon nuevas formas y métodos de violar la intimidad personal, suplantar la identidad, cometer fraude o robo, acceder y difundir contenidos o productos y servicios ilícitos.
>
> Estos delitos han incrementado por el confinamiento que trajo la pandemia originada por la covid-19, que obligó a que todas las actividades transitaran a la digitalización; y en México de acuerdo con el informe de la Secretaría de Seguridad y Protección Ciudadana, se reportó un aumento del 4.1% en delitos relacionados con derechos de autor, propiedad intelectual e industrial, contra vías de comunicación y correspondencia, falsedad y falsificación de información. Con lo anterior en consideración, se evaluará el marco jurídico internacional y nacional aplicable a los delitos informáticos, se analizarán los ordenamientos penales de las entidades mexicanas para determinar si reconocen los delitos informáticos, y si esta acreditación contribuye a la denuncia e investigación.[2]

[2]Miryam Georgina Alcalá Casillas, Delitos informáticos en México. Reconocimiento en los ordenamientos penales de las entidades mexicanas, PAAKAT: revista de tecnología y sociedad, rev.

Hoy en día las empresas que se desempeñan a través del *home office*[3] han hecho eficientes los procesos porque representan menos gastos como por ejemplo en papel y el pago de renta, pero también conoceríamos una nueva realidad que poco o nada es regulada por la ley (un trabajo en casa sin regulación de jornadas laborales y se tendría una idea equivocada que al no salir el trabajador se *ahorraba* mucho por un mismo salario, sin contemplar todo lo que conlleva) y esto daría paso a que los empleados quedaran a disposición de las empresas con la justificación de la *supuesta comodidad en casa*, ahorro de tiempo, de traslado al centro laboral, incluso de ropa; pero las empresas fueron quienes mayormente ganaron por la mano de obra en situación de vulnerabilidad, con menores salarios y sin condiciones adecuadas para los trabajadores mínimamente debían tener un salario digno que percibir y muchas veces sin prestaciones u horarios establecidos.

La comunicación, entretenimiento y trabajo giró en torno a la tecnología y mientras más avanzaba la pandemia, las leyes se quedaban cada vez más atrás. Si bien podemos atribuir a que es *nuevo*, lo cierto es que en ello hubo patrones quienes abusaron y por lo cual causaron víctimas con daños irreparables (en su economía, tiempo, salud y prestaciones) como si se tratará de la época del fordismo, donde los trabajadores se veían como máquinas reemplazables y mano de obra barata moderna.

Tanto el taylorismo como el fordismo representan en la historia el símbolo de lo que significa la producción industrial, ya que ambos se dieron en lo que se denominó Revolución Industrial; en donde lo importante únicamente era más producción, en menor tiempo y a más bajo costo.

---

tecnol. soc. vol.13 no.24 Guadalajara, Epub, versión On-line ISSN 2007-3607, 16-Oct-2023, Computer crimes in Mexico. Recognition in the criminal laws of the Mexican entities, Universidad Michoacana de San Nicolás de Hidalgo, Universidad Autónoma de Baja California, México, SCIELO, de: https://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S2007-36072023000100005

[3]Término para designar al trabajo desde casa o a distancia, casi siempre mediante herramientas y dispositivos electrónicos.

En el caso del Taylorismo (ingeniero estadounidense Frederick Winslow Taylor) se trató de ser eficiente en el trabajo mediante la división de trabajo y de tareas en el mismo. Con esta división llegar al punto de poner tiempos específicos para la realización de cada tarea, que hoy en día se utiliza en los tiempos por ejemplo en empleos como *call center* o métricas a los trabajadores donde se realiza exclusivamente la función sin otro tipo de actividad, lo que genera que el empleado sea experto y cada vez realizará las actividades automáticamente como una máquina. Desafortunadamente, el salario y pago realizado estará de acuerdo con la producción por tiempo o por pieza, no a horarios establecidos en jornadas laborales porque por estas mediciones, lo que vale es la productividad.

En el caso del Fordismo (Henry Ford) se enfatizó en producir en masa, reducir la jornada laboral y el costo en el material para que mediante la reducción de material se pudiera amplificar el público que podría consumir. Esta forma, se buscaba mejorar, se implementa la producción en mayor escala y división en tareas asignadas a trabajador para producir más y en menor tiempo.

El avance tecnológico, incluyo al aparato jurídico se detuvo (posteriormente comenzaron audiencias virtuales en Tribunales, con medidas sanitarias) pero poco a poco comenzaba o se hicieron más tangibles y presentes, vacíos para delitos y actos que ni siquiera estaban tipificados y menos en el caso de México (que las leyes avanzan poco o sólo pueden ser perfectas en papel y no en la práctica) ocuparía recursos o interés para sanciones y prevención.

Los delitos y virus *cibernéticos* han *evolucionado* como las enfermedades físicas, tenemos:

> Los antecedentes de los delitos informáticos van a la par del desarrollo de las tecnologías de la información. Con el desarrollo de la tecnología, la sociedad se ha visto en un panorama de avance y desarrollo en todas sus áreas; por desgracia, la delincuencia también se ha beneficiado de esto. Entre los beneficios que ofrece el uso de redes de comunicación a los delincuentes se encuentran: la capacidad de cometer delitos en y desde cualquier parte del planeta, velocidad, gran cantidad de víctimas potenciales y anonimato, entre otros. Uno de los primeros y más importantes ataques en la historia de Internet se remonta a CREEPER en 1971,

escrito por el ingeniero Bob Thomas, es considerado el primer virus informático que afecto a una computadora el cual mostraba un mensaje en los equipos infectados, el cual, si no causaba daño alguno, fue la base para el desarrollo de ataques posteriores con pérdidas multimillonarias, como se menciona en el sitio web de la INTERPOL "se estima que en 2007 y 2008 la ciberdelincuencia tuvo un coste a escala mundial de unos 8.000 millones de USD".

Es conveniente identificar de forma clara lo que se entiende por delito informático. Existen diversas definiciones respecto; un ejemplo es la definición de Camacho Losa, citada por Leyre Hernández, quien considera como delito informático: "toda acción dolosa que provoca un perjuicio a personas o entidades, sin que necesariamente conlleve un beneficio material para su autor aun cuando no perjudique de forma directa o inmediata a la víctima y en cuya comisión intervienen necesariamente de forma activa dispositivos habitualmente utilizados en las actividades informáticas". Otra definición destacable es la establecida en el Código Penal para el Estado de Sinaloa en su Artículo 217: Comete delito informático, la persona que dolosamente y sin derecho: Una definición más simple que se propone es la siguiente: Delito informático es el uso de cualquier sistema informático como medio o fin de un delito. De esta manera se abarcan todas las modalidades delictivas de acuerdo al marco legal de cada país; para esto es conveniente definir qué es un sistema informático. De acuerdo con el Convenio sobre la Ciberdelincuencia adoptado en Budapest, en 2001: "Por sistema informático se entenderá todo dispositivo aislado o conjunto de dispositivos interconectados o relacionados entre sí, siempre que uno o varios de ellos permitan el tratamiento automatizado de datos en ejecución de un programa. "Esta definición abarca no solo a las computadoras, sino a otros tipos de dispositivos como Data Centers, módems y cualquier otro sistema que permita la ejecución de un programa y/o manipulación de datos. Por otra parte, la guía del taller de Prevención contra el Delito Cibernético de la Secretaria de Seguridad Pública (SSP) define el delito cibernético como: "Actos u omisiones que sancionan las leyes penales con relación al mal uso de los medios cibernéticos."[4]

Los ataques *cibernéticos* a bancos e Instituciones financieras han sido pioneras en el tema de buscar combatir, atacar y sancionar estos delitos mediante mayor control en aplicaciones, códigos de seguridad, requisitos para identificación y métodos para evitar fraudes, sin embargo; esto no ha ocurrido en usurpación de identidad en cuanto a delitos de connotación sexual, acoso y hostigamiento donde sigue estando en segundo plano porque al no estar involucrado el dinero de por medio, la persona no es igualmente respaldada. Por ejemplo, en centros de reclusión es común

[4]Jesús Alberto Loredo González y Aurelio Ramírez Granados, *Delitos informáticos: su clasificación y una visión general de las medidas de acción para combatirlo*, FCFM-UANL Facultad de Ciencias Físico Matemáticas Universidad Autónoma de Nuevo León San Nicolás de los Garza, Nuevo León, México, Investigación/ Seguridad en ti, Celerinet enero-junio 2013, p.45.

escuchar historias de años de sentencia por robo a un *Oxxo*, *Walt Mart* o cadena trasnacional, incluso por un pan o leche, pero en delitos *cibernéticos* de acoso, violencia, en el peor de los casos, desaparición forzada y feminicidios no.

Incluso podemos cuestionar ¿si existe interés real y presupuesto para combatir los delitos *cibernéticos*? La respuesta es no, porque, por ejemplo; en el gobierno de Andrés Manuel López Obrador (AMLO) se enfatizó en apoyo a más y más programas sociales en una especie de dar de comer, en vez de enseñar a pescar, donde es más grave no ser *caballeroso* que atender a víctimas de delitos y sin planteamientos frente a delitos *cibernéticos*, que desafortunadamente las personas no son apoyadas, pero cuando se trata de errores en sus cuentas bancarias o víctimas de fraudes porque es *justicia* para unos (empresarios) con poder ya sea adquisitivo, político o judicial y no para la población que al haber un error en su cuenta pareciera tener que enfrentarse a burocracia del sector privado, pero con mayor herramientas para prevenir y combatir.

Lo anterior, nos lleva a preguntarnos: *¿es más grave el robo financiero que un ataque cibernético a una víctima de acoso, hostigamiento sexual o usurpación de identidad para dañar su reputación?* (en el caso de suplantación de identidad o creación de perfiles falsos en redes sociales como en *Facebook* u otras redes para que incluso la vida de la vida este en peligro).

El *hackeo* de cuentas a empresas como *Coppel*, el robo de identidad a una persona en donde fue víctima de acoso, hostigamiento o que sufre por parte de expareja (s) y usa la tecnología para intimidar, perjudicar a la víctima y su familia, afectando su trabajo, escuela y el daño a la reputación de esta sumado al fotomontaje o historias falsas que se viven en una sociedad que está despersonalizada de valores y con la necesidad de crear vidas falsas en redes sociales o darles un uso delictivo actuando desde la impunidad que la lo digital.

¿Es más grave el ataque *cibernético* a una empresa que el uso mediante la tecnología digital, por ejemplo, en pornografía infantil? ¿la falta de regulación ante ataques terroristas y la facilidad de comunicación entre ellos por la tecnología? Lo cual no significa que sea justificación para acusar sin pruebas y juicio a personas de terrorismo y violar sus derechos humanos.

Las consecuencias hacia los delitos *cibernéticos* en la vida real son importantes para tomar conciencia que ese *mundo que parece irreal* repercute en lo real, en el día a día de una persona como su empleo, reputación y todo a su alrededor. La víctima no sólo tiene que lidiar con las redes sociales, sino con daño psicológico y hasta hostigamiento por parte de cercanos (como vecinos, su misma familia, escuela y lugar de trabajo) en la idea de dejarse llevar por una noticia o perfiles falsos que vuelve a la tecnología una apariencia que posiblemente sea un estereotipo falso.

Situaciones que por una *selfie*[5] en un lugar peligroso se han muerto personas y sólo queda como imprudencia por parte del *cujus*[6] y no en concientizar o prohibir incluso el uso de dispositivos en determinados lugares por parte de las autoridades correspondientes.

Así como la evolución en el comercio electrónico ha unido fronteras y ha permitido que el mundo esté conectado, también:

> En México, la figura del comercio electrónico está regulada principalmente en el Código de Comercio y en la Ley de Protección al Consumidor. En el artículo 89 del Código de Comercio se ha definido a los mensajes de datos como "… La información generada, enviada, recibida o archivada por medios electrónicos, ópticos o cualquier otra tecnología a través de un sistema de información digital". Dicha protección y defensa se realiza, entre otras facultades, a través del procedimiento de conciliación que tiene encomendada la CONDUSEF, quien ha detectado hallazgos que pueden ubicarse en supuesto de riesgo que constituyen vulnerabilidades respecto a las acciones tendientes a la prevención del LD, en perjuicio de los usuarios. Las tipologías identificadas por la CONDUSEF como el uso indebido de tarjetas por parte de terceros, Phising, Pharming. Spoofing. Carding, el uso indebido

[5]Se refiere a tomarse una foto un (a) mismo (a), un autorretrato.
[6]Término jurídico para referirse a una persona muerta.

> de información bancaria conservada en navegadores web, entre otros, constituyen conductas fraudulentas específicas que buscan aprovecharse del engaño o error del usuario para obtener información bancaria del mismo, a efecto de realizar operaciones a su cargo y que actualizan el supuesto que establece la conducta o delito predicado relativo a la realización de operaciones con recursos de procedencia ilícita, mismos que constituyen una vulnerabilidad para el riesgo de LD[7]

Pero más allá de que únicamente se centren en los delitos *cibernéticos* de acuerdo con situaciones como fraude, por ejemplo; en lo económico representa un vacío aún más lejano y poder darle a cada delito *cibernético* el debido tratamiento tanto por quienes hacen las leyes, como por quienes las imparten y en especial, teniendo en cuenta que los medios para obtener pruebas requieren presupuesto y no únicamente la tipificación del delito y después al no cumplirse algún supuesto o exista laguna en la ley da la apariencia como si nada hubiera sucedido, ignorando que existe un delito, una conducta y víctima (s).

> La delincuencia informática se encuadra dentro de lo que se conoce como "Derecho informático". Éste es el conjunto de normas jurídicas que regulan la utilización de los bienes y servicios informáticos en la sociedad, incluyendo como objeto de estudio: 1º el régimen jurídico del software; 2º el derecho de las Redes de transmisión de datos; 3º los documentos electrónicos; 4º los contratos electrónicos; 5º el régimen jurídico de las bases de datos; 6º el derecho de la privacy; 7º los delitos informáticos; y 8º otras conductas nacidas del uso de los ordenadores y de las redes de transmisión de datos…
>
> La expansión de Internet en la década de los noventa llevó aparejado el surgimiento de un nuevo método para difundir contenidos ilegales o dañosos, tales como pornografía infantil o discursos racistas o xenófobos. Serán justamente las conductas vinculadas a la difusión de contenidos ilícitos las que más pueden aprovecharse de la enorme implantación que tiene la Red a nivel mundial…
>
> En este período también se consolida la dependencia que los gobiernos y organismos internacionales tienen de los sistemas informáticos, tanto para su buen funcionamiento como para el almacenamiento de datos importantes y/o secretos y ello pondrá en el punto de mira para la comisión de delitos que atenten contra la seguridad del Estado, como la comisión de ataques terroristas a través de la Red, a los sistemas informáticos de estos Entes.
>
> Hoy, con la expansión del uso de los sistemas informáticos y de la telemática en todos los ámbitos, tanto públicos como privados, prácticamente cualquier delito (homicidio, tráfico de drogas, delito de terrorismo, etc.) puede ver favorecida su comisión a través de la utilización de las nuevas tecnologías de la información.[8]

---

[7]Evaluación Nacional de Riesgos de Lavado de Dinero y Financiamiento al Terrorismo, noviembre 2023, Secretaría de Hacienda y Crédito Público, p.52.

[8]Leyre Hernández Díaz, *El Delito Informático,* Eguzkilore, Número 23, San Sebastián diciembre 2009, Gobierno Vasco, pp. 227-228, 230.

La pornografía y el racismo son temas de mucho tiempo atrás, que han avanzado en su forma de seguir operando, pero de una manera más sutil, justificable y fácil de difundir, disfrazado de un pensamiento más liberal y sitios *web* que no se encuentran regulados en la ley como, por ejemplo, redes sociales donde prácticamente el dinero compra todo y que desafortunadamente puede más que la justicia o el daño provocado.

A lo anterior, se suma el tráfico de órganos y animales que de un continente a otro pueden logísticamente operar para hacer daño con tal de conseguir dinero porque se lucra también mediante el tráfico de animales para laboratorios (que no representan vidas, sino dinero) que también se beneficia de la tecnología y contactos criminales para cometer delitos. Si bien el uso de tecnología podría justificarse para *mejorar* (que esto es realmente cuestionable) se suman los malos tratos que en nada justifica ni en los rastros, zoológicos, animales domésticos y no domésticos en condiciones de maltrato y lo mismo ocurre para obtener dinero con la conciencia de autoridades o leyes que no actúan, no muestran interés (ni por legisladores ni por el aparato judicial) y tampoco tiene recursos para atacar este tipo de delitos que se cometen desde la red.

Estamos en un momento crítico en el sentido de que la tecnología está rebasando al propio humano y a las leyes porque ni siquiera se cuenta con mecanismos y sanciones para los delitos se han ido dando, cuando están surgiendo nuevos que aún no tienen una definición, denominación, supuestos jurídicos y mucho menos sanción.

La solución de más cárceles de alta y mediana seguridad o la existencia de las actuales no ha funcionado, como por ejemplo Guantánamo que no es un lugar de reinserción social, son centros de tortura donde se violan los derechos humanos y la desigualdad de penas para distintos delitos es notoria, porque los que están ahí puede ser desde quién robó algo para comer como quién comete pornografía como

el caso de *Los demonios del Edén*[9] incluso con grabaciones que el dinero, la justicia y la ley no siempre tienen que ver con el delito ni para quién se sanciona o no. Casos de terrorismo (con pruebas) o sólo la sospecha de ser terrorista (sin pruebas) y un juicio que tal vez nunca llegue, pero eso hace diferencia para considerarse una amenaza sin juicio y si permanecer privado de su libertad.

Referirnos a Guantánamo es remontarnos al 11 de septiembre de 2001 en Estados Unidos (las Torres Gemelas en Nueva York y el Pentágono) donde se responsabilizó de dicho ataque al país de Afganistán, específicamente al grupo terrorista de Al-Qaeda bajo el liderazgo de Osama Bin Laden y se desato una guerra desde los discursos hasta lo físico por parte de miembros de esa organización y país, que fueron recluidos en Guantánamo, que es un centro conocido por serias violaciones a derechos humanos y tortura contra prisioneros, pero donde este lugar no reconoce ningún tipo de derecho a quienes están internados por tratarse de ataques directamente contra la Nación.

Puede ser difícil la definición de terrorismo porque ni la ONU ni E.U.A, por ejemplo, han abordado el tema para mayor claridad, ni tampoco otros Organismos han dado una definición al respecto, lo cual es contradictorio porque es común escuchar de la lucha contra el terrorismo, lucha antiterrorista, detenidos y prisioneros por actos de este tipo sin que realmente en principio exista definición, leyes y quién regule dichos centros de detención exclusivamente para este tipo de delitos, lo contradictorio es que operan bajo reglas por debajo del agua y de las cuales la tortura es parte de ello.

La Real Academia Española se acerca un poco más a la definición de terrorismo hacia situaciones de dominación por terror, violencia para crear y propagar terror.

[9]Libro de autoría de Lydia Cacho donde el poder es más fuerte ante la pornografía y prostitución infantil.

Tenemos por ejemplo el delito de robo tiene como fin adueñarse de un bien ajeno, que puede ser por medio de arma (ya sea blanca o de fuego) o por medio de robo por parte de un carterista. El fin es atentar contra el patrimonio para poder apoderarse de algo y obtener lucro con agravantes dependiendo de su modalidad, lo robado y el contexto. Esto ya en la ley y de forma más homogénea es reconocido y tangible en las legislaciones, contrario a otros delitos como el anteriormente mencionado y los tratados a lo largo de esta investigación respecto a delitos *cibernéticos*.

En tiempos electorales está muy de *moda* utilizar las redes sociales para ser más visible y hacer campaña (desde Ciudad de México CDMX y otras entidades como por ejemplo Monterrey candidatos (as) presidenciales como también lo jurídico con el caso del ex Ministro Arturo Zaldivar) en vez de informar ha servido para difamar a una persona, incluso la publicación de una *supuesta nota* que no requiere autoría como en un libro, tampoco identificación de la cuenta ni ningún dato que respalde quién está detrás de determinado comentario puede parecer no tener relevancia, lo cierto es que el derecho y las leyes deben garantizar que no se cometan delitos *cibernéticos* ni de ningún tipo, contemplando mecanismos que en verdad persigan y castiguen a quienes incumplen la ley porque parece más delito ser víctima que cometer algún delito.

La tecnología en la parte positiva (y el rumbo que debió seguir lo digital) ayudó en la contingencia del COVID-19 creando rápidamente vacunas, difusión de la situación y comunicación en el mundo, pero también esa tecnología (en el lado negativo) se usó para desinformar y crear pánico ante una emergencia sanitaria *nueva*.

Pero de esta tecnología que se iba desarrollando rápidamente pasamos a depender del tipo de persona que las utiliza y de esto su buen o mal uso son las leyes y operadores jurídicos quienes deben hacer justicia, porque no significa libertad de expresión utilizar un medio electrónico para dañar cualquier aspecto de la persona

y peor aún sin que haya consecuencias de por medio, poniendo incluso en duda su buen nombre sólo en base a la aparente *libre expresión* sin límite que básicamente se justifica para hacer y decir lo que sea, incluso sin ética personal de por medio.

Las redes sociales fueron fundamentales para no detener el mundo laboral durante la contingencia (por ejemplo, seguir trabajando y por lo tanto no dejar de percibir salario mediante *home office*[10]) sin embargo; se generó abuso por parte de patrones para extender horarios laborales, justificar no percibir el mismo salario porque ya no había que usar transporte para llegar al lugar de trabajo y sin regulación alguna que respaldará los derechos de los empleados. Lo cual nos muestra que por una parte la tecnología iba avanzando en ciencia y por el otro los delitos se deban y continuaban en medio de caos social y psicológico de la incertidumbre de qué sucederá, cuándo acabará o en qué tiempo se podría tener un poco de certeza respecto a la vida que teníamos antes, incluso si volvería esa *normalidad* antes de la contingencia.

El término *home office* se refiere al trabajo desde casa o aquel lugar que no sea una oficina, lo que ha generado *comodidad* en el trabajador y ahorro de presupuesto por parte de las empresas, por ejemplo: ahorro en renta de instalaciones (oficinas) o equipo (computadoras, impresoras, mobiliario) obteniendo el trabajo por parte del trabajador.

No se contempló una nueva modalidad de trabajo en donde las empresas eran responsables de brindar condiciones adecuadas para los trabajadores como por ejemplo, equipo de oficina como una silla o el pago por electricidad e internet que el empleado absorbía de su mismo salario, no se contemplaron las horas extras, tampoco condiciones favorables para que no se convirtieran en una nueva forma de *esclavitud moderna laboral* que empeoraba con reuniones virtuales denominadas *salas permanentes* en tiempo real como si se tratará de cámaras de video durante las jornadas laborales porque invadían la privacidad del trabajador (de su hogar y

[10]Término para designar el trabajo desde casa.

su familia) violatorio derechos humanos incluso, sin tomar en cuenta la inversión para trabajadores a su privacidad o en el caso de las escuelas si los niños tenían computadora o equipo necesario para esta nueva vida que de no ser así serían desplazados y haría más evidente la brecha social de poder adquisitivo, así como herramientas en que las empresas gastaban menos y era más redituable como por quienes ya no utilizaron las instalaciones físicas y por tanto el pago de renta del inmueble o servicio.

Las leyes no estaban acordes al avance mediante la tecnología y el mal uso avanzando en medio del pánico durante y al término del COVID-19 (poque apenas serían más evidentes las secuelas) que incluso socialmente creó temor como si se tratará de una película donde por tanto tiempo se estuvo en cautiverio y ahora el reto para la sociedad, leyes y autoridades era brindar mecanismos óptimos de seguridad, la psique de las personas al volver a incorporarse a una nueva forma de vida y de exposición por las redes sociales que las leyes aún no contemplaban porque:

> Los delitos informáticos, son actos ilícitos cometidos mediante el uso inadecuado de la tecnología, atentando contra la privacidad de la información de terceras personas, dañando o extrayendo cualquier tipo de datos que se encuentren almacenados en servidores o gadgets.[11]

Los delitos *cibernéticos* pueden parecer intangibles y por lo tanto las consecuencias o repercusiones no son a simple vista tangibles, pero presentes en la vida de las personas y más en una era virtual de la cual sería impensable llegaría tan rápido, parecía de un futuro no próximo como si se tratará de una película o caricatura sin mecanismos y donde poco a poco se daban más caos de revictimización desde la misma toma de denuncia para algo que no existía, donde el agresor seguiría libre, la víctima con impunidad y vida arruinada en un país (México) que incluso en feminicidio siguiendo un camino difícil donde las autoridades, esperan que la de

[11]Maria Gabriela Acosta, Benavides, Merck Milko García, Nelson Patricio, *Delitos informáticos: Impunidad organizacional y su complejidad en el mundo de los negocios Cybercrime: Impunity organizational and its complexity in the business of the world*, Revista Venezolana de Gerencia, Universidad del Zulia, vol. 25, núm. 89, 2020, Universidad del Zulia.

cujus demuestre que fue víctima de violencia y aun así impune porque a veces las revictimización puede venir del mismo género.

Dentro de los derechos humanos que son vulnerados o violentados a causa del *home office* se encuentran:
-Acoso laboral, que se puede dar entre los mismos compañeros (misma jerarquía), por un superior, el jefe sea víctima, en la designación no equilibrada de actividades, designar actividades innecesarias, no designar trabajo, exceso de trabajo, cambio de puesto repentino y sin justificación.

-Agresiones psicológicas:
Criticas innecesarias, denostación, demeritar su trabajo, menospreciar al trabajador, ignorar y aplicar *ley del hielo*, descalificación.

-Daños por acoso laboral:
Ansiedad, depresión, estrés, frustración, terminar con autoestima, impotencia, falta de sociabilización, humillación, problemas mentales y físicos.

-Sociales:
No incluir en actividades, pérdida del empleo, disminución de la productividad, rotación.

-Derechos Humanos violentados por acoso laboral:
*La vida (por las consecuencias mentales y físicas).
*Integridad física, psicológica y moral (por las alteraciones que se generan y en lo moral las humillaciones).
*Libre desarrollo de la personalidad.
*Acceso a una vida libre de violencia.
*Discriminación.
*Trato digno.
*Ambiente laboral sano.

*Igualdad laboral y condiciones justas.
*Igualdad ante la ley.

Es por ello importante enfatizar en legislación y leyes en materia de delitos *cibernéticos* como prioridad, protegiendo, apoyando y previniendo existan víctimas.

Donde el delito efectivamente sea plasmado y sancionado por la ley, con personas (Ministerio Público, policías, fiscalías y jueces) con empatía hacia una posible víctima que vive en una cárcel mental e incluso no logra ver una vida mejor y más allá de paranoia, de creerle siempre y obtenga justicia.

Las elecciones presidenciales que se llevaron a cabo el pasado junio de 2024, desde los debates no existieron propuestas en nada, sólo la exposición para evidenciar quién es peor o ha dejado de hacer más, no hay reformas para códigos en materia de delitos informáticos, que se minimizan desde el momento de poner una denuncia y los supuestos para que se cumpla el delito, incluso en temas tan delicados como la vida en el caso de feminicidio sigue sin ser importante para la sociedad y menos para las autoridades que son responsables del bienestar de la población.

Los debates presidenciales sirvieron para ofender y denostarse entre ellos (as) mismos (as) como si se tratara de quién puede ocupar el tiempo en prometer lo inalcanzable, sin presentar propuestas reales e importantes como en temas de delitos *cibernéticos* y en salud mental que tanto afecta a quienes sufren la impunidad y vacíos en leyes.

La política se ha convertido en un circo y lo preocupante es que entonces las reformas y propuestas de reformas están a cargo de quienes no cuentan con conocimiento ni interés para víctimas reales.

No existe interés tanto de candidatos(as) como legisladores(as) para castigo real a estos delitos que tanto dañan a las víctimas y a la sociedad, también asumir que somos culpables como sociedad por seguir estereotipos y dejarnos llevar por canciones en campañas o *influencers*[12] (como Mariana Rodríguez en Monterrey) y sea más importante que en enfatizar en la importancia en las penas para los delitos de carácter *cibernético* y los daños.

Por ejemplo, la canción que se utilizó como parte de la campaña de Mariana Rodríguez:

> 'Lo Nuevo': canción de Mariana Rodríguez y Samuel García
> La canción de 'Lo Nuevo' de Mariana Rodríguez con Samuel García, producida al estilo de una campaña, dura minuto y medio y dice lo siguiente:
> ¡Arráncate compadre!
>
> Lo nuevo es emocionante
> Lo nuevo es apasionante
> Lo nuevo está siempre adelante.
> El futuro es brillante
>
> El pasado ya no funciona
> Lo nuevo emociona
> El pasado se desmorona
> El futuro es ahora
>
> El pasado nos dividía
> Hoy comienza un nuevo día
> El pasado nos deprimía
> El futuro es alegría
>
> Es el comienzo, todo estará mejor
> Y si no me crees, pregúntale a Nuevo León[13]

Este tipo de publicidad, como difusión, ritmo y mensaje tienen relevancia porque más allá de presentarse como una propuesta *juvenil* en debates o en iniciativas en mejora de la población, nos habla de una persona que desde su privilegio llega a un sector que tal vez este o no interesado en el fondo de su agenda política, pero

[12]Término para referirse a una persona que tiene influencia sobre otro (a), específicamente en redes sociales.
[13] Trascripción de la canción difundida en diversos medios y redes sociales.

que al centrarse en este tipo de campañas mediante la música abarca a un amplio sector de la población que al ser de más bajos recursos (incluidas las comunidades indígenas que son los más vulnerables) realmente se recuerda el nombre de ella frente a otra persona que puede presentar propuestas reales, pero el tener el nombre presente puede ser determinante para una elección por más absurdo que parezca.

Puede más la influencia de una canción o cara *bonita* (en términos de burgués y racismo) que propuestas donde por lo menos durante tres o seis años podrá convertirse en justicia o injusticia:

> En 1983, la Organización de Cooperación y Desarrollo Económico (OCDE) inició un estudio de la posibilidad de aplicar y armonizar en el plano internacional las leyes penales a fin de luchar contra el problema del uso indebido de los programas computacionales.
> Las posibles implicaciones económicas de la delincuencia informática, su carácter internacional y, a veces, incluso transnacional y el peligro de que la diferente protección jurídico-penal nacional pudiera perjudicar el flujo internacional de información, condujeron en consecuencia a un intercambio de opiniones y de propuestas de solución…
> La mayoría de los miembros de la Comisión Política de Información, Computadoras y Comunicaciones recomendó también que se instituyesen protecciones penales contra otros usos indebidos (Lista optativa o facultativa), espionaje informático, utilización no autorizada de una computadora, utilización no autorizada de un programa de computadora protegido, incluido el robo de secretos comerciales y el acceso o empleo no autorizado de sistemas de computadoras…
> Una vez desarrollado todo este proceso de elaboración de las normas en el ámbito continental, el Consejo de Europa aprobó la recomendación R(89)9 sobre delitos informáticos, en la que se "recomienda a los gobiernos de los Estados miembros que tengan en cuenta cuando revisen su legislación o preparen una nueva, el informe sobre la delincuencia relacionada con las computadoras... y en particular las directrices para los legisladores nacionales". Esta recomendación fue adoptada por el Comité de Ministros del Consejo de Europa el 13 de septiembre de 1989.
> Las directrices para los legisladores nacionales incluyen una lista mínima, que refleja el consenso general del Comité, acerca de determinados casos de uso indebido de computadoras y que deben incluirse en el derecho penal, así como una lista facultativa que describe los actos que ya han sido tipificados como delitos en algunos Estados pero respecto de los cuales no se ha llegado todavía a un consenso internacional en favor de su tipificación.
> Adicionalmente, en 1992, la OCDE elaboró un conjunto de normas para la seguridad de los sistemas de información, con intención de ofrecer las bases para que los Estados y el sector privado pudieran erigir un marco de seguridad para los sistemas informáticos el mismo año…

Por otra parte, en el ámbito de organizaciones intergubernamentales de carácter universal, debe destacarse que en el seno de la Organización de las Naciones Unidas (ONU), en el marco del Octavo Congreso sobre Prevención del Delito y Justicia Penal, celebrado en 1990 en la Habana, Cuba, se dijo que la delincuencia relacionada con la informática era consecuencia del mayor empleo del proceso de datos en las economías y burocracias de los distintos países y que por ello se había difundido la comisión de actos delictivos.

Además, la injerencia transnacional en los sistemas de proceso de datos de otros países, había traído la atención de todo el mundo. Por tal motivo, si bien el problema principal hasta ese entonces era la reproducción y la difusión no autorizada de programas informáticos y el uso indebido de los cajeros automáticos, no se habían difundido otras formas de delitos informáticos, por lo que era necesario adoptar medidas preventivas para evitar su aumento.

En general, se supuso que habría un gran número de casos de delitos informáticos no registrados.

Por todo ello, en vista de que, los delitos informáticos eran un fenómeno nuevo, y debido a la ausencia de medidas que pudieran contrarrestarlos, se consideró que el uso deshonesto de las computadoras podría tener consecuencias desastrosas. A este respecto, el Congreso recomendó que se establecieran normas y directrices sobre la seguridad de las computadoras, a fin de ayudar a la comunidad internacional a hacer frente a estas formas de delincuencia.

Partiendo del estudio comparativo de las medidas que se han adoptado a escala internacional para atender esta problemática, deben señalarse los problemas que enfrenta la cooperación internacional en la esfera de los delitos informáticos y el derecho penal, a saber: la falta de consenso sobre lo que son los delitos informáticos, falta de definición jurídica de la conducta delictiva, falta de conocimientos técnicos por parte de quienes hacen cumplir la ley, dificultades de carácter procesal, falta de armonización para investigaciones nacionales de delitos informáticos. Adicionalmente, la ausencia de la equiparación de estos delitos en los tratados internacionales de extradición…

Al respecto se debe considerar lo que dice el Manual de la Naciones Unidas para la Prevención y Control de Delitos Informáticos el cual señala que, cuando el problema se eleva a la escena internacional, se magnifican los inconvenientes y las insuficiencias, por cuanto los delitos informáticos constituyen una nueva forma de crimen transnacional y su combate requiere de una eficaz cooperación internacional concertada. Asimismo, la ONU resume… los problemas que rodean a la cooperación internacional en el área de los delitos informáticos:

-Falta de acuerdos globales acerca de que tipo de conductas deben constituir delitos informáticos.

-Ausencia de acuerdos globales en la definición legal de dichas conductas delictivas.

-Falta de especialización de las policías, fiscales y otros funcionarios judiciales en el campo de los delitos informáticos.

-No armonización entre las diferentes leyes procesales nacionales acerca de la investigación de los delitos informáticos.

-Carácter transnacional de muchos delitos cometidos mediante el uso de computadoras.

> -Ausencia de tratados de extradición, de acuerdos de ayuda mutuos y de mecanismos sincronizados que permitan la puesta en vigor de la cooperación internacional…
> la Asociación Internacional de Derecho Penal durante un coloquio celebrado en Wurzburgo en 1992, adoptó diversas recomendaciones respecto a los delitos informáticos. Estas recomendaciones contemplaban que en la medida en que el derecho penal tradicional no sea suficiente, deberá promoverse la modificación de la definición de los delitos existentes o la creación de otros nuevos, si no basta con la adopción de otras medidas (principio de subsidiaridad). Además, las nuevas disposiciones deberán ser precisas, claras y con la finalidad de evitar una excesiva tipificación deberá tenerse en cuenta hasta qué punto el derecho penal se extiende a esferas afines con un criterio importante para ello, como es el de limitar la responsabilidad penal con objeto de que éstos queden circunscritos primordialmente a los actos deliberados.[14]

El derecho internacional y en este caso lo referente a lo penal, ha quedado lejano a tipos penales y sanciones correspondientes, por ejemplo, en casos emblemáticos por crímenes contra la humanidad como los juicios de *Nuremberg* que muestran las consecuencias desde la prevención, falta de legislación e incumplimiento de la ley ¿por qué decir esto? Porque si temas tan delicados en donde por omisión y comisión del delito fueron torturadas y asesinadas miles de personas, nos lleva a cuestionarnos qué tanta importancia se le puede dar a situaciones como los delitos *cibernéticos*, que aún en la población la falta de información empeora el poder defenderse ante algo que ni siquiera se emite su nombre.

Es claro el adelanto y la intención en discurso, pero en la realidad se sigue en espera histórica por hacer justicia a todos los delitos en donde poco o nada se ha erradicado en el día a día. Efectivamente la presión, claridad y tipificación puede ayudar a que en realidad exista interés y los delitos de índole penal se persigan eficazmente.

Podemos entender una realidad distinta en cada parte del país, donde aún ni siquiera se logra empatizar con minorías, por ejemplo, las comunidades indígenas, pero al mismo tiempo el crecimiento de la urbe los olvida sin exigir mejora para ellos porque aún no se les contempla.

[14]Santiago Acurio del Pino, *Delitos Informáticos: Generalidades*, Profesor de Derecho Informático de la PUCE, 2024, pp.30-33, de: https://www.oas.org/juridico/spanish/cyb_ecu_delitos_inform.pdf

1.2. TIPOS DE VIOLENCIA DIGITAL O CIBERVIOLENCIA.

La violencia digital en México y otros países (Irak, Irán, Israel, Afganistán) ha sido justificada por *los usos y costumbres o tradición* que hoy en día siguen existiendo lapidaciones en actos públicos, mujeres que no pueden salir de casa sin un hombre que las acompañe, matrimonios arreglados o en México (infantiles) y una cultura tan machista que sigue juzgando el papel de la mujer (como creer que se necesita se sigan los denominados piropos) aparentemente diferente al otro lado del continente, pero se señala a aquella que sólo trabaja y decidió no tener hijos y optar por una forma de vida diferente, incluso que se le cuestiona y hostiga desde la misma familia si rompe con *tabús* o el deber ser y su rol dentro de la sociedad o trabajo.

El mal uso de la tecnología puede terminar con la vida de las empresas y las personas, pero no existe real conciencia en que lo que sucede en redes se está viviendo y traspasando en la vida real, en el día a día y en que lo que está en la *web* no sólo se queda ahí, incluso cualquier cosa que suceda internet siempre *tendrá memoria*, porque no estamos hablando de tiempos donde se olvidar o perder como cuando solo se trataba de algo escrito en un lugar y después al perderse dejar de existir, se trata de la memoria también imborrable y lo perjudicial es que las consecuencias serán a lo largo del tiempo, desde el presente y futuro.

¿Cómo hablar de evolución al parejo del crecimiento de lo digital si ni siquiera ha terminado el machismo y peor aún muchas mujeres muestran ya matices de esto? La tecnología ha avanzado y con ello los delitos que pasan de lo físico a lo digital, y es por ello que hablar de violencia debe ser prioridad en la legislación y leyes donde en primer lugar se contemple la gravedad mental que lleva consigo la violencia. Un avance fue:

> CONTRA LA INTIMIDAD (LEY OLIMPIA) Comete el delito de violación a la intimidad sexual, aquella persona que divulgue, comparta, distribuya o publique imágenes, videos o audios de contenido íntimo sexual de una persona que tenga la mayoría de edad, sin su consentimiento, su aprobación o su autorización. Así como quien video grabé, audio grabe, fotografíe, imprima o elabore, imágenes, audios o videos con contenido íntimo sexual de una persona sin su consentimiento, sin su aprobación, o sin su autorización…

> SEXTORSION Consiste en chantajear o extorsionar bajo amenaza de publicar o enviar imágenes en las que el protagonista muestra una actitud erótica, el chantaje consiste en solicitarle a la víctima fotografías o videos de carácter erótico y en casos extremos un contacto físico sexual.[15]

Los medios de comunicación han normalizado la publicación de cualquier forma de violencia, así como su reproducción, la línea de *informar* y cometer un delito al invadir imágenes, incluso de carácter sexual o de feminicidio como si fuera dar cualquier noticia del clima o hecho que no sea la vida y la afectación a la víctima y su entorno.

Los delitos informáticos han evolucionado al grado en que una persona crea un perfil, *hackea*, humilla, insulta o roba identidad de otra persona, cometer robo, fraude, falsificación, estafas sin repercusiones porque no se cuenta con presupuesto, interés ni legislación al respecto.

Abordar un tema como delito *cibernético* es difícil en México porque existe tanta educación, cultura, empatía; que es la mayoría que no cuenta con internet o dispositivos electrónicos como, por ejemplo, en muchas comunidades lejos de la Ciudad de México donde existen muchas realidades coexistiendo y que posiblemente se tarden años para unificación del país entre quienes si tienen y no cuentan con acceso a la tecnología en el buen uso, la *ciberdelincuencia* cuenta con los recursos y poder factico para continuar operando cuando en México muchos ni siquiera conocen *códigos QR*.

> Hoy en día, el mundo está más conectado digitalmente que nunca. Los delincuentes se están aprovechando de esta transformación en línea para atacar, a través de sus puntos débiles, las redes, infraestructuras y sistemas informáticos. Esto tiene una enorme repercusión económica y social en todo el mundo, tanto para los gobiernos, como para las empresas o los particulares.
>
> El phishing, el ransomware y las violaciones de la seguridad de los datos son solo algunos ejemplos de las actuales ciberamenazas, eso sin contar que continuamente están surgiendo nuevos tipos de ciberdelitos. Los ciberdelincuentes son cada vez más ágiles y están mejor organizados, como demuestra la velocidad con que

[15]Fiscalía General de Justicia Ciudad de México, Unidad de Inteligencia Cibernética, Policía de Investigación de la Ciudad de México, *Glosario de Delitos Cibernéticos,* 2024.

> explotan las nuevas tecnologías, y el modo en que adaptan sus ataques y cooperan entre sí de forma novedosa.[16]

El daño de por vida se da porque los delitos *cibernéticos* no se quedan únicamente en lo digital, sino traspasan la esfera a lo personal con secuelas psicológicas, laborales, reputación y nombre de la persona, como su vida privada e íntima. Lo anterior, desencadenando estrés, ansiedad y demás problemas que pueden poner en riesgo la vida de la persona o en robo de datos bancarios estar de por medio el patrimonio.

Incluso se pueden dar delitos como pornografía infantil, sabotajes *cibernéticos*, invasión a la privacidad, fraude y difícilmente combatidas por parte de las autoridades competentes, lo cual no resulta ajeno si en casos como feminicidio ni siquiera de toman medidas pertinentes para prevenir, combatir y erradicar.

La violencia digital o *ciberviolencia* es una conducta que se realiza mediante medios electrónicos atacando la privacidad sexual, integridad, psique, economía y moral de las personas.

Incluir al lenguaje *ciberviolencia, ciberdelincuencia* y la tipicidad a las mismas acciones, contribuyen al cambio y conciencia para un mundo donde los delincuentes han abusado de la tecnología para robar, difamar, hostigar y cometer actos que en una contingencia como la del COVID-19 y el mundo estaba en *shock* y la información era vital (incluso en ese tiempo la desinformación para crear pánico sobre el virus, cómo surgió y repercusiones) que se utilizó también con otros fines como estafas, pánico y desinformación.

[16]International Pólice (policía internacional INTERPOL, Ciberdelincuencia, *La ciberdelincuencia traspasa fronteras y evoluciona a gran velocidad*, 2024.

Tenemos:

-Delitos *cibernéticos* como estafas informáticas (engañar para obtener un lucro de determinada persona y adquirir patrimonio).

-Delitos informáticos de daños (como lo son los virus informáticos para borrar, dañar, cambiar o alterar y causar un daño a una persona).

-Delitos *cibernéticos* en las telecomunicaciones (por ejemplo, quienes se roban el internet de un vecino o un establecimiento).

-Delitos informáticos contra la intimidad (mediante la tecnología acceder a contenido privado de una persona).

Hablar de violencia es símbolo de evolución a la par de la tecnología en donde es común hacer uso de herramientas *cibernéticas* tanto para pedir y recibir comida (el uso de una *app*) como para buscar y realizar algún trabajo o la comunicación en tiempo real con cualquier persona, incluso en el caso de padres de familia que trabajan y pueden comunicarse con hijos en *tiempo real*.

> La concepción de los delitos informáticos en nuestro país tendrá escasos diez años; sin embargo, en los Estados Unidos de Norteamérica, la primera propuesta de legislar con este respecto, se presentó en 1977 por el senador Ribicoff en el Congreso Federal.
>
> Años después, en 1983 en París, la oecd designó un comité de expertos para discutir el crimen relacionado con las computadoras y la necesidad de cambios en los códigos penales. El dictamen de esta organización, recomendó a los países miembros la modificación de su legislación penal, de forma que se integraran los nuevos delitos informáticos…
>
> También se llegó a discutir sobre estos temas en el Décimo Tercer Congreso Internacional de la Academia de Derecho Comparado de Montreal en 1990, en el Octavo Congreso Criminal de las Naciones Unidas celebrado en el mismo año, y en la Conferencia de Wurzburgo, en Alemania, en 1992.
>
> En 1996, se estableció por el Comité Europeo para los Problemas de la Delincuencia, un nuevo comité de expertos para que abordaran el tema de los delitos informáticos.
>
> Con el fin de combatir los delitos informáticos, sobre todo los cometidos a través de las redes de telecomunicaciones, en Internet, como pueden ser las transacciones de fondos ilegales, la oferta de servicios ilegales, la violación de los derechos de autor, así como también los delitos que violan la dignidad humana y la protección de los menores, se encargó la tarea de elaborar un borrador del instrumento legal obligatorio al recién formado “Comité Especial de Expertos sobre Delitos relacionados con el empleo de Computadoras”.
>
> El veintitrés de noviembre de dos mil uno, el Consejo de Ministros de Europa, compuesto por los ministros del interior de los estados que conforman la Unión

Europea, conjuntamente con Estados Unidos, Sudáfrica, Canadá y Japón, firmaron en Budapest, la convención sobre delitos informáticos, cuyos objetivos fundamentales fueron los siguientes:

1. Armonizar las leyes penales sustantivas aplicables a las conductas delictivas que tienen como escenario el entorno informático.
2. Proveer reglas de procedimiento penal que brinden a las autoridades nacionales competentes las facultades necesarias para la investigación y persecución de tales conductas delictivas, y
3. Establecer un régimen dinámico y efectivo de cooperación internacional.

En nuestro sistema jurídico se incluyó a los delitos informáticos justamente con las reformas que se publicaron en el Diario Oficial de la Federación el diecisiete de mayo de mil novecientos noventa y nueve.

Los novedosos ilícitos se ubicaron dentro de Título Noveno del código punitivo federal, al que se denominó "Revelación de Secretos y Acceso Ilícito a Sistemas y Equipos de Informática".

Resulta de interés al desarrollo de estas líneas las causas medulares que dieron origen a la exposición de motivos de la reforma, al considerarse que la iniciativa propone adicionar un capítulo al código penal para sancionar al que sin autorización acceda a sistemas y equipos informáticos protegidos por algún mecanismo de seguridad, con el propósito de conocer, copiar, modificar o provocar la pérdida de información que contenga, por lo que se pretende tutelar la privacidad y la integridad de la información.

Lo anterior refleja que para el legislador fue de suma importancia proteger el acceso no autorizado a computadoras o sistemas electrónicos, la destrucción o alteración de información, el sabotaje por computadora, la intercepción de correo electrónico, el fraude electrónico y la transferencia ilícita de fondos, ilícitos que no son privativos de nuestro entorno, sino que suceden con frecuencia en el ámbito internacional y que constituyen…un grave problema ante la revolución tecnológica que ha rebasado las estructuras de contención, control y vigilancia por parte de los Estados.

En un sentido similar, se conduce Erika Tinajeros Arce al señalar que el uso de las técnicas informáticas, ha creado nuevas posibilidades del uso indebido de las computadoras, lo que ha propiciado a su vez la necesidad de regulación por parte del Derecho. Añade que el sabotaje informático es el acto mediante el cual se logra inutilizar, destruir, alterar o suprimir datos, programas e información computarizada, sus inicios se dieron en los laboratorios del Instituto de Massachussets en 1960, al crearse un dispositivo informático destructivo mediante la utilización del lenguaje assambler.

El diverso delito de revelación de secretos que establece el artículo 211 del enunciado Código Penal Federal, prevé sanción de uno a cinco años, cuando la revelación punible sea hecha por persona que presta servicios profesionales o técnicos o por funcionario o empleado público, o cuando el secreto revelado o publicado sea de carácter industrial, el subsecuente numerario 211 Bis, de dicho ordenamiento legal, dispone que a quien revele, divulgue o utilice indebidamente o en perjuicio de otro, información o imágenes obtenidas en una intervención de comunicación privada, se le aplicarán sanciones de seis a doce años de prisión.

Tales ilícitos también pueden considerarse como un fin en tratándose del uso de computadoras, sobre todo cuando se trata de información de tipo industrial, en relación con el ordinal 211 Bis, de la ley del enjuiciamiento penal federal, la Primera

> Sala del más alto Tribunal de Justicia de la Nación, ha establecido de que el vocablo "indebidamente" empleado en dicho precepto legal, no provoca confusión; en primer lugar, porque es posible precisar su significado a través de su concepto gramatical y, el segundo, porque su sentido puede fijarse desde el punto de vista jurídico y determinar cuando la conducta es indebida para considerarse delictuosa. Además, el hecho de que el Código Penal Federal no contenga un anunciado especial que desentrañe el significado de ese elemento normativo, lo cual se entiende por constituir un elemento de valoración jurídica, no implica infracción a la citada garantía, pues, se trata de un concepto cuyo contenido resulta claro tanto en el lenguaje común como en el jurídico.[17]

Es también esta manera tan común del uso de redes sociales donde la violencia ha llegado y pareciera *invisible* ante relaciones (laborales, sentimentales o para cometer delitos) sus efectos en víctimas reales podían ser demasiado exagerado creer que se cometan delitos cuando no se está *cara a cara* con el agresor, sin embargo; la violencia digital no sólo ha sido minimizada por la sociedad, sino por las autoridades y la misma ley, sin entender que el daño más grave es de por vida (la *psique*) afectación a la honra, honor y buen nombre, que de ello puede depender un trabajo o el acoso de los mismos cercanos por historias falsas, como si estuviéramos en tiempos de la *Santa Inquisición* donde era decir cualquier cosa, juzgar, señalar sin prueba alguna, difamar y encarcelar a una persona inocente.

El cometer una acción dolosa no es exclusivo de la presencia física, sino con repercusiones en la vida cotidiana de la persona que pueden ser desde psicológicas, financieras (fraudes/patrimonio) trabajo y la misma vida de la persona por amenazas, intimidación, filtración de material comprometedor o imágenes que no son reales como *photoshop*.

Las nuevas generaciones tan familiarizadas con la tecnología y tan poco con el buen uso de las mismas, han puesto *de moda* el hacer ver al estudio, dedicación, esfuerzo y trabajo como *irrelevante e inútil* porque el pago mediante redes sociales o ser *influencer* resultan mejores en cuanto a lo que se genera económicamente en años de estudio y trabajo.

[17]Jorge Esteban Cassou Ruiz, *Delitos informáticos en México*, 2024, pp.226-228.

Lo anterior, también tiene que ver con falta de regulación que termina siendo un mensaje en que es más fácil obtener dinero de otras formas que no tienen que ver con educación y en menos tiempo.

Tan de moda son las redes sociales, que incitar a enfermedades por aparentemente creer verse bien como *bulimia* y *anorexia*, para cumplir con estereotipos que cualquier persona sin conocimientos dice (ni sentido común por el deterioro de la salud) en nutrición da dietas milagrosas u opinión de cualquier situación sin experiencia ni fuentes que realmente avalen ello como lo es la ciencia.

La despersonalización entre familia o la forma en como se ha desarrollado la tecnología, minimiza que la *ciberviolencia* está más presente. El *bullying cibernético* y los delitos de este tipo suceden a raíz del crecimiento de la tecnología sin que la legislación de la misma estuviera de por medio. Aparentes bromas en redes sociales para burlarse y *normalizar* falta de ética y empatía para percibir en qué momento se vuelve acoso situaciones que no porque se lleven realizando de otras generaciones significa que eran correctas, incluso que la ley mucho tiempo ha preferido evitar.

De acuerdo con la Ley de Acceso de las Mujeres a una Vida libre de Violencia de la Ciudad de México, en sus artículos:

> Artículo 20 Quáter.- Violencia digital es toda acción dolosa realizada mediante el uso de tecnologías de la información y la comunicación, por la que se exponga, distribuya, difunda, exhiba, transmita, comercialice, oferte, intercambie o comparta imágenes, audios o videos reales o simulados de contenido íntimo sexual de una persona sin su consentimiento, sin su aprobación o sin su autorización y que le cause daño psicológico, emocional, en cualquier ámbito de su vida privada o en su imagen propia.
> Así como aquellos actos dolosos que causen daño a la intimidad, privacidad y/o dignidad de las mujeres, que se cometan por medio de las tecnologías de la información y la comunicación.
> Artículo 7.-IX. Violencia digital.- Es cualquier acto realizado mediante el uso de materiales impresos, correo electrónico, mensajes telefónicos, redes sociales, plataformas de internet, correo electrónico, o cualquier medio tecnológico, por el que se obtenga, exponga, distribuya, difunda, exhiba, reproduzca, transmita, comercialice, oferte, intercambie y comparta imágenes, audios o videos reales o simulados de contenido sexual íntimo de una persona, sin su consentimiento; que atente contra la integridad, la dignidad, la intimidad, la libertad, la vida privada de

> las mujeres o cause daño psicológico, económico o sexual tanto en el ámbito privado como en el público, además de daño moral, tanto a ellas como a sus familias.
> Se manifiesta en presión, persecución, hostigamiento, acoso, coacción, vejación, discriminación, amenazas o privación de la libertad o de la vida en razón del género.[18]

Los derechos de la víctima no sólo están afectados por la falta de regulación y protección de la ley, sino por el nulo interés de legisladores y por no priorizar en la salud mental como tema principal a todas las edades en cuanto a hospitales y medicamentos con gratuidad, porque aún existiendo penas para agresores que tal vez nunca se cumplan no existe reparación a víctimas, tanto en su patrimonio, vida, libertad y salud mental si es importante no dejar de lado que se necesita priorizar en que la reparación y prevención vaya de la mano de salud mental.

Es importante el dato brindado por el INEGI respecto al Módulo sobre Ciberacoso (MOCIBA) porque se pueden tener estadísticas más precisas en cuanto a que sector, rango de edad o población son más susceptibles al uso de internet, lo cual al poner atención en ello la restricción y combate por parte de autoridades competentes daría mayor eficacia al ataque de estas.

De igual forma, es importante porque la recopilación de datos como identidad, sexo e impacto en la víctima, edad y nivel escolar arrojan información para mejora en el ataque a estos delitos. Tener en cuenta que es alarmante cifras de *ciberacoso* en 2022 en 20.8% porque se traduce a 17.4 millones que han sido afectadas y no solamente se quedan en supuestos de posibles víctimas, sino en reales.

Sumado a ello, la falta de comprensión por parte de la sociedad por no dimensionar el daño y efectos que los delitos de carácter *virtual y violencia digital* tienen de por vida en la(s) persona(s).

[18]Ley General de Acceso de las Mujeres a una Vida Libre de Violencia, Ley de Acceso de las Mujeres a una Vida Libre de Violencia de la Ciudad de México, Capítulo IV TER, De la violencia digital y mediática, 2024.

Los violentadores y maltratadores cobardemente se refugian detrás de un dispositivo electrónico (computadora, celular, *tablet*) para hacer que sus acciones queden impunes en una sociedad machista (tanto por el pensamiento como por la acción de hombres como de las mismas mujeres) que pareciera que *no es tan grave* y minimizado a no ser tomado como algo importante y realmente grave.

La forma machista incluso de los juzgadores de justicia es perceptible en muchos casos, esto también es visible en centros de reclusión donde incluso la familia actúa de forma diferente, si se trata de hombre o mujer quien se encuentra privado de su libertad *los privilegios al ser visitado marcan una brecha abismal*, lo cual nos da un panorama de cómo la sociedad aparentemente avanza, sobre todo en teoría y discurso, lo cual es lamentable que la tecnología nos está rebasando de tal forma que podríamos imaginar un futuro donde en los museos se exhiban cerebros humanos y quienes acuden a ver son robots y máquinas.

> En México… se han identificado cuatro factores que propician estas acciones:
> 1) El aumento del número de personas que estudian computación.
> 2) El aumento del número de empleados con acceso a los equipos.
> 3) La facilidad de uso de los equipos de cómputo.
> 4)El incremento en la concentración del número de aplicaciones y consecuentemente de la información. Por otra parte, según un estudio del Instituto Mexicano de Auditores Internos las causas que propician los fraudes se debe a la combinación de dos factores: el primero debido a las fallas o inexistencia de elementos de control, y el segundo, por las características propias del personal que se encuentran en situaciones inconvenientes tales como:
> 1) Antecedentes de deshonestidad.
> 2) Problemas económicos ocasionados por endeudamiento, ingresos insuficientes, nivel de vida insatisfactorio, etc.
> 3) Estados de ánimo… como resultado de una molestia ó frustración.
> 4) Rotación excesiva.
> 5) Falta de goce de vacaciones.
> 6) Personal "indispensable" para la exclusividad en el manejo de ciertos sistemas y transacciones. De aquí que la probabilidad de que las compañías puedan ser afectadas, radica en los siguientes factores:
> 1) La deshonestidad del posible perpetrador.
> 2) La oportunidad que la compañía ofrece por poseer controles inadecuados.
> 3) La motivación oculta de los posibles perpetradores para cometer el fraude. Los estudios realizados indican… los motivos de… estas acciones, son, entre otros:
> 1) Beneficio personal (lucro).
> 2) Beneficios para la organización.
> 3) Beneficio a otra persona o institución.

4) Rechazo a la organización.
5) Problemas financieros.
6) Deseo de sobresalir en alguna forma. Con base en lo anterior, se considera particularmente que los motivos de los empleados deshonestos y la falta de seguridad adecuada son las causas principales para la comisión de estos delitos. A continuación, se describen los sujetos del delito, como personas físicas o morales que intervienen o que se ven afectadas:
a) El sujeto activo, usualmente identificado en los operadores, que pueden modificar, agregar, eliminar o sustituir información o programas, copiar archivos para venderlos a competidores; los programadores, que pueden violar o inutilizar controles protectores del programa, dar información a terceros ajenos a la empresa, modificar archivos, acceder a información confidencial; los analistas de sistemas, que comúnmente son los únicos que conocen la operación de un sistema completo y pueden estar en colusión con los programadores u operadores; así como cualquier personal involucrado con los sistemas como el personal técnico y de servicio, los funcionarios, los bibliotecarios, hasta cualquier persona que tenga acceso a documentos o listados dejados sobre los escritorios que pueda ser vendida a competidores. Una lista publicada en los E.U.A., menciona que de 674 "criminales bancarios", recientemente detectados, 120 eran promotores de datos, 32 vicepresidentes y gerentes de operaciones, 29 funcionarios de préstamos y 14 presidentes de bancos. Desgraciadamente en México no se disponen de muchas estadísiticas sobre estos actos ya que la mayoría no se llevan a juicio ni se divulgan. Sin embargo, con lo expuesto anteriormente, se puede concluír que pueden ser cometidos por personas de cualquier nivel que tengan acceso a los sistemas.
b) Los sujetos Pasivos, generalmente instituciones financieras o comerciales, y en menor medida sector público o gubernamental, en la mayoría de las ocasiones carentes de sistemas de seguridad adecuados, evidenciando que el crecimiento de los fraudes por computadora es mayor que áquel que se presenta en los sistemas de seguridad, agudizado por la escasa denuncia de irregularidades de este tipo de pérdidas, por temor a sufrir daños en la imagen corporativa, o a una posible pérdida de competitividad, clientela o confianza por parte de los mismos accionistas.[19]

Las Instituciones financieras son quienes han mostrado mayor interés para prevención y castigo hacía quienes cometen delitos, donde la tecnología pareciera no favorecer a la población porque si bien ha sido una herramienta para acceder fácilmente y poder realizar una transacción o en el caso de los migrantes llegue y se envíe dinero, también pareciera que sólo cuando se les afecta a estas Instituciones se voltea a ver el delito como el fraude, usurpación de identidad, robo se buscan algún mecanismo, pero no en el caso de personas que ven afectadas sus cuentas no existen mecanismos inmediatos para resolver y devolver el dinero a la(s) víctima(s).

[19]Julio Téllez Valdés, *Los "Delitos Informáticos": Situación en México*, pp.462-464.f, 2024.

En ocasiones el temor de las personas ha generado que se sientan más seguros (as) *guardar* su dinero en su casa que el respaldo al guardarlo en el banco porque ante cualquier situación como en otros delitos, la burocracia e impunidad permea ante la víctima y la solución no es inmediata.

De acuerdo con datos del INEGI:

> Del 13 de junio al 5 de agosto de 2022 se levantó el Módulo sobre Ciberacoso (MOCIBA), 2022. Su objetivo es generar información estadística para conocer la prevalencia de ciberacoso entre las personas de 12 años y más que usan internet en cualquier dispositivo. También se busca identificar el tipo y la caracterización del ciberacoso. El MOCIBA 2022 presenta resultados de la prevalencia de ciberacoso en los 12 meses previos a su levantamiento y caracteriza las diferentes situaciones declaradas. Asimismo, busca establecer la identidad y sexo de la persona que lo cometió, la intensidad y el impacto que causó en la víctima. Además, incluye el rango de edad y nivel de escolaridad de la población que se declaró víctima de ciberacoso, las acciones que se tomaron contra este y las medidas de seguridad que realizó la población usuaria de internet para proteger su información y equipos. PRINCIPALES RESULTADOS En México, la Encuesta Nacional sobre Disponibilidad y Uso de las Tecnologías de la Información en los Hogares (ENDUTIH) 2022 estimó que la población de 12 años y más fue de 105.8 millones de personas. De ese total, entre marzo y agosto de 2022, 79.5 % utilizó internet en cualquier dispositivo, lo que representa 84.1 millones de personas: 44.0 correspondió a mujeres y 40.1 millones, a hombres…
> Población que experimentó ciberacoso En 2022, 20.8 % de la población usuaria de internet vivió alguna situación de acoso cibernético, lo cual representa un total de 17.4 millones de personas de 12 años y más. De estas, 9.8 millones fueron mujeres (22.4 %) y 7.6 millones, hombres.[20]

La modernidad en vivir mediante apariencias en redes sociales y el *oversharing*[21] han despersonalizado al ser humano y su convivencia en sociedad, porque resulta más *importante* exponer toda la vida (que muchas veces puede ser ficticia o superficial como para tener seguidores) en redes sociales o tratar de aparentar algo que no es a vivir con tranquilidad.

[20]Instituto Nacional de Estadística, Geografía e Informática (INEGI), comunicado de prensa núm. 404/23 13 de julio de 2023 página 1/21, comunicación social módulo sobre ciberacoso 2022, pp.1,3, de: https://www.inegi.org.mx/contenidos/saladeprensa/boletines/2023/MOCIBA/MOCIBA2022.pdf
[21]Término que se refiere a la sobreexposición en redes sociales, compartir en exceso.

La vida dio un giro drástico a raíz de las redes, que poco a poco dejó de ser importante la convivencia que una nueva era de personas que viven su vida a través de la tecnología (muchas veces mentira) lo cual también habla del estrés por aparentar ser algo que sin importante los daños o consecuencias, tanto para la persona como el mensaje como sociedad y cambios en la misma composición del cuerpo humano por la exposición a los dispositivos electrónicos.

Situaciones que se han dado en redes como fraudes mostrando una vida que no es para engañar, defraudar o fomentar trastornos alimenticios como enfermedades y trastornos alimenticios bulimia, anorexia o actos atroces como la pedofilia y trata de personas que resuelta sumamente redituable vender muchas veces el cuerpo y realizar trabajo esclavo (que les es más fácil por medio de los denominados *avatars* que podríamos asemejar a *robots* de nuestra propia persona) incluso con víctimas mayores de edad que buscaban trabajo, fueron engañados y captados por el crimen organizado o en búsqueda de pareja de igual forma estafados(as) en plataformas digitales aparentemente que muestran la modernidad en que hemos *evolucionado* y han crecido las redes sociales.

Las solicitudes de *supuestos empleos* que se ofertan en internet y al llegar a los lugares de entrevistas o que los citan para el empleo pueden ser extorsionados o secuestrados por el organizaciones criminales o personas sin escrúpulos, como si habláramos de que en búsqueda por mejor vida y oportunidades para salir adelante, así como de sus familias puede ser su propia *tumba* y desaparecer en una nueva trata de personas en diferentes modalidades y con fines de explotación.

> La evolución de las tecnologías de la información y la comunicación y la extensión de su uso a través de los servicios y aplicaciones de Internet, como redes sociales, mensajería instantánea o correo electrónico en dispositivos inteligentes, ha llevado a que se utilicen no sólo como un cauce habitual de comisión de infracciones en materia de protección de datos, sino también para cometer hechos tipificados como delitos. Expresiones como ciberacoso, ciberbullying, sexting, grooming, phising, pharming o carding, que nos van resultando cada vez más familiares, son

términos en inglés que identifican situaciones de acoso, amenazas, coacciones, revelación de secretos, delitos sexuales, violencia de género o estafas[22]

La evolución incluso en el mismo lenguaje y contar con definiciones de los delitos *cibernéticos* implica avance porque si bien aunque las que se están dando actualmente son en inglés y no en la denominación del delito en latín o español, esto muestra avance y también que las situaciones no son exclusivas de un país, son delitos que se han dado en otros países y afortunadamente gracias a la conciencia y avance en la necesidad de regulación que viene de fuera, obliga a que todos de acuerdo a Tratados Internacionales suscritos y de cooperación, México se vea obligado a incluirlos en su legislación (aunque en teoría y de forma muy lenta).

La despersonalización de verse a si mismo desde fuera, que tiene que ver con la manera en que se percibe, puede ser grave porque se puede estar aparentemente despierto, pero en una especie de sueño que trae consigo angustia y miedo, lo cual provoca que la persona no tenga una vida tranquila. La ansiedad, depresión y el intento de la mente por bloquear episodios traumáticos o problemas económicos, personales o laborales es un tema de salud mental presente en y las secuelas de los delitos *cibernéticos* que no se toman en cuenta como parte fundamental para el avance en la legislación y reparación de daño.

Actualmente en nuestro país, mencionar el *ciberbullying* ha tenido mayor auge por situaciones que se normalizaron durante mucho tiempo en el sistema escolar y más en localidades de bajos recursos, en donde se disfraza de *broma* el mal actuar en una sociedad machista (que aún esta en debate si debe la mujer o no tener derecho a abortar y que, sobre todo, es un debate en el norte del país) que se mide el ser hombre en que tanto aguanta golpes, insultos o el levantar la voz ante cualquier injusticia se tacha de descalificativos.

[22]Protección Datos y Prevención de delitos, Agencia Española de Protección de Datos, 2024, p.2, de: https://www.aepd.es/guias/guia-proteccion-datos-y-prevencion-de-delitos.pdf

Temas alarmantes de desapariciones, violencia y feminicidios tan presentes en el país (como si fuera común y costumbre) que en lo positivo, gracias a la era *digital* que estamos viviendo también se cuenta con mayor evidencia como en situaciones donde existen grabaciones, cámaras de video o alguien que con su celular cuenta con evidencia es que se utiliza para esclarecer situaciones que no son casos aislados, sino que forman parte de un sistema tan violento que intentaba negar que generalmente las víctimas tenían algún tipo de relación cercana o conocían a los agresores y que no hace falta salir a la calle para ser víctima de un delito, se puede cometer desde el mismo hogar.

Claramente el país necesita crear conciencia en quienes legislan e imparten (deberían) justicia y las consecuencias de estos delitos porque si bien son de carácter *cibernético*, el trasfondo y secuelas son de la vida cotidiana y es ahí donde las autoridades son responsables de erradicar y dar seguridad a la población.

CIBERBULLYING O CIBERACOSO.

Un tema que ha tomado mayor auge como aparentes *bromas* o casos en los que era *normal* en escuelas a todos los niveles, pero mayormente a nivel medio superior o secundarias, incluso con videos como evidencia del delito, existen quienes dejan de estudiar por este delito o han muerto (ya sea por suicidio o por las mismas peleas físicas y golpes).

> *CIBERBULLYING* Es una adaptación de las palabras en inglés *cyber y bullying*; en español lo conocemos como ciber abuso o violencia entre iguales. Es un término que se utiliza para describir cuando un niño o adolescente es molestado, amenazado, acosado, humillado, avergonzado o abusado por otro niño o adolescente, a través de Internet o cualquier medio de comunicación como teléfonos móviles o *tablets*. Se caracteriza por que el acoso se da entre dos iguales, en este caso, menores. El *ciberbullying* se presenta de distintas formas: insultos, discriminación o burla sobre características físicas, forma de vestir, gustos, hacer pública información o fotografías que avergüenzan a la víctima, robo de identidad y suplantación, hasta amenazas de daño físico y otros cargos que pueden ser tipificados como delincuencia juvenil. [23]

[23]Fiscalía General de Justicia Ciudad de México, Unidad de Inteligencia Cibernética, Policía de Investigación de la Ciudad de México, Glosario de Delitos Cibernéticos, *op.cit.*

Enseñar, educar e inculcar valores corresponde a los padres porque son ellos quienes eligieron tener y por lo tanto su obligación es formar a este menor, porque culpar al sistema, falta de oportunidades, analfabetización y poca cultura es muy fácil para no hacerse responsable con conciencia que la solución no es por fuera.

Todos en algún momento hemos pasado por etapas donde nos hemos enfrentado a situaciones como amenazas (de distinta índole) pero es el entorno cercano, autoridades competentes y la sociedad en general quienes deben proteger de cualquier indicio de violencia como se ha viralizado en casos donde alguien sigue a una persona (generalmente mujer) y se le auxilia ya sea por medio de señas, de pedir ayuda o de situaciones inusuales que se están convirtiendo muy comunes (como en estaciones del metro de la Ciudad de México que se han reportado sentir un piquete y de pronto alguien se la lleva cuando es evidente que no está consciente la víctima).

Lo anterior, porque en un país tan machista, las respuestas próximas a una agresión son: *haz lo mismo o responde*, no existe conciencia sobre el delito y por consecuencia una sanción, lo que también tiene que ver a la falta de acceso a la justicia e impunidad que han vivido quienes intentan recurrir a las leyes. Pero son las leyes, quienes nos hacer vivir y convivir en sociedad (su función) con normas de lo permitido y lo no permitido, por ello la difusión de los delitos *cibernéticos* debe formar parte no sólo del conocimiento de quién ya vivió desafortunadamente una situación, sino desde pequeños abordar estas situaciones y como sociedad apoyar y creer siempre en víctimas reales, exigiendo justicia y defensa a nuestros derechos humanos.

> ¿Qué es el *Cyberbullying*? Se trata de emplear cualquiera de las posibilidades de uso de las nuevas tecnologías de la información y de la comunicación para hostigar con ensañamiento a su víctima. En un análisis reciente realizado por Belsey sobre el fenómeno del Ciberbullying señala que se define como el uso de algunas Tecnologías de la Información y la Comunicación como el correo electrónico, los mensajes del teléfono móvil, la mensajería instantánea, los sitios personales vejatorios y el comportamiento personal en línea difamatorio, de un individuo o un grupo, que deliberadamente, y de forma repetitiva y hostil, pretende dañar otro. Las herramientas disponibles en Internet ayudan a la propagación de ese

comportamiento en el que las víctimas reciben malos tratos de sus iguales, sea a través de ridiculizaciones, amenazas, chantajes, discriminaciones, todo ello de manera anónima, para que este desconozca quien es el agresor.

Consideramos que existen dos modalidades de *Cyberbullying*: aquel que actúa como reforzador de un *bullying* ya emprendido, y aquella forma de acoso entre iguales a través de las *TIC's* sin antecedentes. En la primera modalidad, consideramos al *cyberbullying* como una forma de acoso más sofisticada desarrollada, generalmente, cuando las formas de acoso tradicionales dejan de resultar atractivas o satisfactorias. En este caso el agresor es fácilmente identificable, ya que coincide con el hostigador presencial. Los efectos de este *Cyberbullying* son sumativos a los que ya padece la víctima, pero también amplifican e incrementan los daños, dada la apertura mundial y generalización del acoso a través de las páginas web.

En lo que respecta a la segunda modalidad, son formas de acoso entre iguales que no presentan antecedentes, de modo que sin motivo aparente el niño empieza a recibir formas de hostigamiento a través de las *TIC's*. En ocasiones, después de un tiempo de recibir este tipo de acoso, el *cyberagresor* decide completar su obra con una experiencia presencial, dando la cara.

Este tipo de acoso en red presenta unas características de similitud con otras formas de acoso, como el hecho de ser una conducta violenta o de acoso altamente premeditada e intencionada; que se encuentra fundamentada en una relación asimétrica de control y poder sobre el otro…pero también con unas características particulares que lo diferencian de otras formas de acoso presencial y directo:

• Exige el dominio y uso de las *TIC's*.

• Se trata de una forma de acoso indirecto.

• Es un acto de violencia camuflada, en la que el agresor es un total desconocido, a no ser que haya sido hostigador presencial de la víctima antes o que decida serlo después del *Cyberbullying*.

• El desconocimiento del agresor magnifica el sentimiento de impotencia.

• Recoge diversos tipos o formas de manifestar el acoso a través de las *TIC's*.

• Desamparo legal de estas formas de acoso, ya que aunque se puede cerrar la web, inmediatamente puede abrirse otra.

• El acoso invade ámbitos de privacidad y aparente seguridad como es el hogar familiar, desarrollando el sentimiento de desprotección total.

• El acoso se hace público, se abre a más personas rápidamente. A pesar de que los estudios al respecto son escasos, y que se desconocen empíricamente los efectos derivados de esta forma de acoso tecnologizado, las primeras tentativas al respecto, trasladan los efectos del *bullying* presencial al virtual.[24]

[24]Ma Ángeles Hernández Prados; Solano Fernández, Isabel Ma, *Ciberbullying, un problema de acoso escolar*, RIED. Revista Iberoamericana de Educación a Distancia, vol. 10, núm. 1, 2007, pp. 17-36, Asociación Iberoamericana de Educación Superior a Distancia, Madrid, Organismo Internacional, ISSN: 1138-2783, pp.23-25, 2024, de: https://www.redalyc.org/pdf/3314/331427206002.pdf

Por mucho tiempo, se había tomado con *normalidad* estar en una sociedad donde la burla hacia cualquier aspecto de una persona era parte de la adolescencia o *cosas de niños*, incluso comentarios como *los niños son crueles*, pero este tema va más allá de la niñez o adolescencia afecta a todas las edades y clases sociales (aunque algunos más que a otros) donde los niveles de educación son bajos, además de situaciones que empeoran las condiciones de los estudiantes con burlas o agresiones, pero es darle un nombre, contexto y definición lleva a una sociedad a la evolución y el *ciberbullying* no es sólo la palabra, son las consecuencias en la víctima sin importar la edad porque debe ser tipificado, castigado por parte de autoridades y las leyes es que lo que hará una sociedad con valores al igual que en el desarrollo de la tecnología y que es precisamente el castigo a este delito y bajo las leyes seguir caminando hacia tener una mejoría en ello.

SEXTING.

> (“sexting”: “sex”=sexo, “texting”=envío de mensajes de texto a través de telefonía móvil) pero todas hacen referencia al mismo hecho: enviar fotografías y vídeos con contenido de cierto nivel sexual, tomadas o grabados por el protagonista de los mismos, mediante el teléfono móvil…existe gran variedad de implicaciones jurídicas que conlleva el Sexting, puesto que puede acarrear acciones consideradas ilegales en lo que respecta a los delitos contra la intimidad, libertad sexual y pornografía infantil.
>
> Desde una perspectiva internacional, Europa está haciendo grandes avances en cuanto a la regulación de este fenómeno. Una de las acciones más representativas es el Convenio del Consejo de Europa para la protección de los niños contra la explotación y el abuso sexual, que entra en vigor en España el 1 de diciembre de 2012 regulando dichos actos que se dan en el contexto de las Tecnologías de la Información y Comunicación (TIC). En España aún no se contempla una ley específica para el sexting, pero se está avanzando penalizando delitos relacionados implicados en este fenómeno:
>
> • Responsabilidad penal del menor: cuando el autor del delito es menor de edad, siendo mayor de 14 años, se aplica la Ley Orgánica 5/2000 o Ley del Menor. En la determinación de la pena se establecerán sanciones diferentes que, en función de la gravedad de la conducta, podrán ir desde la amonestación hasta el internamiento, pasando por asistencias a centros de día o prestaciones en beneficio de la comunidad.
>
> • Aumento de la protección del menor: se presenta una reforma en diciembre de 2010 (Ley Orgánica 5/2010, de 22 de junio) por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal. Supone la respuesta a las nuevas formas de criminalidad, dirigida especialmente a las relacionadas con las nuevas tecnologías y explicitando una mayor protección a los menores víctimas de delitos

> sexuales… De hecho, la generación, difusión y posesión de contenidos de carácter sexual podría llegar a considerarse, según el artículo 189 del Código Penal, creación y distribución de pornografía infantil, siempre que los contenidos impliquen a menores en actitudes explícitamente sexuales: "será castigado el que produjere, vendiere, distribuyere, exhibiere, ofreciere o facilitare la producción, venta, difusión o exhibición por cualquier medio de material pornográfico en cuya elaboración hayan sido utilizados menores de edad o incapaces, o lo poseyere para estos fines, aunque el material tuviere su origen en el extranjero o fuere desconocido". Se convierte así el Sexting en una controvertida cuestión jurídica, ya que "los fiscales no están de acuerdo sobre si procesar y cómo hacerlo a los menores y los adultos jóvenes que se involucran en conductas de Sexting primario y secundario". aseguran que "comprender el Sexting desde la perspectiva de los jóvenes es fundamental para el desarrollo de estrategias de prevención de daños potenciales".[25]

El envió de mensajes de texto y conversaciones en redes sociales y/o aplicaciones sin duda han revolucionado la forma de comunicarnos haciendola más rápida, eficiente y eficaz, incluso cuando la señal por llamada podía complicar se realizará fluida, por lo que la tecnología por medio de videollamadas o llamadas por ejemplo en *whats app* mediante teléfonos inteligentes y el envió de mensajes de texto e información ha logrado llegue más rápido y en tiempo real a una o varias personas a la vez (como las cadenas o reenvió de mensajes) como por ejemplo noticias, advertencias de precaución o algún tipo de aviso y de lo cual también la regulación es necesaria por delitos como fraudes ya sea para pedir dinero, estafas de haber ganado un premio o falsos secuestros para lucrar con las personas.

Tenemos por ejemplo el *ciberbuying* que significa el abuso o violencia que generalmente se presenta más en los niños y adolescentes (aunque no es exclusivo) en donde se está amenazado, acosado, humillado y en ocasiones incluso se utilizan dispositivos móviles para grabar dichas agresiones y difundir en la red.

[25]Ma Isabel Fajardo Caldera ; Gordillo Hernández, Marta; Regalado Cuenca, Ana Belén *Sexting: nuevos usos de la tecnología y la sexualidad en adolescentes, International Journal of Developmental and Educational Psychology*, vol. 1, núm. 1, 2013, pp. 521-533 Asociación Nacional de Psicología Evolutiva y Educativa de la Infancia, Adolescencia y Mayores Badajoz, España, International Journal of Developmental and Educational Psychology ISSN: 0214-9877, Asociación Nacional de Psicología Evolutiva y Educativa de la Infancia, Adolescencia y Mayores, pp. 523, 524-525.

Es un acoso entre iguales que puede ser también mediante discriminación, insultar, burlas y amenazas. Lo anterior, utilizando a la tecnología para grabar, fotografiar o difundir, lo cual agrava la agresión porque la víctima es atacada en la red y el pasado siempre es presente por que lo que se sube en la red, se queda en la red por el daño por figuras anónimas.

El *sexting* son los mensajes enviados por medio de dispositivos móviles en cuanto a contenido de índole sexual. Europa es quien ha avanzado mediante el Convenio del Consejo de Europa para la protección de los niños contra la explotación y el abuso sexual haciendo énfasis en que la tecnología está presente en la explotación y el abuso sexual infantil.

Pero ¿qué pasa cuando esta tecnología se ocupa para dañar, perturbar o incriminar a otra persona? Ha sido sumamente importante el uso de estos mensajes que en juicios y audiencias se toman como prueba mediante capturas impresas que se agregan a expedientes y carpetas de investigación como evidencia de conversaciones que no queden únicamente en un intercambio de información, sino en un escrito que es un medio probatorio (donde incluso al tomar captura de pantalla se guardan sin importar que el mensaje haya sido borrado y que es uno de los elementos donde más puede contribuir la policía *cibernética*) pero la falta de interés, recursos y tecnología por parte de las autoridades encargadas de investigar por ejemplo en realizar rastreo de códigos *IP* para ayudar a las víctimas quienes sean víctima de cualquier persona que ocultándose detrás de un medio electrónico abusa de impunidad en un país donde no se otorgan recursos adecuados, personal ni leyes a favor de evitar estos delitos.

STALKED.

> El delito de acoso, también conocido como stalking, es un fenómeno al alza. Estados Unidos fue el primer país en definir y criminalizar esta conducta durante la década de 1990. Tras irse introduciendo en los distintos Estados norteamericanos, la nueva figura de delito fue extendiéndose a otros países anglosajones, llegando finalmente a países de Europa continental, como Alemania o Italia. Actualmente 21 estados miembros de la Unión Europea recogen en sus legislaciones el fenómeno de

> stalking, si bien es cierto que existen diferencias en su definición. En España es en el año 2015, y tras la ratificación del Convenio del Consejo de Europa sobre prevención y lucha contra las mujeres y violencia doméstica, cuando se produce la reforma del Código Penal, que supuso la introducción del artículo 172.ter que define y castiga el acoso. En este artículo se establece lo siguiente: "el que acose a una persona llevando a cabo de forma insistente y reiterada, y sin estar legítimamente autorizado, alguna de las conductas siguientes y, de este modo, altere gravemente el desarrollo de su vida cotidiana: 1.ª La vigile, la persiga o busque su cercanía física, 2.ª Establezca o intente establecer contacto con ella a través de cualquier medio de comunicación, o por medio de terceras personas, 3.ª Mediante el uso indebido de sus datos personales, adquiera productos o mercancías, o contrate servicios, o haga que terceras personas se pongan en contacto con ella, 4.ª Atente contra su libertad o contra su patrimonio, o contra la libertad."[26]

Un delito importante y totalmente negligente para la correcta aplicación de la ley que afecta a las personas víctimas y que sin duda pone sobre la mesa un tema tan difícil de probar y perturbador en la vida de la(s) víctima(s) porque el acoso invade todas las esferas para llevar una vida libre de violencia, afectando tanto a quién la padece como a su entorno, esto porque incluso el acoso físico al no presentar lesiones *visibles* como golpes, las autoridades minimizan y desestiman como si quién la padece exagerara o inventara situaciones, pero ¿cómo concientizar a la sociedad y autoridades (tanto quienes proponen, promulgan, aprueban y ejecutan las leyes) si ni siquiera la violencia doméstica o casos de feminicidio se atienden, investigan y terminan? Y que revictimizan con comentarios en cuanto a la forma de vestir, su vida y forma de ser, poniendo al agresor prácticamente como víctima.

Posiblemente, nos encontramos como país en una realidad que poco o nada cambie ni mejore para las víctimas (las presentes y futuras) porque precisamente en pleno siglo XXI se siguen dando pensamientos contrarios al avance ideológico de respeto por cualquier tipo de vida, todavía existen quienes se atreven a meter recursos (como amparos) para que las corridas de toros se abran, argumentando que se trata de una *arte* (entonces matar, torturar, divertirse con el dolor ajeno y mutilar hay

[26]Análisis jurídico-criminológico del stalking a partir de un estudio de sentencias1 Victoria Fernández-Cruz2 y José R. Agustina Universitat Internacional de Catalunya – Barcelona, International e-Journal of Criminal Sciences Artículo 3, Número 14 (2019), Supported by DMS International Research Centre, ISSN: 1988 7949, pp.2-3, de: file:///C:/Users/javis/Downloads/21275-265-81962-1-10-20191204.pdf

quienes lo denominan *arte*, o que nos da respuesta a porque no avanzamos en cuestión de derechos humanos y el primer derecho que es a la vida dentro de nuestra Constitución Política de los Estados Unidos Mexicanos) entonces podemos creer en el avance si se sigue creyendo e intentando justificar que la violencia forma parte de la vida o tradición.

Referirnos a la pedofilia puede no ser algo nuevo, pero si más público y difundido gracias a las redes sociales y es mediante la presión mediática que las autoridades en algunos casos hacen seguimiento al respecto, porque también en otros casos las redes se utilizan para desinformación.

Hablar de parafilias es remitirnos a fantasías o comportamientos en donde este aparente *deseo* lleva consigo un daño. Pero es importante no perder de vista que la ley siempre debe ser quien proteja a quienes son víctimas y evitar que se den más porque el intentar atribuir un problema mental por el cual el sujeto activo actúa es demeritar el sufrimiento de quien usa la ley para crear impunidad. En una sociedad tan acostumbrada a la violencia, justificar el soportar situaciones por los hijos o seguir en *familia,* aunque sea de esa forma.

GROOMING.

> un acoso ejercido por un adulto y se refiere a las acciones realizadas deliberadame establecer una relación y un control emocional sobre un situaciones de acoso con un contenido sexual explícito o implícito. Simplificando mucho, e un acoso entre iguales, mientras que en el grooming el acosador es un existe una intención sexual.[27]

Actualmente el ejemplo más claro de *grooming* en redes sociales se dio con Florencia Guillot[28] donde tratando de normalizar la vida en pareja por mucho tiempo, presentó de forma irresponsable el caso de Paulina Florencia y su esposo Mauricio Cuevas que es muestra de lo que la manipulación hacia un menor puede hacer

[27]Instituto Nacional de Tecnologías de la Comunicación INTECO, guía legal sobre ciberbullying y grooming, observatorio de la seguridad de la información Área Jurídica de la Seguridad y las TIC, 2024, p.4.
[28]Influencer que trato de normalizar el grooming y abuso a una menor haciéndolo ver como historia de amor y no de delito.

creer para situaciones de índole sexual, lo cual es absurdo porque entonces en países como Medio Oriente que escandalizan al mundo con temas de matrimonios entre mayores con menores de edad o la violencia hacia las mujeres, incluso desde la coerción para la forma de vestirse o cómo deben estar ciertas actividades destinadas para ellas, podríamos llevarnos a preguntar si el *grooming* es esa pedofilia y violencia que se señala en otros países y en *culturas avanzadas o civilizadas* aún tiene un toque imperceptible que es lo mismo que se señala en otro, pero aparentando que depende del país si debe o no haber ley y justicia porque:

> *GROOMING* Es la acción deliberada de un adulto, varón o mujer, de acosar sexualmente a una niña, niño o adolescente a través de un medio digital que permita la interacción entre dos o más personas, como por ejemplo redes sociales, correo electrónico, mensajes de texto, sitios de chat o juegos en línea. Los adultos que realizan grooming suelen generar uno o varios perfiles falsos, haciéndose pasar por un niño, niña o adolescente, buscando generar una relación de amistad y confianza con él o la menor a quien quieren acosar.[29]

Es importante crear valores, lazos entre la sociedad y comunidad porque si bien se ha comenzado a abordar más temas como este, lo cierto es que muchas conductas se siguen llevando a cabo y normalizando los delitos.

La información o desinformación respecto a este delito toma relevancia porque cada día el tipo de familia tiene como figura paterna o materna a alguno o ambos que trabajan y los hijos, sobre todo durante y después del COVID-19 con tecnología más presente, tanto niños muy pequeños como más grandes acostumbrados a dispositivos electrónicos, pero a la vez expuestos a la manipulación de quién esta del otro lado, donde desafortunadamente se puede hacer querer ver como *amistad virtual* cuando estamos hablando del comienzo del *grooming* y sin una guía respecto a los peligros en lo digital.

[29]Fiscalía General de Justicia Ciudad de México, Unidad de Inteligencia Cibernética, Policía de Investigación de la Ciudad de México, Glosario de Delitos Cibernéticos, *op.cit.*

Generaciones donde han querido *volar* rápido (porque el crecimiento y derechos va de la mano con obligaciones) que intentan imitar estereotipos o relacionarse con personas más grandes no sólo psicológicamente sino afectivamente con daños y/o justificación del *abandono* por parte de los padres sin entender un mundo que se ejemplifican en lo laboral sin oportunidades y con una forma moderna de esclavitud donde los estafadores se aprovechan de las necesidades y carencias para utilizar la tecnología engañando y cometiendo delitos en total impunidad.

SHAMING.

> Es un tipo de acoso en línea, el cual busca avergonzar y humillar a una persona en redes sociales (Twitter, Facebook, Instagram, TikTok, entre otras).[30]

Es importante darle nombre a situaciones como lo son delitos *cibernéticos* porque desafortunadamente no ha significado que ya no se den, ni tampoco que se este atendiendo el problema, los *memes*, por ejemplo, han sido una forma *divertida*, incluso de ataque en campañas presidenciales, pero en realidad no se han tomado como una manera real de avergonzar y humillar a cualquier persona en un momento desafortunado, donde fácilmente quién está detrás de un dispositivo móvil toma una fotografía o video, se sube a la red y la persona que pasa por una situación penosa se convierte en burla mundial y que más allá de ello, está el honor y dignidad que pueden incluso darse como un hecho o influir en que lo despidan en su trabajo, se dañe su reputación y buen nombre.

Tener a la mano un teléfono para grabar, tomar una fotografía o compartir en tiempo real en las redes se ha vuelto común, con millones de vistas y reproducciones, pero al mismo tiempo puede no ser lo que aparentemente se quiere creer y realmente también ser una estafa, como ha sucedido en ciertos casos donde supuestamente se expone a una autoridad o restaurante por un cucaracha en la comida y en realidad es un engaño para ocultar que se trata de estafadores que usan esto como

[30]Código de ética para la prevención de la violencia digital contra las mujeres. Uso y consumo seguro de los servicios de telecomunicaciones, Gobierno de México, Secretaría de Economía, Instituto Nacional de las Mujeres (INMUJERES) y Procuraduría Federal del Consumidor (PROFECO), 2024, p.5.

forma de causar daño, obtener lucro, difamar o intimidar para obtener algo a cambio de la(s) víctima(a).

En el caso de las paqueterías, por ejemplo, con acusaciones de choferes que se *roban supuestamente* los paquetes o no llega lo que el cliente pidió, haciendo ver a los repartidores como amantes de lo ajeno, pero sin pensar que puede haber muchas historias detrás de una imagen (a veces vale más la historia o relato que lo que la imagen realmente se intenta presentar) porque no siempre lo que parece es y si la consecuencia de una fotografía puede repercutir en la vida de la persona, desde su trabajo, su familia o simplemente burla de quién identifique esa toma.

DOXING.

> El término proviene de la frase en inglés *dropping docs,* y consiste en la extracción y la publicación en línea no autorizadas de información personal.[31]

Actualmente, poner una palabra en internet arroja muchos resultados con el nombre de una persona, aparece una lista en donde posiblemente no se autorizó o dio su consentimiento, mucho menos la información de la descripción que aparece y esto es violatorio a derechos humanos porque incluso si se tratara de alguien que estuvo en reclusión, al pagar su pena se esperaría que la persona intente integrarse a la sociedad, con ello lo referente también a trabajo y aparecer en internet como *fichado* podría traer consecuencias para su vida, honor y empleo, que aunque demandara por el daño aún con sentencia absolutoria la misma sociedad ya condenó y posiblemente ni siquiera se reparara el daño. Por aún, nadie se hace responsable de ese daño porque sería como pensar en demandar a todos los que vieron el video, lo compartieron, se burlaron de cualquier forma.

[31]La violencia de género en línea contra las mujeres y niñas, Guía de conceptos básicos, OEA/CICTE, OEA/CIM/MESECVI, Secretario General Organización de los Estados Americanos (Arthur Weintraub), Secretario de Seguridad Multidimensional Organización de los Estados Americanos (Alison August Treppel) Secretaria Ejecutiva Comité Interamericano contra el Terrorismo (CICTE) Alejandra Mora Mora Secretaria Ejecutiva Comisión Interamericana de Mujeres (CIM) Equipo Técnico de la OEA Programa de Ciberseguridad Kerry-Ann Barrett Mariana Cardona Gabriela Montes de Oca Fehr Comisión Interamericana de Mujeres / Mecanismo de Seguimiento de la Convención de Belém do Pará Luz Patricia Mejía Guerrero Alejandra Negrete Morayta, Katya N. Vera Morales, apoyo financiero del Gobierno de Canadá, 2024, p.50.

Fácilmente se puede decir cualquier cosa sin una fuente confiable, sin una cita académica, sin datos de dicha información u opinión y nos estamos enfrentando a prejuzgar o dar por hecho algo, vivir de lo que creemos y no de la realidad porque cualquiera puede hacer uso y mal uso de información mediante la tecnología para su publicación sin quién se haga responsable de responder a la víctima.

Aunque se trate de una publicación emitida por una persona mediante su red social a nadie le da derecho el robo de ello y es precisamente esta acción lo que cambia y se convierte en delito y no perseguido, sino reproducido miles de veces y en algunos casos para crear perfiles falsos o inventar cosas de una persona y como dice el dicho *a veces una verdad contada tantas veces, aunque sea mentira se vuelve verdad,* para los demás pero lo lamentable es que parece también ser una verdad para la autoridad que no legisla y aplica la ley a favor de la víctima.

Este es un tema de igual forma de derechos humanos, la evolución y auge después de los *Juicios de Nuremberg*[32] en este tipo de información que cualquier persona puede subir a la *web* ya tiene intención dolosa de causar daño a otro.

> *Doxing o doxxing* (de dox, abreviación de documentos en inglés) es un término proveniente del inglés que se utiliza para describir la práctica en Internet de investigación y publicación de información privada (especialmente información personal) sobre un individuo o una organización, generalmente con el propósito de intimidar, humillar o amenazar.[33]

La información en redes sociales ayuda en casos de emergencia por ejemplo sanitarias, conflictos armados y pedir justicia como en los casos de violencia (por pruebas y conocimiento de dominio público) en desaparición y feminicidios, pero ¿qué pasa cuando el único propósito es la publicación para humillación y/o violencia hacia la víctima?

[32]Crímenes contra la humanidad que se dieron al finalizar la segunda guerra mundial y donde se juzgó a oficiales de alto rango Nazi.
[33]Fiscalía General de Justicia Ciudad de México, Unidad de Inteligencia Cibernética, Policía de Investigación de la Ciudad de México, Glosario de Delitos Cibernéticos, *op.cit.*

Tenemos cada día más público respecto a esto, como en el caso de figuras conocidas o personas que usan redes personales para alzar la voz, pero sigue sin transformarse en investigación real porque el *litigio* en las redes sociales se ha convertido para la población más importante que en los Tribunales y esto ha generado que no se tome con la seriedad, sino en situaciones mediáticas o que después de un tiempo *pasará de moda* cuando es un problema que se debe tomar en serio mediante la ley.

A lo anterior, se agrega que también el auge en redes se usa para debatir, informar, denunciar, informar o desinformar ha sido por personajes públicos que toman esta tecnología para en cualquier momento y a cualquier hora hacer publicaciones. Es entonces el ser humano de quien depende que la tecnología sirva en pro y no en contra de uno mismo y menos el volverse dependente o utilizarse con fines delictivos para dañar.

Abogados como el ex Ministro Arturo Zaldivar en pequeñas intervenciones ha informado y hablado de derecho, lo cual hace que hasta quienes no cursaron la carrera de derecho tengan acceso a conocimiento de situaciones y términos jurídicos, pero también existen abogados como en casos públicos como Héctor Parra y Sergio Andrade que más es publicidad que una forma de querer hacer presión para obtener justicias se ha dejado de litigar en Tribunales para hacerse notar y en casos sumamente cuestionables, que toman medios de comunicación como verdades emitidas por autoridades jurisdiccionales correspondientes, lo cual tampoco ayuda a que las redes estén reguladas, pero eso no significa que sustituyan al aparato judicial y su aplicación. Entonces pueden las redes verse como medio para que la opinión mediática se vuelva a su favor.

PHISING.

> Consiste en el envío de mensajes (anzuelos) a una o varias personas, recurriendo a la suplantación de la identidad de una empresa o entidad pública con el objetivo de persuadir a la futura víctima para revelar sus datos personales o financieros que involucran nombres de usuario y contraseñas. Una vez obtenida esta información es utilizada con fines maliciosos para realizar acciones como transferencias de fondos a cuentas bancarias y compras con tarjetas de crédito entre otras acciones delictivas que afectan económicamente a la víctima.
> En la actualidad la actividad de phishing utiliza principalmente el correo electrónico enviando correos falsos por parte del atacante. En estos correos se solicitan contraseñas o detalles de las cuentas bancarias argumentando comúnmente situaciones como problemas técnicos, procesos de actualización y revisión de datos buscando aprovecharse de la ingenuidad de los usuarios para obtener información. En algunos casos se emplean técnicas más sofisticadas como el uso de sitios web falsos, instalación de caballos de Troya, key-loggers, screen-loggers, envíos de mensajes de SMS, mensajes en contestadores automáticos y llamadas telefónicas.[34]

La información por medio de sitios *cibernéticos* ha beneficiado el uso de robo que va desde responder un mensaje como, por ejemplo, en aplicaciones de bancos, pero ¿qué sucede con tantos *hackers*[35], personas que dolosamente realizan acciones utilizando la tecnología para obtener información confidencial y cometer fraudes? Sobre todo, hoy en día que prácticamente podemos hacer todo mediante la tecnología, el *supermercado*, realizar compras en tiendas departamentales, pagar una tarjeta de crédito y más, sin embargo; este tipo de facilidades parecen ser las mismas en que personas con malas intenciones abusan.

La suplantación de identidad es un tema que conforme pasa el tiempo se perfecciona más (desafortunadamente en manos equivocadas y con fines de lucro y daño), sumando a homónimos en donde mientras se investiga o se deslinda responsabilidad la persona queda expuesta por parte de autoridades.

[34]Miriam J. Padilla Espinosa, Universidad Nacional Autónoma de México (UNAM), revista. seguridad | 1 251 478, 1 251 477| revista bimestral, Coordinación de Seguridad de la Información (UNAM CERT), Seguridad de la Información, pescando información phishing, 2024.
[35]Persona que tiene conocimientos amplios en informática y en teoría debe desarrollar mejora.

Si bien, ya existe mayor difusión por parte de Instituciones Bancarias para no compartir datos, contraseñas y ningún tipo de información, incluso que no se le solicite a sus clientes ningún tipo de datos confidenciales, lo cierto es que en grupos vulnerables como por ejemplo adultos mayores que generalmente buscan y estafan en brindarles supuestas ayudas por no tener conocimiento de tecnología, pero si con cuentas o apoyos sociales que necesitan cobrar, puede prestarse a no las mejores intenciones desde sus cercanos o por ejemplo comunidades indígenas que se enfrentan a la falta de comunicación e información correcta por el idioma necesitan también quien les apoye para poder hacer retiro de algún deposito en algún cajero electrónico.

De igual forma los migrantes en el envió de dinero a sus seres queridos, son más vulnerables al *phising* porque no se trata únicamente de poder realizar los depósitos, sino del retiro y el idioma.

Nos parece sumamente importante que la difusión de este tipo de delitos acompañe la misma precaución de no compartir información o contraseñas porque en una era donde todo se convierte en digital, es de igual forma la modernización para cometer delitos que avanzan más rápido ante la nula o solo posible solución al delito o quién fue víctima de ello se haga justicia.

No se trata sólo de un mensaje, porque al involucrar temas bancarios como tarjetas de crédito y todo aquello de índole económico es el patrimonio de la(s) persona(s) y familia, significa el esfuerzo realizado para poder obtener esa remuneración y de la cual tan fácilmente aparentando un botón puede invalidar todo el esfuerzo, sacrificio y tiempo para poder obtener ello.

Por lo anterior, la legislación, prevención y destino de recursos para la tecnología es necesario, sobre todo en un país como México en que los candidatos presidenciales podrían abordar este tipo de delitos que, si bien ellos hacen uso de las redes sociales para campañas o hablar mal de otros, son conscientes de la

importancia de la tecnología y que del buen o mal uso de ello las consecuencias no se quedan en un video, sino trascienden a la vida.

La suplantación de identidad no es exclusiva de alguien, por ejemplo de una determinada profesión o actividad económica, es un tema que puede afectar a todos por igual, por lo que abordar en legislación y castigo para ello puede ser la diferencia entre poder acceder a la canasta básica, acceder a la educación, tener o no un patrimonio.

PHARMING

> El pharming es una combinación de los términos "phishing" y "farming" que significa cultivo y "phishing" que representa una técnica nueva y más complicada para acceder a información personal o bancaria de otra persona. De acuerdo con la CONDUSEF, el pharming es aquella práctica que consiste en la redirección a una página de internet falsa mediante ventanas emergentes, con el objetivo de robar información. A través de esta actividad se busca obtener beneficios económicos e información privilegiada, muchas veces para la generación de estafas…
> Esta práctica aprovecha la vulnerabilidad del software de los servidores con la intención de modificar o sustituir el archivo del servidor de nombres de dominio cambiando la dirección IP de una entidad, ya sea que se hagan pasar por los sitios de banca electrónica o de pago para redirigirlos a una otra IP que se aloja en una página web falsa (la misma que fue introducida por el ciberdelincuente) y, de esta forma obtener las claves de acceso a las diferentes cuentas.[36]

La difusión de este tipo de delitos para que la población en general tenga mayor precaución en cuanto a que aunque reciban supuestas noticias por parte de alguna Institución bancaria es importante siempre acudir o preguntar tanto a la dependencia como a alguna autoridad como Ministerio Público o Fiscalía, esto debido a que también debe contemplarse que al recibir este tipo de datos, las personas por desconocimiento, desesperación o sin apoyo (como guía o teléfono de emergencia y acudir) pueden caer en cada vez más modernización por quienes cometen estos delitos que pareciera tener que competir con *hackers* aparentemente *profesionales* y que puede incluso tratarse de una persona de

[36]Guía para Prevenir el Pharming, Secretaria de Hacienda y Crédito Público, Instituto Federal de Telecomunicaciones, 2024, pp.1-2.

hecho menor de edad con conocimientos en informática y tecnología desde cualquier lugar.

Sin duda, el robo de información se ha modernizado y encontrado auge en la era del avance, sobre todo porque generaciones que no crecieron con lo tecnológico son quienes más fácilmente han caído en estas estafas.

El derecho por mucho tiempo se había mantenido el litigio en Tribunales de forma tradicional, esto significa que no había el sistema oral y aún más en el sistema penal, lo cual para quienes toda su vida vivieron de esa forma, representó un desafío por lo que muchos incluso debían replantearse si continuar o no porque al estar en audiencia orales, grabaciones y sin tener los documentos para en cualquier momento hacer uso de ellos representaba un reto que no todos podrían acoplarse (esta nueva realidad del derecho), cambio incluso la forma de llevar los procesos porque es aquí que cobra más relevancia que muchas audiencias empezaron a realizarse de forma virtual.

Lo anterior, representó avance para comenzar a empaparnos en una era donde la tecnología estaba de la mano con cualquier actividad y que sobre todo en época de pandemia por COVID-19 se vivieron momentos en donde jueces llamaron la atención a quién se encontraba del otro lado de la pantalla (como abogados de oficio o defensores) porque fueron captados en momentos penosos (algunos en ropa interior, otros en condiciones informales para llevar a cabo las audiencias y muchas más situaciones donde también personas de su familia entraban o salían) porque la tecnología no era ir en contra con la formalidad y las maneras en que se estaba comenzando a vivir, era una forma de poder seguir adelante en un mundo incierto, incluso para las leyes y el derecho.

> *HAPPY SLAPPING* "Bofetada feliz". Se trata de una forma de acoso y violencia en la que se graba una agresión y se cuelga en la red con el objetivo de agravar la humillación. A diferencia de otras formas de acoso, una de las características que distingue al happy slapping es la planificación premeditada de la agresión física, verbal o sexual a la víctima. Como parte de esa planificación, el agresor busca una excusa para aislar a su víctima y elige el lugar donde llevará a cabo la agresión, a

menudo un sitio en el que no le puedan interrumpir. El propio agresor o quien/es le acompaña/n se encarga/n de subir el contenido a Internet en un intento de fortalecer su ego personal y humillar aún más a la víctima.

GRIEFING La situación en que un niño o adolescente es repetidamente atormentado, acosado, humillado, avergonzado o de alguna manera molestado por otro niño o adolescente a través de mensajes de texto, correo electrónico, mensajería instantánea, o cualquier otro tipo de tecnología de comunicación como bien pueden ser los sitios de redes sociales, foros… de videos en línea.

GOSSIP (RUMORES) Extender rumores es una práctica habitual entre las personas y, por tanto, también entre las jóvenes. Pero con las posibilidades tecnológicas, el alcance y permanencia de los rumores se amplifican. En esta práctica se utilizan los programas de mensajería o las redes sociales para extender rumores. Además de los riesgos derivados de la falsedad de la información asociada al rumor, extender estos rumores en Internet puede ser un detonante de conductas de ciberacoso o, simplemente, una forma de acoso más.

OVERSHARING Sobreexposición en redes sociales a partir del contenido compartido. En parte, esta sobreexposición genera un contexto favorable a algunos formatos y prácticas de acoso y ciberacoso.

REVANGE PORN (PORNO VENGANZA) Se trata del crimen ejercido a través de la exposición pública de imágenes, fotos o videos íntimos de terceros de manera no consensuada (aunque las imágenes sí se hayan tomado con el consentimiento de la víctima). Normalmente el agresor es una pareja o ex-pareja que divulga aspectos íntimos para vengarse tras el fin de la relación sentimental. Las imágenes también pueden ser obtenidas por el hackeo o invasión de cuentas de la víctima.

SEX-CASTING Se define como la grabación de contenidos sexuales a través de la webcam y la difusión de los mismos por e-mail, redes sociales o cualquier canal que permitan las nuevas tecnologías.

MOBBING Se produce en el ámbito laboral, se refiere a todas aquellas acciones encaminadas a intimidar, vejar o degradar a un trabajador con el objetivo de empeorar su clima laboral y empujarle a abandonar la empresa. Este hostigamiento puede realizarse a través de diferentes métodos, por ejemplo, insultos, amenazas, humillaciones, aislamiento del resto de compañeros, difusión de rumores falsos.

ROBO DE IDENTIDAD, *IDENTITY THEFT O ID THEFT* La usurpación de identidad es uno de los ciberdelitos más comunes y suele tener una finalidad económica (compra de bienes o contratación de servicios a cargo de la identidad afectada) o bien en fin relacionado con el ciberacoso…

CIBERVIOLENCIA DE GENERO La violencia contra las mujeres, en muchos casos adolescentes, es un problema que ha encontrado en Internet un nuevo contacto y nuevas formas para su desarrollo.

ESCNNA La Explotación Sexual Comercial de Niños, Niñas y Adolescentes (ESCNNA) es la utilización sexual de niños, niñas y adolescente (NNA) por parte de uno o varios adultos a cambio de un pago en dinero o en especie... La ESCNNA viola los derechos a la vida, salud, dignidad y al desarrollo pleno de la niñez y adolescencia.

MASNNA El material de abuso sexual de niñas, niños y adolescentes (MASNNA) son fotos o videos que muestran a menores de edad en situaciones sexuales.

RANSOMEWARE O MALWARE o secuestro de datos, es un tipo de programa dañino que restringe el acceso a determinadas partes o archivos del sistema operativo afectado y pide un rescate a cambio.

ASNIC Se expresa con palabras en clave en plataformas digitales para obtener material sensible como pornografía infantil.
CRYPTOJACKING MALWARE Es un malware que infecta las computadoras para…cripto monedas, generalmente sin el conocimiento de los usuarios. [37]

Desafortunadamente con el avance, pareciera existir o venir un retroceso en las personas, como sociedad y en valores que más allá de que la tecnología ha aportado por mejora, también se ha vuelto una era en la que desde relacionarnos unos con otros empieza a ser un problema porque existe una diferencia de opiniones, de poder ceder o tener la forma para poder coexistir y convivir unos con otros con respeto y que al parecer volvernos a integrar a una vida en sociedad cambiaría.

La misma forma de video juegos ha cambiado y se han incluidos *juegos* que normalizan la violencia y pérdida de valores, como por ejemplo matar (sexoservidoras) disparar, robar y demás aspectos que en teoría se tomarían a simples dinámicas, pero ¿qué pasa por la mente de quién crea este tipo de supuestos juegos y también quién consume y juega esto?

La vida no es un juego en el que alguien decide matar, en el que los valores no existen al lado de dinero, se nos ha rebasado esta realidad virtual a la vida, porque casos sobre todo en Estados Unidos de Norteamérica tienen con personas que entran a las escuelas y matan a otros, ya sea compañeros(as) o/y maestros(as).

También casos en donde se ha utilizado tener un supuesto daño por culpa de los videojuegos para declararse incompetente en juicio, con algún daño mental de lo cual se usa y se burla de la ley.

El exceso de vida virtual y no real ha provocado delitos como *pornovenganza* que la falta de atención psicológica para el agresor que generalmente es la expareja se vuelve una realidad enferma en el mundo virtual porque la difusión de imágenes o

[37]Fiscalía General de Justicia Ciudad de México, Unidad de Inteligencia Cibernética, Policía de Investigación de la Ciudad de México, Glosario de Delitos Cibernéticos, *op.cit.*

videos, *hackeo* o invasión en cuentas de redes sociales de la víctima (ex pareja) debe ser condenada por parte de los cercanos, quienes se prestan a escuchar hablar mal de quien fue su pareja, de juzgar cuando no son capaces ni siquiera de tener una vida sana, de académicos que pueden ser cercanos y dejar de lado su ética para que el morbo sea más importante o la misma familia que no condena la violencia y promueve la salud mental acudiendo, por ejemplo, a terapias.

En el ámbito laboral no promoviendo el respeto hacia los mismos compañeros y subordinados, que tan fácilmente se dejan comprar por un ascenso pese el dolor, humillación o acoso de un cercano, que nuevamente tiene que ver con falta de valores y en una sociedad que pareciera creer vivir en una realidad virtual, en la que pareciera no entender por lo que pasa una víctima, como si se tratara de avanzar en tecnología y perder valores.

Formamos parte de un continente que mucho juzga a países de Medio Oriente, lo cual no significa que muchos de los señalamientos sean correctos y violatorios a derechos humanos, dignidad y vida, pero la violencia y *ciberviolencia*, pornovenganza (en países desarrollados), crear rumores para difamar, robo de datos (personales e íntimos) nos hace ¿menos violentos? No, la violencia es violencia y existe peor violencia como tortura y todo aquello que atente contra los derechos humanos, pero entonces es fácil hablar de usos y *costumbres atrasadas,* pero ¿la tecnología justifica otro tipo de delitos?

La comunidad internacional juzga la forma en que el presidente salvadoreño Nayib Bukele actuó para acabar el crimen organizado de las pandillas, pero nada hicieron cuando estos hoy en día prisioneros atacaban a la población civil. Guantánamo desafortunadamente famosa por las violaciones graves a derechos humanos nada ha cambiado esa realidad. Entonces la tecnología que puede ayudar para la difusión de estos casos, para que se actúe y no existan víctimas sólo funciona en ciertos casos y en otros no ¿de qué depende? Podría ser del poder adquisitivo, político, económico o en casos de exparejas incluso del poder del agresor sobre la víctima.

CARDING.

> operaciones datan de finales del siglo XX y…la aparición de Redes Sociales, se evidencia que estas dan su gran salto en 2004 con la creación de Facebook, es decir, hace 13 años, tiempo en el que tanto la complejidad de la comunicación como el mundo digital han tomado mayor vigor en desarrollo de la humanidad. Cuando se trasciende del contexto internacional y se revisa un concepto como el de Carding que se refiere al fraude con tarjetas de crédito y débito. "El Carding consiste en comprar usando la cuenta bancaria o la tarjeta crédito de otro, esto se consigue con un poco de ingeniería social… con una correcta vigilancia de la víctima"[38]

Es preocupante este delito porque el hecho de contar con tarjeta de débito o crédito no significa poder adquisitivo, puede ser mucho tiempo de esfuerzo y sacrificio para que de un momento a otro por culpa de otra persona dolosamente la víctima quede en estado de indefensión, lo cual si bien existe un poco más de difusión respecto a tener cuidado, lo grave en pocas palabras es culpar a quién sufre el delito porque no se le hará justicia, reparación y es quién debe invertir tiempo para acudir a las instancias y autoridades correspondientes con excesiva burocracia de por medio y se le haga justicia, que puede llegar o ser sumamente tardada, para lo cual esta persona ya ha dejado de percibir dinero por ausentarse a trabajar, empeorando su situación y viviendo la impunidad de las personas que cometieron un fraude.

CRACKING.

> El 'cracking' consiste en la destrucción o en la producción de daños en su sistema, datos, programas informáticos o telemáticos.[39]

Cada vez es más común que las mismas empresas tengan un sistema de ingenieros e informáticos para respaldo de su información, datos sensibles y confidenciales para evitar este tipo de daños, pero quienes están más expuestos a ello son las personas que podríamos denominar como *comunes* (de la sociedad y vida cotidiana) porque son las que al no contar con este tipo de conocimiento(s),

---

[38]Jonathan Durán Pamplona, P*rincipales características, modos de perpetración y vulneración de la seguridad informática a través de la modalidad carding*, Universidad Nacional Abierta y a Distancia "UNAD" Escuela de Ciencias Básicas, Tecnología e Ingeniería (ECBTI) Especialización en Seguridad Informática Bogotá, Colombia, 2020, p.25.

[39]Ilustre Colegio de la Abogacía de Madrid, 2024, p.15, de: https://web.icam.es/bucket/Faustino%20Gud%C3%ADn%20%20Nuevos%20delitos%20inform%C3%A1ticos.pdf

pero si expuestos en todo momento en información/desinformación de supuestos avisos por ejemplo bancarios, como en el *hot sale* o demás temporadas de *rebajas*, correos y mensajes *en línea* que han hecho del comercio electrónico una aparente forma de pedir algo sin salir de casa, pero que también se ha prestado para otro tipo de estafas, fraudes y delitos.

Podría pensarse que en el mundo existen tantos temas delicados que difícilmente se puede lograr una sociedad más justa, pero dos temas fundamentales que pretende abordar esta investigación es: la violencia (*ciberviolencia*) salud mental porque de estas dos parten muchos problemas que se vuelven delitos y que siguen escalando sin conciencia real.

Es indescriptible pensar que existen seres humanos capaces de cometer actos tan atroces como se ha desarrollado en el presente capítulo, pero resulta peor una sociedad y autoridades cómplices por no hacer o callar en un país con sed de justicia, impotencia y muerte en vida, aunque suene contradictorio.

Por esto que en el siguiente capítulo se desarrollarán a detalle las legislaciones que pasan imperceptibles y se pierden en una población *zombie* que podría definirse como los *juegos del hambre* (de forma muy parecida a la conocida película que sintetiza la vida actual).

El tema no es arreglar todos los problemas del mundo porque es imposible, pero sí empatizar en no darles continuidad a delitos que tan comúnmente se pueden presentar, por ejemplo: en el ámbito académico y que la pregunta sería ¿por qué callar ante el dolor de otros(as) por qué cubrir a quién violenta, por qué juzgar el actuar de la víctima y por qué voltear como si estuviéramos exentos a estos delitos?

CONCLUSIONES DEL CAPÍTULO

El comercio electrónico ha facilitado el intercambio a través de internet para mejorar la vida de las personas, la llegada rápida de mercancía, compra y venta de productos de forma más eficiente y eficaz, sin embargo; este es uno de los usos en los cuales la tecnología ha permitido que la vida de las personas mejore como lo fue en la contingencia de COVID-19, que gracias a esta forma de comercio electrónico y entregas, muchas personas pudieron tener ingresos para poder comprar con comida o quienes desafortunadamente padecieron las secuelas y necesitaron medicamentos estuvo a su alcance poder continuar generando dinero y por lo tanto la vida no dejara de seguir y existir.

Lo que tal vez fue tan rápido en medio de caos social, económico y psicológico ya que la tecnología daría pasos gigantes para quedarse y demostrarnos una vez más que no podemos permitir que nos rebase, que se viole derechos humanos o que sea el medio para cometer delitos, aprovechándose de vacíos o ausencia de leyes.

Es por ello tan importante poder darle nombre a los delitos que se mencionaron a lo largo del capítulo, para que se logre se tipifiquen en todo el país, siempre con la bandera de que no haya víctimas y normalizando el uso de leyes respecto a delitos *cibernéticos*.

En el siguiente capítulo, se realizará un análisis en cuanto a la legislación con que cuenta México respecto a los delitos *cibernéticos* y poder evidenciar que, si bien ya existían víctimas cuando no se tipificaban los delitos o no se conocían jurídicamente, lo cierto es que es urgente legislar, no sólo se den penas en años y más años de prisión, no sólo simulación o que únicamente se aplique al sector financiero o con poder adquisitivo sino la mínima importancia o todos los delitos. Que no se trate de poner en balanza en qué delito es más grave o que consecuencia es por la que se debe aplicar la ley, porque todas las víctimas y personas son importantes y tienen derechos.

CAPÍTULO 2. ANÁLISIS DE LA LEGISLACIÓN EN MATERIA DE DELITOS CIBERNÉTICOS EN MÉXICO.

Es importante concientizar a la población respecto a las múltiples formas en que los delitos *cibernéticos* pueden afectar a las personas, porque no se trata únicamente de temas que pueden sonar lejanos, la realidad es que esto podría llevarnos a estar más alertas, informados y tener herramientas para pedir ayuda, ya que entre más difusión se tenga al respecto más preparados estarán los gobernados y serán conscientes para exigir a las autoridades mecanismos reales contra este tipo de delitos.

Dentro de la legislación especial que se tiene en el país en materia de delitos informáticos podemos sintetizarlos de la siguiente forma:

1.-Ley de Instituciones de Crédito.
2.-Ley de Instituciones de Seguros y de Fianzas.
3.-Ley del Mercado de Valores.
4.-Ley General de Títulos y Operaciones de Crédito.
5.-Ley Federal de Protección de Datos Personales en Posesión de los Particulares.

En general siempre un factor en el que se ha priorizado es lo económico y aquello que represente plusvalía o se obtenga remuneración al respecto, difícilmente se legisla o se pone atención como, por ejemplo; en los delitos *cibernéticos* de tipo sexual en donde las secuelas por parte de las víctimas en su mayoría son de por vida e imperceptibles para los demás, pero la (s) victima (s) con una vida destrozada y la exposición que internet almacena como para nunca olvidar.

Se debe brindar atención psicológica (mediante terapia, gratuidad en medicamentos) médica y asesoría jurídica gratuita, así como información de sus derechos cuenten o no con conocimientos al respecto y garantizar en medida de lo posible la reparación del daño.

Atención psicoemocional y médica mediante centros de salud, pero no exclusivas para mujeres, sino quien sea que haya sido víctima, sin importar del género, edad ni ningún tipo de discriminación.

Quiénes sobreviven, *cargan* con el peso de no haber obtenido justicia, de señalamientos que pueden incluso llegar hasta la pérdida de empleo o de no poder rehacer su vida, peor aún el Estado no provee ni cuenta con la capacidad para brindarles atención psicológica y apoyo económico mediante la reparación del daño y el pasar de tantos años terminen por revictimizar más a quién desafortunadamente nada le devolverá su vida, tranquilidad, ni le dará justicia.

Podría sonar absurdo remitirnos a que lo mejor es bloquear mentalmente todo a continuar en un proceso legal que dura años sin que esto sea relevante para que verdaderamente se aplique la ley al agresor(a).

Nos parece que respecto al tema de delitos *cibernéticos* de carácter sexual aún falta mucho por avanzar, no sólo porque en México, aún existen muchos *tabús* al respecto y peor aún cuando los medios de *información* son las redes en donde nadie se hace cargo las consecuencias de lo dicho. Internet ha representado un lugar tan accesible que quiénes cometen *ciberviolencia* encontraron un hogar que no cuestiona, no regula y permite se continúe en el tiempo de los delitos pasados, presentes y da lugar a los futuros.

La falta de comunicación entre las mismas familias y la despersonalización más tangible en la pandemia da la impresión de que se trata de una nueva forma de esclavitud, que al importar sólo lo económico, el trabajo se vuelve la vida de las personas, con hijos en el abandono y refugio en redes sociales sin tener en cuenta los delitos *cibernéticos* a los que se podían enfrentar.

La conciencia entre la población es fundamental para erradicar este tipo de delitos, porque más allá de la pena, debemos preguntarnos ¿cuáles son las consecuencias de la falta de comunicación y empatía entre personas? Esto porque pareciera que existen dos mundos: *el virtual y el real* que mucho del auge tiene que ver con la contingencia por COVID 19 en donde no solamente cambió la manera de ver al mundo sino de relacionarnos unos con otros, pero también a una vida que la modernidad ha transformado en pláticas virtuales en mensajes, videojuegos (con violencia) sin guía ni formación personal.

Lo anterior, no significa que sean delitos exclusivos de menores de edad, precisamente lo delicado es que cualquier persona puede ser víctima de ello y para quién sea la justicia puede ser inalcanzable. Las víctimas no son más víctimas si son hombres o mujeres, si son creyentes o no porque las víctimas no tienen una calificación de acuerdo a su vida pasada, tienen esa calidad como persona y que desde el ámbito laboral podríamos entender como empleados, para ser un número reemplazable, lo que significa que se deja ver y tratar al ser humano como persona, para ser números, cifras y daños colaterales de la delincuencia.

El dinero más que nunca se ha vuelto necesario durante y después de la pandemia (porque no se trató de recobrar lazos familiares, sino a generar más y más porque el valor y sentido de la persona se ha enfatizado en el nivel económico de vida, que se ha traducido a que es lo que vale el ser humano). La realidad *virtual* donde las *criptomonedas* tienen un valor, pero no son tangibles como el avance en la tecnología.

Desafortunadamente las personas pueden ser capaces de muchas atrocidades (tenemos antecedentes donde la maldad y crímenes contra la humanidad se dieron durante el genocidio a los judíos por parte del sistema de Nacismo, la Guerra de Vietnam, Corea y Guerra de los Balcanes (racismo)) por odio, dinero o por trastornos psicológicos (que no justifica el daño hacia otros (as)).

La salud mental es equilibrio y bienestar de la persona como con su entorno, lo que podría también traducirse en que si tiene salud mental no existen trastornos mentales y tampoco se darían situaciones delictivas, como por ejemplo los delitos *cibernéticos*. Por ejemplo, para la OMS significa un estado de bienestar tanto lo mental, físico y lo social.

Cuando se ve afectada la seguridad, esperanza, tranquilidad, salud física y mental, alimentación, sueño, estado de ánimo, defensas, emociones, tolerancia, la forma de resolución, confianza en sí mismo(a), adaptabilidad y toma de decisiones no se puede priorizar en tecnología, sino en brindar a la población las herramientas al alcance para salud mental, lo cual también ayudaría a evitar muchos delitos, incluso *cibernéticos*.

Lo psicológico en la víctima no sólo se afecta desde el cambio de perspectiva hacia el cómo en un momento todo es diferente, sino en trastornos como depresión, estrés postraumático, ansiedad, alimentación, sueño, no encontrar sentido a su propia vida. Porque al verse afectada la salud mental se pierde el sentido.

Es importante mencionar a Michel Foucault (pensador francés) quien hablo ampliamente del poder que se encuentra en todos lados, una red de relaciones de iguales y que no solamente se refiere a lucha de clases. La preocupación respecto del poder y cómo funciona, analizando los sistemas penitenciarios desde el poder, enfatizando la voluntad y control en los individuos lo cual se traduce a disciplina.

Esa disciplina que es normalizada como forma de pensar, lo cual define que es lo normal y que no, es por ello que la definición de loco es la construcción que quita la libertad porque por medio de vigilar y castigar significa y es igual a poder y control del individuo de normalización y domesticación.

Si bien, los avances en herramientas digítales, lo laboral o personal, plataformas como *meet*, *zoom* y demás han permitido y facilitado la cercanía entre familias o amigos, en el trabajo estar en tiempo real en juntas desde distintas partes del mundo, trabajo en casa u oficina en distintos lugares y países, también tenemos el uso lamentable de sitios como la denominada *deep web*[40] que autoridades están conscientes de su existencia, pero en la realidad inexistente para tantas víctimas (personas y animales) que no sólo existe dinero de por medio, sino como sociedad valdría la pena preguntarnos ¿qué tan mal estamos que es tanto el vacío o ningún sentimiento para ser capaces de permitir (por acción u omisión) siga existiendo este mercado y consumirlo? Porque esto bien no existiría o terminaría si no hubiese consumidores.

> Desde 1999, México tiene legislación federal para sancionar delitos informáticos en México, afectando principalmente al sector financiero, y las organizaciones afectadas pueden enfrentar interrupciones, pérdidas financieras, daños reputacionales y consecuencias legales.
> Los delitos informáticos son acciones ilícitas que se realizan utilizando medios informáticos o en línea. Estos delitos pueden variar desde el robo de datos y la suplantación de identidad hasta el fraude financiero y el sabotaje de sistemas informáticos. Quienes cometen estos delitos pueden ser individuos con conocimientos técnicos en informática, grupos organizados especializados en actividades delictivas en línea, o incluso entidades estatales que realizan ciberataques por motivos políticos o económicos…
> Algunos ejemplos de estos delitos incluyen:
> **1.-Acceso ilícito a sistemas y equipos de informática:** Se refiere al ingreso no autorizado a sistemas informáticos, redes o dispositivos electrónicos con el propósito de obtener información confidencial o cometer acciones perjudiciales.
> **2.-Revelación de secretos:** Consiste en la divulgación no autorizada de información confidencial o secreta, ya sea mediante el acceso indebido a sistemas o la revelación deliberada de datos sensibles.
> **3.-Alteración o manipulación de medios de identificación electrónica:** Implica la modificación o manipulación fraudulenta de documentos electrónicos o medios de identificación, como contraseñas, para cometer actividades ilícitas o suplantar identidades.

[40] *La Deep Web* se refiere a cualquier *sitio web* al que no se puede acceder fácilmente a través de un motor de búsqueda convencional como *Google* o *Yahoo*! La razón de esto es porque el contenido no ha sido indeseado por el motor de búsqueda en cuestión.
En términos simples, podemos responder a la pregunta "¿qué es la *Deep web*?" señalando que es solo otro "nivel" de Internet. Residiendo debajo de la "superficie", es el nivel más profundo de Internet (aunque está la *Dark web* que es lo más profundo dentro de la *Deep Web*).
Revista Digital INESEM, Escuela de líderes Masters Online, Cursos y Postgrados, INESEM Business School,12/06/2024, de:
https://www.inesem.es/revistadigital/informatica-y-tics/para-que-sirve-la-deep-web/

4.-Delitos contra la indemnidad de privacidad de la información sexual: Engloba acciones que vulneran la privacidad sexual de las personas, como la difusión no consentida de imágenes íntimas o la invasión de la privacidad en línea.
5.-Delitos en materia de derechos de autor: Incluye la reproducción, distribución o uso no autorizado de obras protegidas por derechos de autor, tanto en línea como fuera de ella, con fines comerciales o no comerciales.
6.-Engaño telefónico: Se refiere a la manipulación o el uso fraudulento de comunicaciones telefónicas para cometer estafas, obtener información confidencial o realizar actividades delictivas.
7.-Falsificación de títulos: Implica la creación o alteración fraudulenta de documentos, certificados o títulos con el fin de obtener beneficios indebidos o engañar a terceros.
8.-Suplantación de identidad: Consiste en hacerse pasar por otra persona, ya sea en línea o fuera de ella, con el propósito de cometer fraude, obtener información confidencial o realizar acciones ilegales en nombre de la víctima.
9.-Delitos equiparados al robo: Engloba acciones que, aunque no sean robos en el sentido tradicional, implican la sustracción indebida de recursos, información o activos a través de medios electrónicos.
10.-Casos de acoso sexual: Incluye conductas de acoso, hostigamiento o intimidación de naturaleza sexual realizadas a través de medios electrónicos, como el envío de mensajes no deseados o la difusión de contenido sexual sin consentimiento.
11.-Distribución o posesión de pornografía ilegal: Refiere a la distribución, posesión o promoción de material pornográfico que involucre a menores de edad o que haya sido obtenido ilegalmente, lo cual constituye un delito grave con implicaciones legales y sociales significativas.[41]

El poco o nulo conocimiento respecto a leyes, por lo menos en México ha resultado muy convincente para quiénes cometen delitos como para las autoridades corruptas o que simplemente ni siquiera tienen empatía por las víctimas.

O tenemos otra situación en la que es lamentable que quién comenta un delito *cibernético* (peor aún de tipo sexual) tenga conocimiento de las leyes, que haciendo uso del conocimiento de las legislaciones se escude en cómo arruinar la vida de las personas, que su salud mental este tan afectada y su vida sea tan poco valiosa sea psicológicamente más enfermo cometer delitos *cibernéticos*, porque una vida que no ha servido más que para obtener cosas a costa de la desgracia de otros, que se suma la impunidad por parte del aparato judicial también que no empatizan con las

[41]Maricela Ochoa Serafín, *Delitos Informáticos en México. Conozca las leyes y las multas*, DIGIXEM 360, Digital for Empowerment, 01 Dic 2023, de:
https://www.itmastersmag.com/ciberseguridad/delitos-informaticos-en-mexico-que-dice-la-ley/

víctimas. Esto es reflejo de como los delitos *cibernéticos* podrían ser inexistentes mediante salud mental, leyes que realmente prevengan, combatan y erradiquen.

Enfrentarse como víctima de un delito a instancias del Estado, creadas en la teoría para hacer que se aplique la ley y en realidad no interesadas en ayudar, orientar, incluso realizar su trabajo es una constante en un país que ha clamado justicia por años y que día a día se vuelve tan común la impunidad y la falta de aplicación de la ley sin importar condición social, económica, política, con poder o género.

El años pasado tuvimos elecciones presidenciales donde ni el candidato, ni las candidatas presentaron propuestas hacia combatir y erradicar los delitos *cibernéticos* anteriores (ni siquiera fue tema y menos de relevancia para emitir propuestas) no se abordó ni siquiera por los moderadores, ni preguntas de la sociedad, incluso ni siquiera el máximo Tribunal en nuestro país (Suprema Corte de Justicia de la Nación SCJN) no ha realizado pronunciamientos o encontrado canales masivos o mediante amparos y resoluciones, fomentar el alto a delitos *cibernéticos*, prevención, causas, apoyo para la prevención y evitar ser víctima o en caso de serlo obtener justicia mediante jurisprudencia, información y leyes.

Por ejemplo, extorsiones en centros penitenciarios y el *módus operandi* es alarmante porque lo primero a cuestionar es si ¿estos centros no están cumpliendo con su función de reinserción, económicamente con su creación y mantenimiento derivado de impuestos de los(as) mexicanos(as) y por lo tanto la rendición de cuentas que fundamental, entonces deberían continuar operando?

No se necesitan más centros penitenciarios, se necesita aplicación de leyes y justicia con empatía, contar con interés de no ser cómplices de burlas, hostigamiento, acoso desde la casa, escuela y centros de trabajo. Que sea la falta de empatía hacia una víctima tan grave como robar un auto (porque al parecer un auto tiene más valor para una sociedad, leyes y autoridades que la misma vida) que se persigue más que el feminicidio.

La existencia de los delitos *cibernéticos* ha tenido auge por una sociedad vacía goza con imágenes de descuartizados, desollados, todo tipo de violencia física, psicológica y *ciberviolencia*, así como maltrato y tortura a los animales, con el desorden mental de *disfrutar* que se vaya desangrando como en las corridas de toros, volviendo loco al animal para quienes pagaron por un circo sádico que gozan en las redes al igual que se traslada a las personas y la violencia cada día más deshumana.

Tristemente erradicar los delitos *cibernéticos* puede transformarse en una lucha y círculo como en el predicamento de qué fue primero ¿el huevo o la gallina? donde en realidad queda en lo ético, filosófico y etimológico que nada vale en una sociedad mentalmente dañada.

2.1. LEGISLACIÓN EN EL PAÍS COMO MARCO GENERAL.

Actualmente, las empresas desde el inicio del proceso de selección incluyen en los contratos apartados de confidencialidad de los empleados hacia la empresa, esto conlleva la no divulgación de información, el uso de temas sensibles, la no revelación de fórmulas como en el caso de recetas de comida en *Kentucky Fried Chicken (KFC)* y lo que implica la revelación de este tipo de secretos, que en el Código Penal Federal en México nos dice:

> TITULO NOVENO
> Revelación de secretos y acceso ilícito a sistemas y equipos de informática
> CAPITULO I
> Revelación de secretos
> Artículo 210.- Se impondrán de treinta a doscientas jornadas de trabajo en favor de la comunidad, al que sin justa causa, con perjuicio de alguien y sin consentimiento del que pueda resultar perjudicado, revele algún secreto o comunicación reservada que conoce o ha recibido con motivo de su empleo, cargo o puesto.
> Artículo 211.- La sanción será de uno a cinco años, multa de cincuenta a quinientos pesos y suspensión de profesión en su caso, de dos meses a un año, cuando la revelación punible sea hecha por persona que presta servicios profesionales técnicos o por funcionario o empleado público o cuando el secreto revelado o publicado sea de carácter industrial.
> Artículo 211 Bis.- A quien revele, divulgue o utilice indebidamente o en perjuicio de otro, información o imágenes obtenidas en una intervención de comunicación privada, se le aplicarán sanciones de seis a doce años de prisión y de trescientos a seiscientos días multa.
> CAPÍTULO II
> Acceso ilícito a sistemas y equipos de informática
> Artículo 211 bis 1.- Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a dos años de prisión y de cien a trescientos días multa…
> Artículo 211 bis 2.- Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática del Estado, protegidos por algún mecanismo de seguridad, se le impondrán de uno a cuatro años de prisión y de doscientos a seiscientos días multa.[42]

[42]Código Penal Federal, 2024, Nuevo Código Publicado en el Diario Oficial de la Federación el 14 de agosto de 1931, Últimas reformas publicadas DOF 17-04-2024, Cámara de Diputados del H. Congreso de la Unión, Secretaría General, Secretaría de Servicios Parlamentarios, pp.68-69, de:
https://www.diputados.gob.mx/LeyesBiblio/pdf/CPF.pdf

Las empresas han sido cada vez más cuidadosas en cuanto a información interna y lo que se tiene como reservada, ejemplo en cadenas como *Kentucky Fried Chicken* (*KFC)* que está de por medio el éxito particular de ingredientes o *Coca Cola*, lo cual pareciera que la ley esta a su favor, sin embargo; en el mismo Código sigue teniendo mayor regulación hacia lo financiero, revelación de secretos que a la vida y dignidad de las personas, al no contar con mayor tipificación, sanciones y ayuda respecto a delitos *cibernéticos* de índole sexual. ¿Entonces, vale más el dinero que la vida, tranquilidad y salud de las personas?

Contamos en México con Instituciones como la Comisión Nacional de los Derechos Humanos (CNDH) y a nivel internacional todo lo que conlleva la protección del Sistema Interamericano de Derechos Humanos, sin embargo; es importante mencionar que el no contar con poder coercitivo, lo cual debe ser fundamental y parte de la composición de los mismos para que sus recomendaciones no sean prácticamente en vano porque la autoridad a quién va dirigida si quiere recibirlas o no es a voluntad y si decide tomarlas en cuenta o no, en la realidad se queda a consideración de las autoridades correspondientes, lo cual es un insulto a un Organismo pagado con impuestos de los mexicanos(as) y si los resultados (recomendaciones) no se acatan, cabe preguntarnos ¿debería seguir operando? Pero que:

> En México, la tipificación de los delitos informáticos está contemplada en diversas legislaciones federales y en el Código Penal Federal. Estas incluyen:
> Ley de Instituciones de Crédito
> Ley de Instituciones de Seguros y de Fianzas
> Ley del Mercado de Valores
> Ley General de Títulos y Operaciones de Crédito
> Ley Federal de Protección de Datos Personales en Posesión de los Particulares
> En el Código Penal Federal mexicano, se encuentra una sección específica, el Título Noveno, que aborda la revelación de secretos y el acceso ilícito a sistemas y equipos de informática. En su segundo capítulo se detallan las conductas tipificadas.
> Además, la Ley de Instituciones de Crédito también contempla sanciones para este tipo de ilícitos.
> Estas legislaciones federales y disposiciones en el Código Penal Federal establecen las bases legales para la persecución y sanción de delitos informáticos en México…
> Además, existe la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPP), que establece un tratamiento especial para información que, de divulgarse de manera indebida, afectaría la esfera más íntima del ser humano.

Dicha ley y el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI) garantizan el derecho de protección de datos personales.

¿Cuáles son los delitos informáticos en México en detalle?

1. Acceso ilícito a sistemas y equipos de informática

El artículo 211 Bis 1 del Código Penal Federal…

El artículo 211 Bis 2 sanciona las mismas conductas, pero "en sistemas o equipos de informática del Estado", mientras que el Bis 3 castiga las mismas conductas pero de quien esté "autorizado para acceder a sistemas y equipos de informática del Estado".

2. Objetivos financieros

En los artículos 211 Bis 4 y 5 del Código Penal Federal tipifican los mismos delitos, pero en sistemas o equipos de informática a las instituciones que integran el sistema financiero.

La Ley de Instituciones de Crédito, en su artículo 112 Quáter se castiga "a quien acceda a los equipos o medios electrónicos, ópticos o de cualquier otra tecnología del sistema bancario mexicano, para obtener recursos económicos, información confidencial o reservada, o altere o modifique el mecanismo de funcionamiento de los equipos o medios electrónicos, ópticos o de cualquier otra tecnología para la disposición de efectivo de los usuarios del sistema bancario mexicano".

En tanto, el artículo 112 Quintus añade una pena mayor si quien realice alguna de las conductas señaladas "tiene el carácter de consejero, funcionario, empleado o prestador de servicios de cualquier institución de crédito, o las realice dentro de los dos años siguientes de haberse separado de alguno de dichos cargos".

3. Ley Olimpia

El 3 de diciembre de 2019 se aprobó en el Congreso de la Ciudad de México la llamada "Ley Olimpia", un conjunto de reformas a códigos penales de las entidades federativas, así como a la Ley general de acceso de las mujeres a una vida libre de violencia.

Estas reformas reconocen la violencia digital como un tipo de delito que consiste en actos de acoso, hostigamiento, amenazas, vulneración de datos e información privada, así como la difusión de contenido sexual (ya sean fotos, videos o audios), sin el consentimiento o mediante engaños a una persona.

Para marzo de 2020, la Ley Olimpia ya estaba vigente en 16 estados de la República Mexicana: Puebla, Yucatán, Ciudad de México, Oaxaca, Nuevo León, Querétaro, Baja California Sur, Aguascalientes, Estado de México, Guerrero, Coahuila, Chiapas, Zacatecas, Veracruz, Guanajuato y Tlaxcala. Actualmente está en debate en Sonora y se espera que este mes ingrese como reforma al Código Penal de Tamaulipas.

4. Protección de datos personales

Si bien, cualquier particular, ya sea persona física o moral… puede tratar datos personales, todos ellos deben observar las disposiciones previstas en la ley.

Se define «tratamiento de datos personales» a cualquier operación que se realice con tus datos, desde su obtención, uso, divulgación, almacenamiento y hasta su cancelación y supresión.

Cabe señalar que no están sujetos a las disposiciones de esta ley: las sociedades de información crediticia (buró de crédito) debido a que ya se encuentran reguladas por la Ley de las Sociedades de Información Crediticia, así como quienes traten (personas físicas o morales) los datos con fines exclusivamente personales, sin afán

de divulgarlos o utilizarlos de manera comercial, como sería el caso del directorio telefónico de los amigos y contactos personales…
La normativa indica que se deben establecer y mantener las medidas físicas, técnicas y administrativas para proteger la información personal ante el daño, pérdida, alteración, destrucción o uso no autorizado…
En caso de incumplimiento se podrán imponer sanciones desde 100 a 320,000 días de multa y/o de tres meses a tres años de cárcel a cualquier persona autorizada para procesar datos personales que, con fines de lucro, provoque una violación de seguridad que afecte a las bases de datos; de seis meses a cinco años de cárcel a cualquier persona que, con el objetivo de obtener ganancias ilegales, procese los datos personales engañosamente.
Desde hace 40 años se habla de delitos informáticos
La referencia a los delitos informáticos se remonta a 1983, cuando se dieron los primeros intentos de establecer leyes asociadas a los crímenes informáticos.
La Organización para la Cooperación y el Desarrollo Económico (OCDE) designó en París a un comité de expertos para discutir los crímenes que tuvieran como centro a las computadoras y la necesidad de hacer cambios en los códigos penales.
La OCDE recomendó a los países miembros modificar su legislación penal para integrar este tipo de delitos. La legislación de los delitos informáticos en México se demoró casi 20 años, pero en los últimos años ha habido esfuerzos por actualizarse.
A nivel internacional, varios países han trabajado en actualizar sus marcos legales para abordar los delitos cometidos a través de medios electrónicos y tecnológicos.
En México, desde 1999 se han promulgado leyes a nivel federal para sancionar los delitos informáticos, incluyendo el Código Penal Federal, la Ley de Instituciones de Crédito y la Ley Federal de Protección de Datos Personales en Posesión de los Particulares. Esto refleja la importancia de abordar estos crímenes en el contexto digital actual y la necesidad de actualizar constantemente los marcos legales para enfrentar los nuevos desafíos tecnológicos.[43]

Lo importante de reconocer, legislar para erradicar y sancionar la violencia, como en este caso todo lo relacionado a lo digital (*cibernético*) muestra el tipo de sociedad y valores que se tienen, que desafortunadamente en países de Medio Oriente (como Afganistán, Irán, Irak, India, Palestina) una mujer(s), el ataque y la violencia hacia ellas va de la mano de una *cultura* machista (hasta sádica, sin empatía ni respeto a ningún tipo de vida) reprobable en *usos y costumbres* convenientes para hombres y adultos mayores que se aprovechan de ese poder de ellos ser quienes se juzgan a sí mismos y hacer que quieran, como si se tratará de un cuento y una realidad alterna a los derechos humanos, para no tener castigo alguno por conductas que en otros lugares se denominamos delitos, peor aún el uso de

[43]Maricela Ochoa Serafín, Delitos Informáticos en México. Conozca las leyes y las multas, DIGIXEM 360, Digital for Empowerment, 01 Dic 2023, *op. cit.*

costumbres dadas por los mismos que violentan hacen evidente el paso del tiempo en nada hará justicia para el género femenino.

Los ataques *cibernéticos* hacia hombres y mujeres, pero que han sido mayormente difundidos hacia mujeres, representa no solo logro del movimiento feminista, sino el triunfo de una sociedad para que no se repitan nunca más, porque es imperdonable que no se considere la conducta psicópata detrás de un medio o red digital, siendo capaz de destruir la vida de las personas, que si bien no por dinero, sino por *venganza* que nos hace cuestionar ¿cómo se encuentra nuestro país respecto a salud mental? Que no es importante y menos prioridad para nuestros gobernantes pone atención y plantear acciones reales para mejora de los ciudadanos.

Los delitos informáticos pueden sonar muy familiares para las autoridades judiciales de nuestro país, ya que existen casos de paraísos fiscales, por ejemplo Panamá que opera a través de internet desde otras partes del mundo, pero como es dinero, puede no ser tan relevante si proviene del crimen organizado o cuando se incauta como en el caso de *Zhenli Ye Gon*, quién fue el empresario que en 2007 se le decomisaron millones de dólares en efectivo y casualmente nadie pudo dar explicación veras de dónde esta ese dinero, quién se lo llevó o quiénes participaron en ello.

2.2. LEGISLACIÓN EN LA CIUDAD DE MÉXICO (CDMX).

Si bien el Código Penal de la Ciudad de México señala:

> ARTÍCULO 179 BIS.- Se impondrá de cuatro a seis años de prisión y de 500 a 1000 Unidades de Medida y Actualización a quien haciendo uso de medios de radiodifusión, telecomunicaciones, informáticos o cualquier otro medio de transmisión de datos, contacte a una persona menor de dieciocho años de edad, a quien no tenga capacidad de comprender el significado del hecho a persona que no tenga capacidad para resistirlo y le requiera o comparta imágenes, audio o video de actividades sexuales explícitas, actos de connotación sexual o le solicite un encuentro sexual.[44]

El cuidado legal hacia los menores es fundamental, en especial en una era donde la tecnología puede ser instrumento para quienes cometen delitos, porque la incorporación de la mujer (que anteriormente se dedicaba únicamente al cuidado de los hijos y todo lo referente al hogar) a más puestos de trabajo ha traído un precedente importante para la lucha, respeto hacia ellas, capacidades e independencia económica.

También al salir de casa, los hijos en muchas ocasiones al quedarse solos y sin orientación, son presas fáciles de sitios en internet para *conocer* a alguien, grupos de *chat*, citas amorosas u ofertas laborales no reguladas por las autoridades han desencadenado lamentables situaciones de desaparecidos, víctimas de múltiples vejaciones en donde más allá de que algunos (as) logren escapar y alzar la voz, lo grave es que incluso el artículo 179BIS no repondrán la vida o daño a la(s) persona(s) en caso de que se aplique la ley, sonando tan común y cotidiano que pasa imperceptible a miles de personas, que a diario van normalizando la impunidad o víctimas como cifras en medios de comunicación y digitales.

[44]Código Penal para el distrito Federal, Publicada en la Gaceta Oficial de la Ciudad de México el 16 de julio de 2002, texto vigente, Última reforma publicada en la G.O. CDMX el 19 de febrero de 2024, Gobierno de la Ciudad de México, Asamblea Legislativa del Distrito Federal, II Legislatura, p.58.

Hoy en día con la exposición a redes sociales y los denominados *influencers* la moda se ha vuelto vivir en apariencia, donde no todo o nada de lo que se ve es real. ¿Cuántas situaciones de abuso, de aparentes relaciones son ideales o perfectas? Después delitos que precisamente se han cometido a través de redes sociales, videos de personas que se conocieron por redes sociales como en el año 2018 el caso de *Grace Millane* quien era una mujer británica que conoció a un hombre por medio de una aplicación, acordaron verse, después acudieron a cenar, posteriormente entraron a un hotel y ella terminó dentro de una maleta, lo que fue la última vez que se registra en vida mediante cámaras de video. Esta apariencia en red social ocultaba a un hombre con antecedentes de violencia sexual y a quien se le probó haber realizado búsquedas en internet para deshacerse de un cuerpo y se le denominó *el monstruo de Tinder*.

Incluso el caso de Gisele Pelicot (una mujer francesa que fue víctima de violación, prostitución y drogas por parte de su esposo Dominique Pelicot) que gracias a utilizar de forma positiva las redes sociales y medios de información digitales se ha podido difundir el atroz caso que nos hace cuestionar más allá del esposo, ¿cómo tantas *personas* accedieron a cometer estos abusos, incluso sin pago? Un caso que nos hace reflexionar sobre delitos *cibernéticos* que abarcan desde concretar citas, difusión, compartir imágenes y videos con abusadores, pero sobre todo nos deja la lección como lo mencionó Gisele *la vergüenza debe cambiar de bando*, hacia los abusadores, no en la víctima que además debe cargar con lo emocional y psicológico que la ley debe en medida de lo posible hacer justicia (porque casos como este ¿podría realmente hacerse justicia?), es por ello que el:

> CAPÍTULO VII
> CONTRA LA INTIMIDAD SEXUAL
> ARTÍCULO 181 QUINTUS.- Comete el delito contra la intimidad sexual:
> I. Quien videograbe, audiograbe, fotografíe, filme o elabore, imágenes, audios o videos reales o simulados de contenido sexual íntimo, de una persona sin su consentimiento o mediante engaño.
> II. Quien exponga, distribuya, difunda, exhiba, reproduzca, transmita, comercialice, oferte, intercambie y comparta imágenes, audios o videos de contenido sexual íntimo de una persona, a sabiendas de que no existe consentimiento, mediante materiales impresos, correo electrónico, mensajes telefónicos, redes sociales o cualquier medio tecnológico.

> A quien cometa este delito, se le impondrá una pena de cuatro a seis años de prisión y multa de quinientas a mil unidades de medida y actualización. La pena se agravará en una mitad cuando:
> I.La víctima sea una persona ascendiente o descendiente en línea recta, hasta el tercer grado;
> II.Cuando exista o haya existido entre el activo y la víctima una relación de matrimonio, concubinato, sociedad de convivencia, noviazgo o cualquier otra relación sentimental o de hecho, de confianza, docente, educativo, laboral, de subordinación o superioridad;
> III.Cuando aprovechando su condición de persona responsable o encargada de algún establecimiento de servicio al público, realice alguna de las conductas establecidas en el presente artículo;
> IV.Sea cometido por alguna persona servidora pública o integrante de las instituciones de Seguridad Ciudadana en ejercicio de sus funciones;
> V. Se cometa en contra de personas adultas mayores, con discapacidad, en situación de calle, afromexicanas o de identidad indígena.
> Este delito se perseguirá por querella.[45]

Actualmente un tema penal que hace años se difundió más como morbo o chisme que con la gravedad de delitos que se cometieron, sin empatizar con las víctimas, sin apoyo por parte de la sociedad, ni de las autoridades incluso para realizar su denuncia (muchas de ellas siendo menores de edad y con hijos en brazos) y no minimizar el caso para solo tomarlas como testigo, para evitar que él presunto culpable contra la intimidad sexual, esclavitud, delitos de trata y hoy en día gracias a las redes sociales por una parte se hace justicia al darle voz a los testimonios de víctimas (que en ese tiempo no) pero también a *ciberviolencia* porque se quiere indagar en su pasado para hacerlas ver como personas interesadas que por estar dispuestas al *precio de la fama*, se convirtieron esclavas sexuales de Sergio Andrade, el conocido promotor de cantantes, sin detenernos como sociedad a escuchar lo que estas jóvenes (en ese entonces) declaraban públicamente, narraban de forma objetiva, de delitos, torturas y tratos crueles inhumanos y degradantes que vivieron, no como una noticia del medio del espectáculo ¿no sonaba alarmante menores de edad con bebés de un mismo hombre levantando la voz ante abuso de poder?.

[45]Código Penal para el Distrito Federal, Publicada en la Gaceta Oficial de la Ciudad de México el 16 de julio de 2002, Última reforma publicada en la G.O. CDMX, el 19 de febrero de 2024, Gobierno de la Ciudad de México, pp.60-6, *op. cit.*

¿Por qué mencionar este tema? Porque la *cibervilencia*, los vacíos y beneficios legales o favores jurídicos del lado del agresor (por negligencia, conflicto de interés o por política de lado de su hermano hoy bajo el cobijo de un partido político que habla de la no corrupción y actualmente en el poder) son lo que tienen hoy en día al Estado mexicano demandado ante la Corte Interamericana de Derechos Humanos y a los presuntos responsables, al igual que en los Estados Unidos de Norteamérica (E.U.A) porque México no hizo justicia, ni siquiera abrió las carpetas de investigación para por lo menos once víctimas que mencionaban tortura y esclavitud fueran escuchadas y se siguiera el proceso, tampoco se informó que el juez en ese entonces a cargo no debía serlo por ser esposo de la fiscal del caso, lo cual ya es un grave conflicto de interés, como si en el país los feminicidios, violencia y *ciberviolencia* no fueran suficientes públicos los casos y negligentes las investigaciones.

Pero la *ciberviolencia* hacia testimonios de víctimas, la falta de empatía y violencia para señalarlas por no salir de esa situación ejemplifica lo que la *ciberviolencia* puede hacer en redes sociales, porque más allá del señalamiento de que ¿dónde estaban sus padres, por fama y dinero se sometieron a todo tipo de violencia y demás comentarios? nada justifica la esclavitud ni la trata de personas y menos que la sociedad ejerza *ciberviolencia* hasta para los hijos de las sobrevivientes, el cuerpo no está a la venta y hasta que esto no se tome con seriedad, difícilmente cambiaremos un sistema machista porque el tema no es el agresor o si la víctima es o no es por parte de la sociedad, sino el constante ataque a ellas, la falta de justicia y evidente corrupción de por medio sin poner en primer lugar los delitos y el combate por cualquier tipo de violencia.

Existe una línea muy delgada entre sexualidad y violencia, que sin duda la negativa es determinante, pero también existen situaciones donde las personas pueden ser incluso más vulneradas como por ejemplo ponerles algo en su bebida, en un bar o lo sucedido en el Estado de Puebla donde se clamaba justicia por droga inyectada mediante jeringas y que en redes sociales estuvieron presentes (difundido) en 2022

o en Ciudad de México en el Sistema de Transporte Colectivo Metro (en estaciones como Martín Carrera, Barranca del Muerto, Mixcoac, San Antonio, Indios Verdes y Ermita) que sujetos seguían a mujeres, tomaban videos y como estrategia se comenzaron a implementar *medidas en el metro* para mayor seguridad de ellas, entre testimonios de las mismas y del *modus operandi* hacia las autoridades para estar más alerta, pero se vuelve tangible en lo judicial, sino que pasa inadvertido a las víctimas reales sin justicia ni reparación del daño y falta de investigación.

La incorporación de los delitos anteriores al Código Penal como parte específica de delitos digitales debe ser fundamental en la era actual y futura, donde la tecnología forma parte de nuestro día a día y más en temas que las leyes no han complementado como lo es en la *ciberviolencia*, sobre todo los que son de tipo y connotación sexual, por ejemplo; uno de los delitos más difíciles de probar y perturbadores para la(s) víctima(s) es el:

> CAPÍTULO III
> ACOSO SEXUAL
> Artículo 179 BIS.- Se impondrá de cuatro a seis años de prisión y de 500 a 1000 Unidades de Medida y Actualización a quien haciendo uso de medios de radiodifusión, telecomunicaciones, informáticos o cualquier otro medio de transmisión de datos, contacte a una persona menor de dieciocho años de edad, a quien no tenga capacidad de comprender el significado del hecho a persona que no tenga capacidad para resistirlo y le requiera o comparta imágenes, audio o video de actividades sexuales explícitas, actos de connotación sexual o le solicite un encuentro sexual.
> CAPÍTULO VII
> CONTRA LA INTIMIDAD SEXUAL
> Artículo 181 Quintus. Comete el delito contra la intimidad sexual:
> I. Quien videograbe, audiograbe, fotografíe, filme o elabore, imágenes, audios videos reales o simulados de contenido sexual íntimo, de una persona sin su consentimiento o mediante engaño.
> II. Quien exponga, distribuya, difunda, exhiba, reproduzca, transmita, comercialice, oferte, intercambie y comparta imágenes, audios o videos de contenido sexual íntimo de una persona, a sabiendas de que no existe consentimiento, mediante materiales impresos, correo electrónico, mensajes telefónicos, redes sociales o cualquier medio tecnológico.
> A quien cometa este delito, se le impondrá una pena de cuatro a seis años de prisión y multa de quinientas a mil unidades de medida y actualización.
> La pena se agravará en una mitad cuando:
> I. La víctima sea una persona ascendiente o descendiente en línea recta, hasta el tercer grado;

> II. Cuando exista o haya existido entre el activo y la víctima una relación de matrimonio, concubinato, sociedad de convivencia, noviazgo o cualquier otra relación sentimental o de hecho,
> de confianza, docente, educativo, laboral, de subordinación o superioridad;
> III. Cuando aprovechando su condición de persona responsable o encargada de algún establecimiento de servicio al público, realice alguna de las conductas establecidas en el presente artículo;
> IV. Sea cometido por alguna persona servidora pública o integrante de las instituciones de Seguridad Ciudadana en ejercicio de sus funciones;
> V. Se cometa en contra de personas adultas mayores, con discapacidad, en situación de calle, afromexicanas o de identidad indígena.
> Este delito se perseguirá por querella.[46]

El acoso sexual si bien la ley nos muestra los elementos del tipo penal, lo cierto es que las pruebas y los encargados de ayudar a las víctimas (autoridades correspondientes a quienes se acude a denunciar y quienes deberían aplican la ley) en muchas ocasiones no cuentan con el conocimiento y menos interés, ni empatía para asistir a la víctima, esto porque México tiene implícito el sello de cultura machista que se suma a la revictimización en probar prácticamente el delito por parte de la víctima, sin reparar su salud mental, sanción (física o psicológica) y se le haga justicia, desde las terapias psicológicas al acudir a denunciar porque pareciera que en el Ministerio Público (MP) y la Fiscalía existe una escala o parámetro de qué delito es más importante que el otro(s) para intentar dar seguimiento y no es darle seguimiento e investigación a todos los delitos, incluidos los *cibernéticos* sin distinción alguna.

El desgaste emocional y la exposición de la víctima, representa continuidad al delito porque culturalmente se le da voz al dicho de todos, menos de quién sufrió o sigue sufriendo el delito.

[46]Código Penal para el Distrito Federal, Publicado en la Gaceta Oficial del Distrito Federal el 16 de julio de 2002, Cámara de Diputados del H. Congreso de la Unión, Secretaría General, Secretaría de Servicios Parlamentarios. Última reforma publicada en la Gaceta Oficial de la Ciudad de México el 29 de julio de 2020, pp. 47,49-50, de: https://www.congresocdmx.gob.mx/media/documentos/9cd0cdef5d5adba1c8e25b34751cccfdcca80e2c.pdf

Sumado a ello, la burocracia en todo el proceso, como por ejemplo; las horas al declarar, falta de interés a situaciones de vulnerabilidad de quién acude a denunciar, miedo, intimidación, amenazas de que puede estar sujeta(o) son situaciones que en las autoridades y la ley quedan a la buena fe de quiénes imparten justicia.

El acoso puede ser tan grave para una víctima que minimizar el daño, resulta la fórmula perfecta del violentador con una sociedad que su negligencia fomenta cubrir, encubrir desde la familia hasta los cercanos y autoridades sin pensar que nadie está exento de toparse con un psicópata a lo largo de su vida en cualquier ámbito y si tienen suerte y nos son presas de estas personas mentalmente insanas podrán seguir con su vida adelante.

Es importante que no sólo se impartan cursos, capacitación o se incorporen mayor número de elementos femeninos en los órganos de justicia, es primordial que se realicen exámenes psicológicos que realmente prueben contar con empatía hacia una víctima, porque tan difícil resulta que se investigue una desaparición o feminicidio que entonces el acoso hace imposible auxiliar para obtener justicia porque si un cuerpo para la justicia es motivo de investigación, justicia y aplicación de la ley, menos lo será otro tipo de delito de índole digital que el daño no es notorio a simple vista como en la violencia física.

> La violencia digital contra las mujeres y niñas mediante las redes sociales (también conocida como ciberviolencia), puede tener diversas manifestaciones como el ciberbullying, el sexting, el stlaked, el grooming, el shaming y el doxing, algunos otros ejemplos son la difusión, sin el consentimiento de la víctima, de sus datos e imágenes personales, amenazas, difamaciones, acoso, humillación, ataques que afectan la libertad de expresión de las mujeres, entre otras.
> Además de las redes sociales, los medios que se utilizan como vía para ejercer ciberviolencia son: plataformas de internet, teléfonos móviles, mails, mensajes de texto, fotografías, videos, chats, páginas web, videojuegos, a través de los medios de comunicación también se generan contenidos que representan violencia contra las mujeres. Cabe destacar que el anonimato que algunas plataformas digitales ofrecen, es una condición que utilizan a su favor la(s) persona(s) agresora (s), incluso algunas utilizan nombres y perfiles falsos en redes sociales.
> La violencia digital mediante redes sociales contra las mujeres y niñas representa un obstáculo para su acceso seguro a las comunicaciones e información digital,

> genera consecuencias psicológicas, emocionales y sociales para las víctimas y limita el pleno uso, goce y disfrute de sus derechos humanos.
> Es importante recordar que no se debe culpar a las niñas y mujeres que son víctimas de violencia mediática a través de internet. Ninguna mujer busca, induce ni provoca actos violentos hacia ella en plataformas digitales, su vida, libertad e integridad debe ser respetada en la vida offline y online.[47]

Cuando nos referimos a violencia digital, se cree que sólo abarca a ciertas personas y se juzga desde la forma de vestir, peinarse, el horario de estar en la calle, si ha salido o no con varias personas y peor aún se señala por haber estado con alguien (como si la victima adivinara el futuro y comportamiento de la otra persona lo cual es absurdo porque los (as) violentadores (as), psicópatas (o con trastornos mentales o el futuro acosador y hostigador digital no van con un letrero que digan que lo son, contrario a ello usan mascaras ante la sociedad y futuras víctimas) como si la víctima fuera consciente de su historial de vida, antecedentes y que pese a ese conocimiento decidió estar con alguien que ejerce violencia sin entender que la víctima no eligió serlo ni sufrir violencia de cualquier tipo.

En muchas ocasiones la falta de información y red de apoyo principalmente por parte de la familia hace el escenario perfecto para quien acosa porque este sabe que valiéndose de un país machista cualquier cosa que diga o haga para humillar y denigrar a la mujer quien violente será más válido que lo expuesto por la víctima.

Sumado a lo anterior, cabe aclarar que la sociedad pierde de vista que las redes de apoyo cercanas son lo que ayudarán a que la(s) persona(s) pueda salir de la violencia o permanezca, porque podría el miedo ser tan fuerte (como una cárcel mental) hacia el agresor que prefiere la víctima aguantar y dejar de luchar hasta para proteger a su familia de algún daño por parte de su agresor, es por ello que la salud mental vaya de la mano con el avance de las leyes y justicia para quienes padecen delitos.

[47]Secretaria de las Mujeres, Gobierno de la Ciudad de México, *Visibilización y prevención de la violencia cibernética contra las mujeres y niñas*, 2024, de:
https://www.semujeres.cdmx.gob.mx/violencia-cibernetica-contra-mujeres

Desde las personas y redes cercanas de quien se están realizando comentarios ofensivos, mal intencionados, refiriéndose a otro(a) para humillar o difamar con mensajes que llegan como virus en publicaciones sobre la incitación a violencia, hablar mal de otra persona y peor aún de seguir cercano a una persona que ejerce *ciberviolencia* por más amistad que se tuvo y se refiere, publica situaciones de la vida de su ex pareja también es una señal de alarma y de cuestionarnos que tan mal esta la sociedad que tolera estas situaciones.

Lo anterior, nos da un panorama muy amplio dela sociedad permite y tolera violencia y *ciberviolencia*, que estas actos no son impedimentos para seguir cerca de alguien que comente delitos, ya sea como amistad, conocido incluso familiar}, de igual forma en los ámbitos académicos y laborales poder convivir con quien sea violentador(a) nos permite cuestionar no sólo a quien ejerce violencia, sino a la sociedad porque cómo pasar por alto agresiones, incluyendo las digitales, sólo por ser aparentemente una *amistad* que nadie mejor que la expareja puede conocer ya que difícilmente una amistad se expondría a mostrarse tal cual es.

Un violentador (a) no tiene un letrero que dice lo es, tampoco tiene una apariencia de ogro (como en caricaturas, ciencia fincción, películas o series) puede ser incluso un *excelente vecino(a)*, compañero(a) o familiar.

Tenemos desafortunadamente como mal ejemplo, el artículo 209, respecto a las amenazas, en donde:

> ARTÍCULO 209. Al que amenace a otro con causarle un mal en su persona, bienes, honor o derechos, o en la persona, honor, bienes o derechos de alguien con quien esté ligado por algún vínculo, se le impondrá de tres meses a un año de prisión o de noventa a trescientos sesenta días multa. La pena se agravará al triple cuando la amenaza consista en difundir, exponer, distribuir, publicar, compartir, exhibir, reproducir, intercambiar, ofertar, comerciar o transmitir, mediante materiales impresos, correo electrónico, mensaje telefónico, redes sociales o cualquier medio tecnológico; imágenes, audios o videos de contenido sexual íntimo de una persona sin su consentimiento u obtenido mediante engaño. Se entenderá como personas ligadas por algún vínculo con la víctima: a) A las personas ascendientes y descendientes consanguíneas o afines; b) La persona cónyuge, la concubina, el concubinario, pareja permanente y parientes colaterales por consanguinidad hasta el cuarto grado y por afinidad hasta el segundo; y c) Las personas que estén ligadas

> con las víctimas por amor, respeto, gratitud o estrecha amistad. Este delito se perseguirá por querella.[48]

Al tratarse de un delito por *querella*, la agonía para la víctima continúa ya que por miedo, temor o amenazas hacia ella (él) o su familia podría retractarse o decidir no continuar con la denuncia, por lo que debe ser un delito perseguido de oficio ya que de lo contrario existen muchas situaciones por las que no se sigue adelante, incluyendo lo psicológico y físico.

Lo grave es que para este momento (sufrió el delito y se continua) la persona ya se encuentra en un estado de *trance hipnótico*[49] por lo que difícilmente tendrá energía para poder ver más allá de la situación difícil y con fuerza continuar un proceso legal que será más complicado si nunca tuvo apoyo psicológico.

La ley no contempla la situación psicológica de quien es víctima ni como tampoco los trastornos mentales derivados de haber pasado por una situación de violencia y *ciberviolencia*, por lo tanto sin empatía y apoyo para la víctima, es respaldar a quien agrede y pueda continuar destrozando la vida de la(s) persona(s), utilizando todo a su alcance, como redes sociales, buscador en internet, crear perfiles falsos para amenazar o dañar a su círculo cercano y querer hacer ver a la víctima, crear difamación, hacer creer que la víctima está mal de sus facultades, como si fuera la víctima quien es culpable de distorsionar la realidad a su alrededor y se continue el delito, aunque no esté físicamente quien agrede, el mismo medio violente y revictimice. Lo que se convierte en una jugada perfecta porque ya no sólo fue víctima del agresor(a) sino el entorno y de las mismas autoridades.

[48]Código Penal para el Distrito Federal, Publicado en la Gaceta Oficial del Distrito Federal el 16 de julio de 2002, p.61, Última reforma publicada en la Gaceta Oficial de la Ciudad de México el 29 de julio de 2020, op.cit.
[49]Se le denomina de esta forma para hacer referencia en psicología que la conciencia de la persona ya esta en hipnosis, generalmente por un psicópata.

Es fundamental que se tenga mayor información respecto a los trastornos y enfermedades mentales para poder detectar e incorporar a la sanción justicia penal en los delitos como por ejemplo en el pago de terapias a quienes fueron víctimas y ahora supervivientes (si bien la ley lo contempla, lo cierto es que en muchas ocasiones la víctima ni siquiera llega a este momento porque la revictimización se sigue desde el momento en que intenta poner su denuncia sin que se integre una la carpeta de investigación o peor no se le toma su denuncia) lo cual resulta desafortunado aún más por parte de legisladores y jueces no existe interés real en los delitos de *ciberviolencia* y las víctimas no cuenten como personas con derechos, sino de intenta dejar en situaciones de redes y no como un delito grave en la vida real de la(s) persona(s).

2.3. LEYES EN CONTRA DE LOS DELITOS DIGITALES EN MÉXICO.

La violencia a lo largo de la historia no sólo en México, sino en el mundo ha sido constante, desde colonizar un territorio, intimidar para obtener algo, defenderse en tiempos donde prevalecían las luchas (como la primera y segunda guerra mundial) pero también para abusar y utilizar la violencia como parte de la vida cotidiana en un estado de derecho o en conflictos armas, se ha disfrutado y normalizado el abuso como muy comúnmente ocurre en nuestro país en formas muy sutiles aparentemente e imperceptibles, pero psicológica y *cibernéticamente* igual de agresivas y eficaces para terminar con la vida de una(s) persona(s).

Un país a lo largo de los años marcado la por violencia que se ha ido matizando de lo físico a lo psicológico, pero *evolucionado* con la era digital y redes sociales en delitos que se van evidenciando con alzar la voz de quienes han tenido que padecerlos, para evidenciar los delitos, se hable más de ello y se plasme en la ley.

El reto sigue significando lucha y empatía en medios digitales para no permitir la *ciberviolencia*, darle buen uso a la tecnología y que las redes sociales sirvan como canales de información, comunicación efectiva en tiempo real, pero no para ejercer violencia contra nadie.

En el caso de muchas mujeres que realmente son víctimas (no aquellas que usan el derecho para obtener algo) se ha manifestado:

> **Violencia cibernética** contra las mujeres:
> **Violar la intimidad de las mujeres** al filtrar imágenes y/o videos ya sea realizando algún acto sexual o exhibiendo su cuerpo semidesnudo o desnudo, sin su consentimiento.
> **Sembrar rumores falsos y difamar** a alguna mujer con el propósito de dañar su reputación y buscar avergonzarla en su red social ante sus familiares, amigos y/o conocidos.
> **Crear perfiles falsos y/o usurpar la identidad** de alguna para subir fotos, hacer comentarios ofensivos o hasta ofertas sexuales.
> **Denigrar a mujeres** al difundir fotos, "memes" y/o grabaciones en donde se busque intimidar, agredir, humillar o ridiculizar, denigrar. Asimismo, filmar a través de teléfonos celulares o cámaras digitales actos de violencia en donde se golpea, agrede, grita o persigue a una persona de sexo femenino.

> **Acechar o espiar** (stalked) las publicaciones, comentarios, fotos y todo tipo de información de una mujer en sus cuentas de redes sociales. Esta modalidad puede ir de una simple indagación hasta el deseo de relacionarse con la víctima para intimidarla y acosarla sexualmente.
> **Acoso y amenaza** mediante el envío de imágenes con contenidos sexuales y/o mensajes agresivos y hostigadores en cuentas de correo electrónico, mensajería telefónica o redes sociales de las víctimas; así como intimidar a una mujer con la intención de golpearla, abusarla sexualmente y/o matarla si no accede a sus deseos.[50]

Los denominados *memes*[51] en redes sociales como supuestas bromas o con fines de chistes también se han vuelto en contra de lo que parecía *divertido* porque al tener un teléfono para captar cualquier momento y publicarlo, se ha olvidado la sociedad del impacto, imagen y reputación de quién sin autorización es la burla en internet, sin importar que afecte a su salud mental, emocional, familia, trabajo y vida mediante la reproducción de miles y miles de veces en segundos de una escena que puede o no ser verdad, aunque con el daño irreparable sin detenernos a pensar si es real o el daño que puede estar sufriendo quien lo padece.

Lo anterior, porque todo aquello que denigre, humille o ridiculice a alguien debería ser motivo suficiente que se castigue para evitar que se propague y las leyes deberían contar con mecanismos para que inmediatamente la policía *cibernética* los elimine, de igual forma comentarios en redes sociales y el acoso a una víctima no ha sido tomados con seriedad por las leyes, ni por la sociedad que cada día esta más al alcance de nueves generaciones que normalizan la violencia digital, contrario a la libertad de expresión que es la justificación para la *ciberviolencia*, cuando no se ha entendido la línea tan delgada que se ha perdido la dimensión en que puede afectar cualquier acción de nuestra parte.

[50]Secretaria de las Mujeres, Gobierno de la Ciudad de México, Prevención y visibilización del ciberacoso contra las mujeres y niñas, ¿Qué es la violencia cibernética contra las mujeres?, 2024, de: https://www.semujeres.cdmx.gob.mx/violencia-cibernetica-contra-mujeres/identificala

[51]Término que se utiliza para hacer referencia a poner situaciones de la realidad en forma de caricatura y causar risa de situaciones de la vida real que se difunde por internet.

Existen casos de violencia por parte de ex parejas de quienes trabajan en el Poder Judicial, como Mariel Albarrán, donde sus hijos fueron violentados por su padre y pese al abuso sexual no existe justicia por quién fue su pareja Manuel Horacio Cavazos López (ex Magistrado del Tribunal Superior de Justicia de la Ciudad de México, TSJCDMX)[52] que ha usado el poder, influencias y relaciones que le han permitido no se haga justicia, mostrando que la ley y el castigo es para algunos (la mayoría y que no cuenta con poder adquisitivo).

No se trata únicamente de contar con leyes, sino su correcta aplicación porque entonces estamos hablando de que algunos ciudadanos tienen, otros no, derechos como si se tratara de privilegio de alguno(s) no de todos y que ha sido la lucha constante para mejorar en leyes, mecanismos, protocolos y justicia en las mismas sea invisible.

La violencia no significa un determinado género, estrato social ni economía porque escala a cualquier nivel, sobre todo la psicológica y digital que puede ser imperceptible para la mayoría o todos fuera de la víctima que continúan sin darle importancia y reproduciendo aparentes *memes*, creerle a una persona es el primer paso porque:

> La violencia digital mediante redes sociales (ciberviolencia) contra las mujeres y niñas representa un obstáculo para su acceso seguro a las comunicaciones e información digital, genera consecuencias psicológicas, emocionales y sociales para las víctimas y limita el pleno uso, goce y disfrute de sus derechos humanos.
> Es importante recordar que no se debe culpar a las niñas y mujeres que son víctimas de violencia mediática a través de internet. Ninguna mujer busca, induce ni provoca actos violentos hacia ella en plataformas digitales, su vida, libertad e integridad debe ser respetada en la vida offline y online.
> **Otras definiciones sobre ciberviolencia**
> La Organización de Naciones Unidas lo define como un comportamiento violento en línea que va dese el acoso en línea y el agravio público hasta el deseo de infligir daño físico, incluidos los ataques sexuales, los asesinatos y los suicidios inducidos
> La *Ley de Acceso de las Mujeres a una Vida Libre de Violencia CDMX*, incluye a la **violencia mediática** como aquella publicación o difusión de mensajes e imágenes

[52]El País, *La mujer que denunció a su exesposo por atacar sexualmente a sus hijas gana un amparo con el que podrá reabrir el caso*, México - 06 OCT 2021, de: https://elpais.com/mexico/2021-10-06/la-mujer-que-denuncio-a-su-exesposo-por-atacar-sexualmente-a-sus-hijas-gana-un-amparo-con-el-que-podra-reabrir-el-caso.html

estereotipados a través de cualquier medio de comunicación local, que de manera directa o indirecta promueva la explotación de mujeres o sus imágenes, injurie, difame, discrimine, deshonre, humille o atente contra la dignidad de las mujeres, como así también la utilización de mujeres, adolescentes y niñas en mensajes e imágenes pornográficas, legitimando la desigualdad de trato o construya patrones socioculturales reproductores de la desigualdad o generadores de violencia contra las mujeres.

Es **violencia cibernética** contra las mujeres:

Violar la intimidad de las mujeres al filtrar imágenes y/o videos ya sea realizando algún acto sexual o exhibiendo su cuerpo semidesnudo o desnudo, sin su consentimiento.

Sembrar rumores falsos y difamar a alguna mujer con el propósito de dañar su reputación y buscar avergonzarla en su red social ante sus familiares, amigos y/o conocidos.

Crear perfiles falsos y/o usurpar la identidad de alguna para subir fotos, hacer comentarios ofensivos o hasta ofertas sexuales.

Denigrar a mujeres al difundir fotos, "memes" y/o grabaciones en donde se busque intimidar, agredir, humillar o ridiculizar, denigrar. Asimismo, filmar a través de teléfonos celulares o cámaras digitales actos de violencia en donde se golpea, agrede, grita o persigue a una persona de sexo femenino.

Acechar o espiar (stalked) las publicaciones, comentarios, fotos y todo tipo de información de una mujer en sus cuentas de redes sociales. Esta modalidad puede ir de una simple indagación hasta el deseo de relacionarse con la víctima para intimidarla y acosarla sexualmente.

Acoso y amenaza mediante el envío de imágenes con contenidos sexuales y/o mensajes agresivos y hostigadores en cuentas de correo electrónico, mensajería telefónica o redes sociales de las víctimas; así como intimidar a una mujer con la intención de golpearla, abusarla sexualmente y/o matarla si no accede a sus deseos.[53]

Cuando vemos alguna publicación, imagen, vida o comentario en redes sociales, es tan difícil separar el sentido de veracidad y mentira de lo que en realidad es cierto porque el prejuzgar a las personas desde tiempos como la Santa Inquisición es suficiente un motivo que es igual a rumor para matar o torturar a una persona que no dista de la actualidad y la realidad, aunque pueda parecer extremo, sucede ese mismo linchamiento pero en redes sociales, que se han vuelto parte de nuestra vida porque vivimos en una realidad virtual como en videojuegos y *avatars*[54] que forman parte de un submundo que se ha vuelto nuestra vida real.

[53]Secretaria de las Mujeres, Gobierno de la Ciudad de México, Prevención y visibilización del ciberacoso contra las mujeres y niñas, ¿Qué es la violencia cibernética contra las mujeres?, 2024, *op. cit.*

[54]Son representaciones virtuales de personas reales en un entorno digital.

Que al igual que en la realidad virtual se dan delitos (videojuegos con violencia, armas y prostitución) como si se tratara de cualquier cosa.

La *ciberviolencia* se ha *normalizado* como cuando se comenzaban a dar las primeras noticias de decapitados, muertos y desollados en vía pública, justificada como lucha entre cárteles de narcotráfico, pero empezó a escalar tanto la virtual que hoy en día hemos permitido vivir en esa violencia en el mundo tan normalizada.

Desafortunadamente, la violencia no se abordó en los debates presidenciales, tampoco en propuestas reales de cómo erradicar esto, peor aún las múltiples denuncias a integrantes de la política directamente con el crimen organizado como las realizadas a Omar García Harfuch no fueron importantes (además de otros casos y personajes) que hoy que han concluido las elecciones y tenemos a la presidenta de México donde en parte del del gabinete (más allá de que la *cuarta transformación* en múltiples ocasiones expresará que supuestamente ellos no son ni aceptan a corruptos como en el pasado) con integrantes de todo aquello que se criticó ¿cómo confiar en una nueva realidad cuando sólo cambian de partidos y siguen vigentes con otro color como si se tratará de un equipo de *fútbol*? Pero terminar con la *ciberviolencia*, proteger a víctimas y leyes realmente ejemplares para no querer cometer esto no sea un tema importante, tan irrelevante para el Poder Judicial, política, leyes y la conciencia en la sociedad.

2.3.1.- Ley de Acceso de las Mujeres a una Vida Libre de Violencia.

México en el discurso se ha manifestado a favor de los derechos humanos y en la Ciudad de México con leyes para mejorar y evitar la violencia (anuncios en transporte público rechazando cualquier conducta de acoso, artículos, sanciones o números para llamar) pero acaso ¿la población está más segura, siente confianza de las autoridades o de poder denunciar en caso de cualquier delito sin sentirse y ser revictimizado(a)?

Si lo anterior fuera afirmativo, podríamos transitar libre y tranquilamente en cualquier lugar, no se necesitaría vivir con cámaras que aparentemente y supuestamente (porque cuando sucede un delito y se requieren como evidencia casi por no mencionar nunca sirven) graban cualquier situación (como un ojo que nos vigila las 24 horas del día) y al momento de denunciar, los ciudadanos(as) se topan con respuestas tan comunes como: *no servía la cámara, justo en ese momento dejo de grabar, en ese ángulo no se alcanza a ver* y que se pagan con los impuestos de los ciudadanos.

Las leyes siempre van a ser importantes, fundamentales para vivir y coexistir en sociedad, pero es indispensable su justa y correcta aplicación a todos(as) sin que el dinero o algún interés económico o político haga la diferencia entre obtener o no justicia, como si se tratará de víctimas de primer y segundo nivel porque la justicia es la diferencia en una verdadera sociedad y estado de derecho.

La Ley de Acceso de las Mujeres a una Vida Libre de Violencia debe significar no sólo que las mujeres sino todas las personas tengan una vida sin violencia, física, psicológica, *cibernética*, las redes y medios digítales mediante su regulación hagan eco para justicia y no tener en el caso de quienes tienen hijos siempre con la preocupación de qué ven los menores por el tipo de contenido que implique violencia y *ciberviolencia*.

Que todos(as) obtengan justicia ya sea si son víctimas de *ciberviolencia* o cualquier manifestación de violencia, sin tener de por medio tanta burocracia y revictimización por parte de quienes deberían protegernos (además de que reciben salario por esto) puede hacer diferencia para comenzar a recuperar la confianza en la policía y el miedo o burla de la población.

La *ciberviolencia* es retroceder en leyes donde se supone hemos evolucionado, avanzado y los delitos están regulados en teoría desde una perspectiva de género, ratificando el Estado mexicano ser parte y a favor de los derechos humanos, pero como el feminicidio, la violencia pareciera ser un círculo vicioso que no termina, sino se vuelve como el capitalismo un mundo que cuando se piensa va a terminar, tiene la capacidad de renovarse y reinventarse. Por ejemplo, la:

> LEY DE ACCESO DE LAS MUJERES A UNA VIDA LIBRE DE VIOLENCIA
> Artículo 7 fracción X:
> Violencia digital: es cualquier acto realizado mediante el uso de materiales impresos, correo electrónico, mensajes telefónicos, redes sociales, plataformas de internet, correo electrónico, o cualquier medio tecnológico, por el que se obtenga, exponga, distribuya, difunda, exhiba, reproduzca, transmita, comercialice, oferte, intercambie y comparta imágenes, audios o videos reales o simulados de contenido sexual íntimo de una persona, sin su consentimiento; que atente contra la integridad, la dignidad, la intimidad, la libertad, la vida privada de las mujeres o cause daño psicológico, económico o sexual tanto en el ámbito privado como en el público, además de daño moral, tanto a ellas como a sus familias.
> Las Reformas que se promueven a través de la "ley Olimpia" permite visibilizar y sancionar conductas de violencia sexual cometidas principalmente hacia las mujeres y niñas a través de medios digitales (redes sociales, plataformas tecnológicas, medios de radiodifusión, telecomunicaciones, informáticos o cualquier otro medio de transmisión de datos) las cuales vulneran sus derechos a la intimidad, la dignidad, la libertad o la vida privada, causando un daño de cualquier tipo.[55]

Parece que el mensaje de las autoridades es que debe existir un hecho atroz, víctima o familias que luchen incansablemente para que se les voltee a ver dada la realidad de violencia en el país y los matices con los que se está reinventando constantemente, lo cierto es que en los mismos vacíos legales pareciera no se castiga al violentador y ni el sufrimiento de la víctima, por ejemplo; las madres

[55]Secretaria de las Mujeres, Gobierno de la Ciudad de México, Prevención y visibilización del ciberacoso contra las mujeres y niñas, ¿Qué es la violencia cibernética contra las mujeres?, 2024, *op. cit.*

rastreadoras que su dolor y falta de justicia las obliga a buscar entre basura, fosas clandestinas, sitios del crimen organizado y exposición a todo tipo de peligro para encontrar a sus hijas y que pueden ser ellas las próximas desaparecidas no importa a la sociedad, al Estado ni a las leyes.

2.3.2.-Ley Olimpia.

La ley Olimpia tiene como fin que diversas reformas penales en varios estados de la República Mexicana, así como a la Ley General de Acceso de las Mujeres a una Vida Libre de Violencia se contemplen y apliquen en todo el país, de igual forma que se hable de la violencia digital (*ciberviolencia*) como delito.

La Ley Olimpia es el triunfo para referirnos al delito que se tiene por la violencia a la intimidad y en que todos podemos hacer pleno uso de derechos sexuales, en especial a las mujeres y que la denominada pornovenganza que va en contra de derechos de las personas sea a nivel federal. Este delito usado muy comúnmente en exparejas que no comprenden el fin de una relación (ni su mente psicópata) y nada justifica la exhibición de lo que sucedió para amenazar a la persona, intimidad y degradar.

Es importante cuestionarnos más allá de la víctima y el delito ¿cómo es posible que existan personas con la necesidad de realizar esto? la respuesta va enfocada a la falta de valores, salud mental y machismo en el país. ¿Cómo puede una persona (si es que se le puede llamar así) sentirse con derecho de violentar a otra(o), para dañar todos los aspectos de su vida y dignidad? Peor aún ni siquiera dando la cara, refugiándose y escondiéndose en los *beneficios* que se obtienen al estar detrás de un dispositivo que la ley permite se pueda poner cualquier comentario, ofensa y denostación hacia otra persona, cuando no se debería permitir al agresor exponer y denigrar a nadie, pero tampoco la sociedad integrarlo a la vida como si no hiciera nada o como si no importará el daño a otra (s) persona (s), peor aún como si el hablar mal de su expareja fuera consensuado.

> Olimpia Coral Melo es una mujer que, tras haber sido víctima de la difusión viral sin su consentimiento, de un video suyo con contenido íntimo sexual, conoció el rechazo colectivo, el juicio, el estigma social y la inimaginable violencia comunitaria, social, estructural e institucional que pesa sobre las mujeres por el simple hecho de tener cuerpo de mujer, de ejercer nuestra sexualidad y no encajar en los apretados moldes de “buena mujer” que nos impone un sistema patriarcal. Para fortuna de todas las mujeres en el país, tras un duro proceso de gran resiliencia, ella decidió no callar lo que le había pasado y buscar justicia. Lo intentó mediante las instituciones al acudir a un Ministerio Público en donde vivió una terrible

revictimización, además de que se le dijo que lo que a ella le había sucedido no era un delito. Eso fue justo lo que le dio la valentía de transformar la ley. Si la ley no decía que eso que ella estaba viviendo era un delito, entonces la ley era la que debía cambiar, no las mujeres quienes debíamos seguir callando. Así inicia la historia de esta lucha a la que nos hemos sumado miles de mujeres a todo lo largo y ancho del territorio mexicano y hasta en muchos países de América Latina. Hoy en día las reformas legales que reconocen la existencia de esta modalidad de violencia y las que reconocen esas conductas como delito, son una realidad.

Ley Olimpia se convirtió en el nombre mediático dado a esta gran lucha a favor de que las mujeres y niñas podamos vivir libres de violencia y estar seguras también en los espacios digitales…

¿Qué es la Ley Olimpia?

Es el primer proyecto de reformas en México en materia de violencia digital desde la realidad de las víctimas y con perspectiva de género. Son dos cambios Legislativos: El reconocimiento de esta modalidad de violencia en la Ley de Acceso de las mujeres a una vida libre de violencia y la tipificación del delito contra la intimidad sexual en los Códigos Penales, para castigar la difusión y producción de contenidos íntimos sexuales sin el consentimiento o autorización, así como las amenazas y extorsión…

¿Cuál es su importancia?

*Colocó un tema antes invisible en la agenda pública y lo ha llevado hasta algunas agendas de gobierno: la violencia digital contra la intimidad sexual de las mujeres no es nueva en los hechos, las vidas de muchas mujeres la han conocido desde que se masificaron los espacios digitales, sin embargo, no había sido una problemática visible…

*Contribuye a cambiar el discurso colectivo sobre la violencia sexual contra las mujeres: Más allá del logro que en sí implica haber logrado reformar la legislación mexicana, el gran triunfo de esta lucha llamada Ley Olimpia, ha sido que se han fortalecido algunas bases para transformar las creencias, los estigmas, prejuicios, roles y estereotipos que oprimen a las mujeres y que las colocan en especial vulnerabilidad cuando su intimidad es expuesta. Ya no hay que seguir juzgando a las víctimas, sino a los agresores.

*Desestigmatiza un tema que antes era tabú: Previo al boom mediático de la violencia digital que se logró gracias a la lucha de Ley Olimpia, las personas víctimas de este tipo de violencias se aislaban, se escondían, sentían vergüenza de sí mismas. Hoy al ser un tema mucho más visible, cada vez más mujeres se atreven a hablar, a pedir ayuda, a contar sus historias, porque poco a poco van entendiendo que no son culpables, que fueron víctimas y que no tienen por qué sentir vergüenza.

*Reconoce la violencia digital como una modalidad de violencia…

*Castiga, visibiliza, previene e inhibe la violencia digital desde una PEG. Gracias a las reformas realizadas a los códigos penales de cada entidad y el federal…

Art 63 Las medidas u órdenes de protección en materia penal, se consideran personalísimas e intransferibles y podrán ser…

XV. La interrupción, bloqueo, destrucción o eliminación de imágenes, audios, videos de contenido sexual íntimo de una persona, sin su consentimiento; de medios impresos, redes sociales, plataforma digital o cualquier dispositivo o medio tecnológico.

> Art 72 TER.- Tratándose de violencia digital, la o el Ministerio Público, la Jueza o Juez, procederá de acuerdo al siguiente procedimiento:
> I.La querella podrá presentarse vía electrónica o mediante escrito de manera personal; y
> II.El Ministerio Público ordenará de manera inmediata, las medidas de protección necesarias, ordenando vía electrónica o mediante escrito a las empresas de plataformas digitales, redes sociales o páginas electrónicas, personas físicas o morales, la interrupción, bloqueo, destrucción, o eliminación de imágenes, audios, o videos relacionados con la querella.
> Artículo 181 Quintus. Comete el delito contra la intimidad sexual:
> I.Quien videograbe, audiograbe, fotografíe, filme o elabore, imágenes, audios o videos reales o simulados de contenido sexual íntimo, de una persona sin su consentimiento o mediante engaño.
> II.Quien exponga, distribuya, difunda, exhiba, reproduzca, transmita, comercialice, oferte, intercambie y comparta imágenes, audios o videos de contenido sexual íntimo de una persona, a sabiendas de que no existe consentimiento, mediante materiales impresos, correo electrónico, mensajes telefónicos, redes sociales o cualquier medio tecnológico. A quien cometa este delito, se le impondrá una pena de cuatro a seis años de prisión y multa de quinientas a mil unidades de medida y actualización…
> La pena se agravará en una mitad cuando:
> I.La víctima sea una persona ascendiente o descendiente en línea recta, hasta el tercer grado;
> II.Cuando exista o haya existido entre el activo y la víctima una relación de matrimonio, concubinato, sociedad de convivencia, noviazgo o cualquier otra relación sentimental o de hecho, de confianza, docente, educativo, laboral, de subordinación o superioridad;
> III.Cuando aprovechando su condición de persona responsable o encargada de algún establecimiento de servicio al público, realice alguna de las conductas establecidas en el presente artículo;
> IV.Sea cometido por alguna persona servidora pública o integrante de las instituciones de Seguridad Ciudadana en ejercicio de sus funciones;
> V. Se cometa en contra de personas adultas mayores, con discapacidad, en situación de calle, afromexicanas o de identidad indígena. Este delito se perseguirá por querella.[56]

La Ley Olimpia es un claro ejemplo de cómo la *ciberviolencia* va un paso adelante de las leyes; porque todavía no se ha tipificado el delito y ya existen víctimas aunque las autoridades justifican que no existe delito a perseguir y por lo tanto su falta de actuación, pero si ya existió cambio para mal en la vida de una(s)

[56]Gobierno de la Ciudad de México, Secretaria de las Mujeres, *Manual de Contenidos: Laboratorio de Análisis Multidisciplinario sobre Ley Olimpia*, Frente Nacional Sorodidad, Defensoras Digitales.Org, 2024, pp.5-7, de: https://semujeres.cdmx.gob.mx/storage/app/media/ViolenciaDigital/Manual_Contenidos_Lab_Ley_Olimpia.pdf

persona(s), sumado a la revictimización por haber sufrido violencia de medios digitales que se han convertido en un falso *slogan* de libertad de expresión para que bajo esta premisa el número de víctimas continue y por parte de las autoridades sin propuestas reales para que a nivel nacional, sea real el alto a la *ciberviolencia* de víctimas reales.

Desafortunadamente, hablar de violencia digital y en específico respecto a la vida sexual (mayormente la situación vulnerable en mujeres) ha sido tan señalado que se juzga a la víctima y no se señala a quien agredió que prácticamente se le aplaude sin castigo alguno.

Se ha querido normalizar los denominados *piropos* como si se tratara de *halagos*, lo cual es falso, de hecho, el rechazo hacia esto ha traído comentarios absurdos como: *ni que estuvieran tan buenas*, que es tan lamentable la respuesta por no permitir la ofensa y poner alto. lo que sigue fomentando un país machista (sobre todo en el norte de México) por más que surjan más y más leyes para *protección,* en la realidad cualquiera siente derecho de ofender y denigrar a otros(as).

La vida cotidiana nos muestra si es real o no que las nuevas leyes y mecanismos para erradicar la violencia que poco a poco se ha tornado entre todos(as), no ha sido tangible en poder empatizar en la sociedad, tampoco en obtener justicia en un país que todo lo atribuye a delincuencia organizada.

2.3.3.-Ley Ingrid.

Podemos dejar de creer en la humanidad cuando se engloba un todo que se define en el caso de Ingrid, qué tan mal puede estar la(s) persona(s) para cometer actos tan difíciles de ponerles un calificativo, pero sin duda atroces, que sin importar la razón o no de parentesco se pueden dar situaciones que ni siquiera los animales cometen y se sigue diciendo que los humanos son personas y por eso tener derechos y los animales no. No legislar a favor de ellos, pero si por querer hacer pasar a delincuentes como enfermos mentales.

Igual o peor es la difusión de escenas tan grotescas como si se tratara de un espectáculo, poque es por situaciones como esta que se debe entender la importancia de la salud mental ¿Qué puede llevar a una(s) persona(s) si se le puede llamar así a cometer terribles actos y qué tan mal debe estar una población que quienes deberían encargarse del buen trato a la (s) víctima (s) (de *cujus*), ex parejas o los medios de comunicación que por morbo se hacen *virales* sin sentir empatía? Pero aún seguimos creyendo que el terrorismo, violencia y crueldad ocurre sólo en Medio Oriente no en los países desarrollados o en vías de desarrollo como México y sobre todo en el norte del país.

A raíz de un hecho difundido (porque puede haber miles como este o peores, pero no públicos) es que sucede:

> LEY INGRID una iniciativa de Ley para castigar las filtraciones de los expedientes de Fiscalía. Ingrid Escamilla: Víctima del delito de Feminicidio, cometido por su pareja sentimental.
> Medios de comunicación: En diversos medios informativos impresos y digitales se difundieron imágenes del cuerpo de Ingrid.
> Divulgación masiva: Contenido que causó conmoción en la sociedad e indignación entre sus familiares y amigos.
> La consecuencia de ello, llevó a la sociedad a exigir ¡No más filtraciones!
> ¿Por qué es importante evitar las filtraciones?
> 1.-Cuando una persona servidora pública indebidamente hace difusión de imágenes, audios, videos y documentos sobre los cadáveres, de las circunstancias de su muerte, de lesiones o el estado de salud de las víctimas.
> 2.-Tiene como consecuencia la espectacularización del Feminicidio.
> 3.-Se acrecienta la normalización de la violencia contra las mujeres.
> 4.-Incita al entretenimiento y agrava el daño a las víctimas.

5.-Vulnera la dignidad de las víctimas.
La divulgación de información e imágenes de las víctimas de algún delito constituye una lesión a la dignidad de la persona y la memoria de las víctimas.
* Establecer un tipo penal para sancionar a los servidores públicos que revelen o difundan imágenes o archivos de investigaciones.
* Fortalecer la protección legal a los derechos de las víctimas.
* Combatir la violencia mediática de género.
La Ley Ingrid se publicó el 26 de febrero en la Gaceta Oficial ARTÍCULO 293 QUÁTER: Se impondrán de 2 a 6 años de prisión, y una multa de quinientas a mil Unidades de Medida y Actualización a la persona servidora pública que, de forma indebida difunda, entregue, revele, publique, transmita, exponga, remita, distribuya, videograbe, audiograbe, fotografíe, filme, reproduzca, comercialice, oferte, intercambie o comparta imágenes, audios, videos, información reservada, documentos del lugar de los hechos o del hallazgo, indicios, evidencias, objetos, instrumentos relacionados con el procedimiento penal o productos con uno o varios hechos, señalados por la Ley como delitos.
Las sanciones previstas en el artículo anterior aumentarán en una tercera parte, sí la información que se difunda:
*Sea con el fin de menoscabar la dignidad de las víctimas o de sus familiares;
*Tratare de cadáveres de mujeres, niñas, o adolescentes, o
*Sea de las circunstancias de su muerte, de las lesiones o del estado de salud de la víctima.[57]

Cuando podríamos decir que hombres y mujeres legalmente avanzamos juntos hacía la igualdad de derechos y oportunidades lo real es que es una idea falsa que forma parte del pensamiento común en relación a ver a la mujer supuestamente a la par del hombre y que juntos van de la mano, lo cierto es que daría la apariencia que las leyes en relación a delitos sexuales, violencia de género y *ciberviolencia* no cuentan con mecanismos más que lo escrito y plasmado en una ley o tipificar un delito de tal forma que no exista un castigo real, como por ejemplo; esto podemos observar y trasladar a feminicidios, lo primero sería si realmente el tipo penal no tiene tantos vacíos que seguramente se juzgara a muy pocos y lo real es que son demasiados quienes lo cometen que prácticamente es más fácil dejarlo en cifras por daños colaterales.

[57]Instituto de Formación Profesional y Estudios Superiores, Fiscalía General de Justicia de la Ciudad de México, *Ley Ingrid*, 2024, de:
https://ifpes.fgjcdmx.gob.mx/storage/app/media/2020/comunicacion/infografias/Ley_ingrid_.pdf

Otra situación, es el papel que desempeñan las redes sociales que prácticamente por una *selfie* las personas están dispuestas a arriesgar o perder su vida, podría ser porque en realidad no le encuentren valor y lo grave es que si la vida propia no importa como para arriesgar todo por nada, menos será posible hacer conciencia en lo que representa y vale la vida de otra persona (y cualquier ser vivo), una persona con la que se compartieron momentos que aún después de terminar una relación(amistad, laboral, pareja o familiar) puede ser tan miserable la ex pareja para querer arruinar la vida de otro(a) a costa de lo que sea.

El caso de Ingrid no sólo es doloroso como sociedad, sino muestra clara de todos los elementos que nos pueden indicar como vamos retorciendo en valores sin empatía porque el daño no sólo fue hacia a ella, es hacia las miles y miles de muertes que ocurren en el país, en donde la violencia desde el transporte público pese a las cámaras de videograbación sigue siendo un lugar seguro para cometer muchos delitos, pero aún peor la falta de humanidad para reproducir videos, imágenes y burlas respecto lo que ahora conocemos como Ley Ingrid, siguen siendo virales.

2.3.4.-Ley Ocaña.

Esta ley a la par con la ley Ingrid busca erradicar la difusión de contenido de *cujus* y básicamente con esto el respeto al cuerpo aún en su muerte, todo ello de la mano de la no violencia incluso después de la vida.

Porque si bien como sociedad analizamos los distintos patrones de violencia y hoy en día como si se tratara de evolución o moda a la *ciberviolencia* (esto porque la violencia ha permeado a lo largo de los años e historia, pero se ha disfrazado de distintas formas) volvemos a estancarnos en situaciones que no deberían existir.

Hablar de vida y muerte siempre innatas en nuestra historia como país, desde culturas prehispánicas donde incluso se rendía culto a ello, pero en una forma de respeto para que la persona después de la muerte (como en la cultura egipcia) se le sigue cuidando a trascender por un camino (espiritual) mediante rezos hacia que su alma descanse en paz. Esto nos lleva a pensar, si el cuidado y respeto hacia la muerte de la persona se trataba de algo importante ¿cuándo vida y muerte dejaron de significar y ser importante para el ser humano y la sociedad?

En respuesta a lo anterior, podríamos explicarlo al entender el daño a la salud mental que hemos perdido generación tras generación, que como dice la canción *la vida no vale nada*, entonces si nada tiene sentido y es importante, difícilmente podremos esperar el respeto a la vida ajena y fallecimiento. Porque la muerte es sinónimo de dinero (en las herencias, negocios económicos y sociedades empresariales) es lo que se presenta en redes sociales, aunque sea apariencia, entonces cobra sentido no tener respeto por nada.

> El Congreso del Estado de México aprobó reformas al Código Penal estatal para establecer sanciones de hasta 12 años de prisión en contra de quien participe en la difusión de imágenes de cadáveres de personas, reforma que es conocida como 'Ley Ingrid' o 'Ley Octavio Ocaña se busca salvaguardar la dignidad y honra póstumas, así como garantizar el acceso a la justicia a terceros debido a prácticas ilícitas cometidas por personas servidoras públicas y ciudadanía…
> El dictamen también establece que la persona, que sin tratarse de programas preventivos, educativos o informativos que diseñen o impartan instituciones públicas, privadas o sociales que tengan por objeto la educación, realice actos de

> difusión, entrega, publicación, transmisión, videograbación, reproducción, exposición, filmación, fotografía, comparta u oferte e intercambie imágenes relacionadas con cadáveres de personas, causando menoscabo en la dignidad del honor y la intimidad de la víctima o la seguridad, paz y privacidad de sus familiares, recibirá una sanción de cuatro a ocho años de prisión, así como la reparación integral del daño.
> Además, si en la comisión de este delito participan personas servidoras públicas de salud, protección civil, seguridad pública, procuración y administración de justicia o cualquier otro inherente a la cadena de justicia, que por su empleo cargo o comisión tengan acceso a la información y documentos relacionados con objetos, indicios, evidencias, hallazgos e instrumentos vinculados a un procedimiento penal o una investigación relacionada con el hecho delictivo, se le impondrán de tres a siete años de prisión.
> Además, si el sujeto pasivo de este delito son mujeres, niñas, niños, adolescentes o personas en situación de vulnerabilidad, la pena se incrementará hasta una mitad de las que correspondan, por lo que podrían alcanzar sanciones de hasta 12 años de prisión.[58]

Gracias al seguimiento de igual mediante redes sociales y el buen uso de ellas, podemos hacer presión en casos que podrían seguir invisibles, pero es precisamente este uso correcto de las plataformas lo que debería tratarse, no en difusión de imágenes o videos, que tiene el factor tragedia al cometerse por servidores públicos que su función es lo contrario y proteger a la población.

Cuando la mayoría de los mexicanos piensa en policías, servidores públicos o el sistema judicial no es precisamente en seguridad y justicia, puede sonar tan a la par de pensar en delincuencia organizada (de hecho a estos últimos se les puede llegar a tener mayor respeto en relación a las obras que realizan en ciertos casos en sus comunidades) y por ello tan común que entre litigantes se mencione que *es bueno conocer leyes, pero mejor aún conocer al juez o autoridad a cargo del caso*, lo cual es lamentable porque si ni siquiera se tiene tranquilidad pensar en autoridades a cargo de impartir justicia ¿cómo podremos confiar en las leyes que se emiten o en la seguridad que podría hacer respecto a los ciudadanos?.

[58]Diputadas y Diputados Locales Estado de México, Comunicado 2256, 24 de octubre 2023, Poder Legislativo del Estado de México, *Hasta 12 años de cárcel por difundir imágenes de cadáveres: Congreso*, 2024, de: https://www.legislativoedomex.gob.mx/boletin/a93a2214-e15f-42f7-b250-6e31a67ff785

2.3.5.-Ley Alina.

Esta ley es sumamente importante en un país donde primero se priva de la libertad y después se intenta investigar (lo cual puede tardar años o nunca llegar) y finalmente la persona debe probar que es inocente, pero en situaciones donde los penales de mujeres tienen mayor marginación y vulnerabilidad por el abandono, esto puede ser imposible.

Señalar por defenderse de un agresor(a) es tan mal visto (en una sociedad hipócrita, muy cómodamente que juzga y señala desde su situación de privilegio) como si fuese quien comete delitos, asesina o comete *ciberviolencia*, pero la legítima defensa con perspectiva de género y exceso dentro de la misma abarca demasiadas circunstancias a considerar de como una situación de violencia de todo tipo en un segundo la vida cambia drásticamente, que se entiende por qué muchas víctimas que intentan acudir por ayuda, orientación o denuncia se enfrentan a interrogatorios que básicamente buscan inculpar sin ser quien comete el delito.

Esta ley tiene como fin que se modifique el Código Penal de Baja California en los artículos 23, 79 y 21 que se de el artículo 26BIS para que se de la legitima defensa en casos en que la mujer fue víctima se encuentre su vida en riesgo y no se tome como exceso de legítima defensa, ya sea por intimidación, amenaza o miedo. Así mismo que se le proteja ya sea a petición de parte u oficio.

> Ciudad de México, 27 de agosto, 2022.- Alina Mariel Narciso Tehuaxtle es una mujer expolicía de 27 años que pasó casi cinco años en prisión por matar a su pareja en legítima defensa. La sentencia la condenó a 45 años de cárcel.
> Por este caso se aprobó hace 3 días, La Ley Alina, en Baja California, que considera como legítima defensa los casos de las mujeres víctimas de violencia de género que se defienden de sus agresores, luego de 8 meses de discusión. Y busca ser un punto de partida para que más mujeres en la misma situación puedan obtener su libertad.
> *Los Cambios en B.C.*
> •El Artículo 23 propone que la figura de legítima defensa se incluya cuando quien se defiende de un delito le ocasione a la persona agresora una lesión o incluso lo prive de la vida, actualmente, solo se incluye un daño.
> •Se agregó un párrafo para presumir legítima defensa cuando la mujer sea víctima o haya estado en peligro de ser víctima de violencia física, psicológica, sexual o feminicida, y repela la agresión, o cuando otra persona la repela en auxilio de ella, aun cuando se haya excedido.

> •En este mismo artículo se obliga a la Fiscalía, Ministerio Público, jueces y juezas para actuar con una perspectiva de género para poder determinar el origen de la legítima defensa. Que no será requisito para acreditar la violencia de género del que existan antecedentes.
> •En el artículo 79, se dirá que no se considere un acto de "Exceso de legítima defensa" cuando la persona agredida sufra miedo o terror y se encuentren en un estado de confusión que afecte su capacidad para determinar el límite adecuado de su respuesta o la racionalidad de los medios empleados. Y de igual manera se aplicará este criterio a la persona que ayude o actúe en defensa de una mujer víctima de violencia.
> •En este mismo artículo, según se lee en el decreto, también se considerará la legítima defensa si la persona cuya agresión se repele es físicamente más fuerte y ejerció o intentó ejercer violencia física, psicológica, sexual o feminicida, aunque no concurran los estados de terror, miedo o estado de confusión en la persona que repele el ataque y busca el ayudar psicológica la persona que se haya defendido. También será analizado con perspectiva de género.
> •En la Ley de Acceso para las Mujeres a una Vida sin Violencia, se busca reformar el artículo 21 para que las órdenes de protección puedan ser otorgadas a petición de parte o de oficio, esto quiere decir que la autoridad lo haga, aunque la víctima no lo solicite, se incluyen los actos de legítima defensa en donde se evita el contacto con la parte agresora.
> •Se creó el artículo 26 bis para establecer que el municipio, Fiscalía, jueces y juezas deberá ordenar la protección necesaria, considerando: que sea adecuada, oportuna y proporcional; que los usos y costumbres. Estas órdenes deberán dictarse siempre privilegiando la integridad y la seguridad de las víctimas.[59]

La exigencia para que en todo el país se aplique esta ley debe ser constante para que sea real, sin permitir que se promulgue y de pronto los elementos del tipo penal sean tan ambiguos que se convierta únicamente en un estandarte para que se siga diciendo que en México se avanza en leyes a favor de las víctimas, sin revisar cada una de ellas y se hagan tangibles en una vida libre de violencia para todos(as).

La legitima defensa engloba todas las circunstancias que las leyes contra la violencia no han querido voltear a ver, en casos donde, por ejemplo; defenderse de agresión o patrones constantes de agresión pueden desencadenar si no intenta escapar de ese momento la muerte de quien ha sido víctima.

[59]Servicio de Noticias de la Mujer de Latinoamérica y el Caribe (SEMLAC), *Aprueba congreso de Baja California la Ley Alina, que exime a las mujeres por actuar en legítima defensa*, Sem México La mujer es notica, 27/08/2023, de:
https://semmexico.mx/aprueba-congreso-de-baja-california-la-ley-alina-que-exime-a-las-mujeres-por-actuar-en-legitima-defensa/

2.3.6.-Ley Malena.

No podemos poner en una balanza qué delito resulta peor, más denigrante o atenta contra todo lo malo en que se ha convertido la humanidad, pero la Ley Malena muestra un panorama de impunidad a todas luces, de una muerte en vida y machista para que el rechazo que sienta por el ataque de ácido que recibió lo recuerde toda su vida.

Incluso si la medicina y ciencia pudiera regresar a la víctima a su vida anterior, nada volvería a ser como antes de ese momento, el trauma, impotencia, dolor y una justicia negada es violatorio a derechos humanos, que gracias a la lucha de Malena contamos con visibilizar el ataque por ácidos.

El jefe de Gobierno de la Ciudad de México (CDMX) Martí Batres informó en febrero de 2024:

> "La Gaceta Oficial de la Ciudad de México ha publicado… reformas son para tipificar con mucha claridad los ataques con ácido o sustancias químicas o corrosivas. (...) Incluyen, entrecomillo, 'cualquier acción u omisión que cause o busque causar daño no accidental arrojando, derramando o poniendo en contacto a la víctima con algún tipo de gas, compuesto químico, ácido, álcalis, sustancias químicas, corrosivas, cáusticas, irritantes, tóxicas, inflamables, explosivas, reactivas, líquidos a altas temperaturas o cualquier otra sustancia que por sí misma o en determinadas condiciones puedan provocar lesiones o cualquier tipo de discapacidad'"… los daños causados por este tipo de violencia serán considerados un delito autónomo, sancionado con penas de 8 a 12 años de prisión, así como multas de 300 a 700 veces la Unidad de Medida y Actualización vigente (UMA), y de 11 a 46 años de cárcel cuando las lesiones sean consideradas en grado de tentativa de feminicidio.
> "Se trata de evitar la impunidad, por eso el nuevo Artículo 135 Bis del Código Penal señala, del mismo modo, los daños causados por este tipo de ataques ya no serán considerados un caso más del delito de lesiones en nuestro Código Penal; sino un delito separado, con su propia descripción típica y que entre otras cosas supera las clásicas clasificaciones de lesiones leves o graves o la de temporales o permanentes", señaló.
> La pena, detalló, aumentará hasta en una mitad cuando sea cometida por razones de género, cause incapacidad, deformidad o pérdida de oído, vista o habla; cause alteración o daño en el aparato genital o en las funciones del ejercicio de la sexualidad; se cometa contra niños, niñas y adolescentes, personas con discapacidad o personas transexuales o transgénero; si existe relación afectiva, de supra, subordinación o superioridad, de parentesco; que previo al ataque que causó la lesión haya habido amenazas, acoso u otro tipo de violencia. Además, este

> nuevo delito deberá considerarse tentativa de feminicidio cuando cause daños graves y permanentes a la mujer víctima.
> "De dos a cinco años a prisión, pasamos a una sanción de ocho a 12 años de prisión, pero además, en los casos en los que se equipare a una tentativa de feminicidio que es en los casos en que se disminuya una facultad o el normal funcionamiento de un órgano o un miembro, pasamos de una sanción de tres a cinco años de prisión a una sanción de 11 y hasta 46 años de prisión. (...) Sabemos que el castigo por la vía de penas debe ser siempre la última razón del poder coercitivo de una sociedad civilizada, pero ante la indignante y bárbara violencia machista que somete a las mujeres, es nuestro deber usar con dureza esa última razón, el dolor de las mujeres nos lo exige, por lo tanto, aquí está hoy publicada la llamada Ley Malena".
> La nueva ley obliga a las instancias de salud a reportar de manera sistemática ante el Ministerio Público los ataques mediante ácido, sustancias químicas o corrosivas de los cuales tengan conocimiento.[60]

La lucha de Malena, para que las dependencias judiciales actúen de inmediato debe representar la injusticia que se le negó, pero también debe significar que el poder no puede arruinarle la vida a nadie, lo que también nos lleva a cuestionar: ¿quién se prestó a aventar el ácido lo vale por dinero? Porque si el dinero es lo único que tiene valor o todo, nunca avanzaremos en leyes, en su aplicación y justicia para quienes desafortunadamente han sido víctimas y a las que les debemos esta ley y ya no se encuentran con vida.

[60]Gobierno de la Ciudad de México, Jefatura de Gobierno, *Publica Martí Batres "Ley Malena" que tipifica la "Violencia Ácida" como Delito y Garantiza Justicia a las Víctimas*, 19 febrero 2024, de: https://jefaturadegobierno.cdmx.gob.mx/comunicacion/nota/publica-marti-batres-ley-malena-que-tipifica-la-violencia-acida-como-delito-y-garantiza-justicia-las-victimas

CONCLUSIONES DEL CAPÍTULO

Los delitos *cibernéticos* que se encuentran protegidos y se persiguen por la ley, son de índole financiero (en su mayoría, por no decir que los únicos ya que representan pérdidas para instituciones generalmente financieras y son estos las más interesados en implementar la tecnología *cibernética*) porque difícilmente delitos como el *ciberacoso* representa peligro para todos y sobre todo para quienes poseen medios y poder adquisitivo por lo que es necesario concientizar que también representan secuelas severas y sobre todo porque estamos frente a daños a la psique, vida a la víctima y a terceros (su familia y cercanos).

No necesitamos amplias explicaciones para mirar con claridad distante entre la teoría y la realidad, basta que veamos los impedimentos para que se nos tome una denuncia por parte de la autoridad competente, marcar a algún número de seguridad pública, acudan y realmente brinden apoyo a los ciudadanos en caso de delito o en flagrancia. Hemos (como país) priorizado en la teoría y discurso, más que en la práctica, lo que nos lleva a vivir en dos realidades que constantemente chocan y no van de la mano.

En el mundo pareciera que sólo tenemos a la Ley de Instituciones de Crédito, Ley de Instituciones de Seguros y de Fianzas, Ley del Mercado de Valores, Ley General de Títulos y Operaciones de Crédito y la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, como si los delitos *cibernéticos* existiera en torno a finanzas y visiblemente los únicos y por lo tanto los delitos de índole sexual o trata de personas existen, pero quedan en un segundo plano que tal vez algún día lleguen a tener mayor relevancia para la ley y los legisladores.

Es indispensable tomar en cuenta que, al hablar de delitos *cibernéticos*, no es simplemente a que México mantenga en el discurso deben ser combatidos, que está de lado de las víctimas pero, sobre todo; de la mano con los derechos humanos, cuando realmente es alarmante que ni siquiera la vida como en casos de feminicidio

es protegida. Lo cual es importante empatizar en que incluso el acoso o *ciberbullying* pueden desencadenar pérdida de la vida (como en el suicidio).

Por lo que en el siguiente capítulo, en función del análisis de la legislación en México en materia de delitos *cibernéticos*, se propone una reclasificación de las penas de delitos *cibernéticos*, así como una visión global desde el ámbito nacional e internacional y lo importante que es llevar de la mano no solamente el derecho *más penas y más años en prisión*, sino de la mano de salud mental porque las repercusiones de aislar el derecho de otras ciencias no enriquecerse el prevenir, combatir, sanar y erradicar estos delitos.

De igual forma, plantear límites y riesgos de los avances tecnológicos, que en esta era digital es tan normal crecer con tecnología (aunque no al alcance de todos) pero tan acelerada que nos ha rebasado incluso cuando ya los *robots* que empezaban como asombro, pueden remplazar al mismo hombre y donde el derecho ha quedado lejano ante una realidad *cibernética* en la que el dinero (*criptomonedas*)y *robots* no deben rebasar al hombre.

CAPÍTULO 3. HACIA UNA RECLASIFICACIÓN DE LAS PENAS EN MATERIA DE DELITOS CIBERNÉTICOS.

Hace tan sólo 10 años que el uso de la tecnología en audiencias era impensable, en un sistema jurídico tan cotidiano (una forma tradicional y antijurídica para hacer justicia mediante *propinas*) y burocrático que evolucionaría con el sistema oral en juicios, lo que nos recuerda a la teoría de *Charles Darwin* (selección natural) donde las especies evolucionan a través del tiempo y sobreviven únicamente los más fuertes, los que lograron adaptarse al cambio, el cual se dio en un abrir y cerrar de ojos, pero que nos interpeló a todos porque siempre la brecha entre quienes lo tienen todo y los que no es alarmante.

Que fácil puede sonar en una teoría aplicada en la especie animal referirnos a evolución, pero olvidamos que lo mismo ocurre con las personas en su vida diaria, lo que ha representado un reto porque justamente en la pandemia por COVID-19 esa evolución fue tan acelerada para actualizar toda la forma pasada que por ejemplo, en lo laboral con la incorporación del *home office*, no todos estaban preparados ni con herramientas (como computadoras, internet o dispositivos electrónicos) así como lo jurídico, ya que el uso voraz de la tecnología es fundamental hoy en día, pero olvidando en el análisis los pros y contras como en este ámbito del trabajo muchos se aprovecharon y se beneficiaron de los empleados (los patrones) y ganaron a menor costo.

Muestra de lo anterior, fue el cambio del sistema jurídico escrito a lo oral, donde se dieron situaciones en que los litigantes se enfrentaron a juicios en grabaciones, prohibición en el uso de los códigos como apoyo, sin carpetas de investigación hacía que se pudiera cuestionar la preparación o no de ellos (as), además de la exposición pública de jueces, policías de investigación, fiscalía y aparato del Estado (por falta de capacitación) rechazo o vergüenza ante un paradigma de incompetencia que se impuso a los ciudadanos.

De igual forma, la tecnología permitió la publicación de grabaciones donde se observaba a jueces evidenciando la falta de preparación de los litigantes, desconocimiento o falta de preparación incluso para autoridades como ministerios públicos o policías de investigación, quedando atrás una generación y demostrando que las Universidades aún no estaban listas para este nuevo sistema y se comenzó a adecuar los espacios e instalaciones como Salas Orales desde la formación académica para la vida laboral en litigios.

Desafortunadamente, la tecnología avanzó más rápido que el ser humano, la ciencia y el derecho, poniendo de manifiesto que no podemos permitir nos rebasé porque entonces seremos subordinados de las máquinas (como si se tratará de una película inimaginable). Las leyes de igual forma, en el caso de delitos *cibernéticos*, quedaron atrás frente a víctimas que pagaban las consecuencias de quienes en el *ciber espacio* encontraron la forma ideal de actuar, sin tener consecuencias.

Aún tenemos como primer reto, dar una definición en cuanto a los delitos *cibernéticos* porque todavía se siguen denominando delitos informáticos que generalmente se usan para referirnos a aquellos que tienen que ver con el sistema financiero, como por ejemplo fraudes, espionaje o la usurpación para extraer dinero de cuentas de otros, pero no teniendo en cuenta que no todos los delitos *cibernéticos* se tratarán de una clasificación donde lo financiero es más importante o único que prevalece sobre el *ciberacoso* o delitos de otra connotación como la intimidación.

> Desde un punto de vista criminológico, existen dos enfoques, en cuanto a la naturaleza de este nuevo tipo de fenómeno criminal; el primero de ellos es que los delitos informáticos no son más que delitos convencionales que toman nueva vida a partir del uso de dispositivos informáticos y de servicios y aplicaciones en internet. La segunda perspectiva afirma que las tecnologías de la información y comunicación brindan nuevas herramientas para la comisión de delitos inexistentes, como la distribución de virus o programas maliciosos a través de la red, ataques a sitios web y la piratería del software. Lo cierto es que ambos enfoques son ciertos. Existen delitos tradicionales que adquieren nuevas formas a partir de la intermediación de dispositivos automatizados como también nuevas formas delictivas que no serían posibles de cometerse si no existiese un programa de software o archivos digitales presente, como, por ejemplo, en la elaboración de programas maliciosos con el fin

> de dañar un servidor web para afectar el funcionamiento de la página, o aquellos para extraer información de un dispositivo por ejemplo, los spyware o programas espías, o alterar o dañar el funcionamiento de un dispositivo a través de virus, gusanos y troyanos.
> ¿Pero qué son los delitos informáticos? Si bien no existe una definición específica, desde la década del 70 esbozaron distintas acepciones en cuanto al alcance del término. Según el Manual de Recursos de Justicia Criminal del Departamento de Justicia de los Estados Unidos de 1979 se entienden por estas conductas a "cualquier acto ilegal donde el conocimiento de la tecnología computacional es esencial para el éxito de su prosecución". Según una definición brindada por la Organización de Cooperación y Desarrollo Económico en 1983, el delito informático es "cualquier comportamiento antijurídico, no ético o no autorizado, relacionado con el procesamiento automático de datos y/o transmisiones de datos". Para el Consejo de Europa, según una definición de 1995, es "cualquier delito penal donde las autoridades de investigación deben obtener acceso a información que ha sido procesada o transmitida por sistemas computacionales o sistemas de procesamiento electrónico de datos". Para el criminólogo Majid Yar, la ausencia de una definición específica sobre el fenómeno del cibercrimen se debe fundamentalmente a que "la delincuencia informática se refiere no tanto a un único distintivo tipo de actividad delictiva, sino más bien a una amplia gama de actividades ilegales e ilícitas que comparten en común el único medio electrónico (ciberespacio) en el que tiene lugar".[61]

Desafortunadamente, tenemos datos desde 1979 en donde se comenzaba a hablar de ello y en 2024 referencia acerca de delitos *cibernéticos* sigue sonando novedoso, desconocido y sin una definición unificada donde en un país como México el analfabetismo, la falta de acceso a servicios básicos, sin educación y menos con incorporación a dispositivos electrónicos e internet para todos (la población) lo cual se agrava al intentar tratar de explicar este *ciberespacio* o delitos de connotación sexual en el mismo.

En las comunidades indígenas donde las políticas públicas y la ley pueden sonar a hablar de otra realidad y no respecto por los mismos mexicanos puede llevar mucho tiempo que el país en primer lugar imparta acceso para todos a las nuevas tecnologías como para contar con educación a distancia y acortando virtualmente o lugares lejanos a las comunidades.

[61]Gustavo Sain, *Cibercrimen y Delitos Informáticos. Los nuevos tipos penales en la era de internet*, ERREIUS, Dirección Nacional del Derecho de Autor. Hecho el depósito que marca la ley 11723, ISBN 978-987-4405-56-2, p.9, 2018, *op.cit*.

Pongamos como analogía, para intentar entender la falta de actuación de autoridades, inexistencia de la ley, falta de valores, ética y empatía como si se tratará de explicar si *fue primero el huevo o la gallina*. ¿Por qué lo anterior? Porque más allá de continuar en un debate casi filosófico, lo alarmante es no actuar ante la falta de actuación e implementación de mecanismos y leyes que protejan a las víctimas y eviten que surjan más.

No se trata de creer o clasificar a los delitos *cibernéticos* como *un tema de moda*, sino de actuar para la protección de los derechos humanos porque la vida que se protege en el primer artículo de nuestra Constitución Mexicana en teoría, en foros y discursos, pero que poco se ha actuado con leyes y su aplicación, no sólo de prevención sino de verdad y justicia para dimensionar que realmente no tenemos por lo menos como país actuación para protección y sanción ante ellos.

Las penas en materia de delitos *cibernéticos* no necesitan se den más años de prisión a quienes los cometen, tampoco la construcción de más centros de reclusión (que implica mayor contribución a impuestos por parte de la población) que en realidad no han logrado la posterior incorporación a la sociedad en vías haber adquirido herramientas por parte del Estado (al salir a la sociedad) como talleres psicológicos y bienestar mental como laborales, más bien han funcionado como mundo alterno donde ante la falta de inexistencia del Estado y leyes sobreviven en el mal *llamado hotel más caro*.

La reclasificación de los delitos debe ir de la mano con la salud mental, hacia la educación y conciencia de cómo afecta la vida de quienes son víctimas y las autoridades a reparar y prevenir situaciones, porque si bien la ley puede y debería clasificar y sancionar estos delitos *cibernéticos* con más años de prisión, eso no contribuye a que se erradiquen los delitos para quien, en una *sociedad líquida* (término que hace alusión a una vida sin sentido) al no encontrar valor en su vida y mucho menos en la de los demás, sobre todo si tiene un precio o pueda obtener

algo, no tenga nada que perder que encuentra en el daño y afectación al otro absurda *diversión* por su infelicidad.

Los delitos *cibernéticos* muestran una fría y cruda realidad en la manera en que la sociedad está *evolucionando* y el derecho quedando atrás. Aún se cree que las penas por delitos como feminicidio o secuestro deben ser más altas para que ya no se den, inseguridad, miedo y medidas que se han destinado por parte del Ejecutivo o aplicación de leyes por parte del Poder Judicial se siguen creando en una realidad y mundo alterno al que la población vive cotidianamente (lo cual es entendible para quienes su salario y prestaciones no representan a la población, por lo tanto; su realidad poco o nada puede importarles).

La formación de los futuros litigantes, integrantes del Poder Ejecutivo, Legislativo y Judicial no se basa en cursos con perspectiva de género únicamente, porque la falta de educación desde casa difícilmente ayudará con teoría, mil cursos o más penas para quienes la violencia es parte de su vida, familia, entorno y *normalidad*.

La verdad y justicia han sido silenciadas no sólo por impunidad sino por falta de actuación del sistema político, económico y judicial en una población que vive en estado *zombie* (como máquinas, sin un sentido respecto su vida y la de los demás) capaz de encontrar en los delitos *cibernéticos* aparente escape, como si se tratará de jugar un *videojuego* (lo cual también existe violencia, incluso de índole sexual donde el dinero vale más para violentar, matar en un *juego* que no es realidad), donde la justificación para sus acciones pueden ser tan absurdas en la vida real porque la falta de regulación y ley hacia sus acciones o el dinero que la corrupción goza sin importar las vidas perdidas o afectadas por el *ciberespacio*.

La justicia no debe ser tan anhelada como un sueño que al despertar se vive otra realidad, debe ser el cumplimiento, prevención, atención y no repetición que las leyes deben seguir y no quedar en *buenas intenciones* que sólo se manifiestan para discursos políticos o con fines electorales.

Si bien es indispensable que los delitos *cibernéticos* sean sancionados, también deben incluir el tratamiento a la salud mental y la educación a toda la población que no se trate de un lujo que poder estudiar y vivir en un Estado de derecho real no sea privilegio del poder adquisitivo. Aclarar, por ejemplo:

> El concepto de delitos informáticos son actitudes contrarias a los intereses de las personas en que se tiene a las computadoras como instrumento o fin (concepto atípico) o las conductas típicas, antijurídicas, culpables en que se tiene a las computadoras como instrumento o fin (concepto atípico); es decir, se refiere a que son acciones ocupacionales porque muchas veces se realizan cuando el sujeto está en el trabajo, son muchos los casos y pocas las denuncias, todo ello debido a la falta misma de regulación jurídica a nivel internacional, presenta grandes dificultades para su comprobación, esto es por su mismo carácter técnico…
> con la misma premisa de que los ataques informáticos van dirigidos a dos distintos objetivos; las personas o los dispositivos informáticos.[62]

La regulación jurídica es indispensable para comenzar a combatir los delitos *cibernéticos* porque la protección a la vida e integridad de las personas debe ser parte de una realidad, no únicamente desde la filosofía y teoría en códigos.

Hacer referencia a delitos *cibernéticos* aún suena lejano cuando se sigue con prácticas machistas o sin igualdad en derecho para hombres y mujeres, incluso en lugares en donde los *matrimonios* forzados o el cambio de personas por dinero o ganado sigue presente la realidad jurídica y de la población debe ser a la par de tecnología, brindando herramientas educativas y no solamente en la vida de intentar cambios que puede pasar años o siglos.

No se trata de poner una escala de qué delito es más grave, por ejemplo; entre lo financiero, el daño a la *psique* o cuerpo de la persona, se trata de leyes donde no exista exclusión como si se valorara de acuerdo poder adquisitivo, en una sociedad donde todos(as) somos importantes y poder entender como otros países han sido pilares en avanzar en dirección correcta.

---

[62]Armando Valencia Álvarez. Impacto de los delitos informáticos en la sociedad actual en *Revista de la Facultad de Derecho de la Universidad Veracruzana*, Publicación semestral, número dos, , abril 2020, pp.3-4, de:
https://www.uv.mx/derecho/files/2019/04/Revista-de-la-Facultad-de-Derecho-No-3-Impacto-de-los-delitos-informaticos-en-la-sociedad-actual.pdf

Es importante mostrar lo que han realizado otros países en cuanto a delitos *cibernéticos*, en lo cual México podría apoyarse en avanzar y unificar de acuerdo a su población. Lo anterior, con el fin de que la justicia (llegue a todos, desde un banquero a quien *hackeron* su sistema, como a una persona en comunidades indígenas para poder cobrar las ganancias de sus productos como artesanías o siembra en campo o tejidos) sea tangible incluso desde programas sociales y lleguen con el destino para lo cual se crea un monto de apoyo o programa social como puede ser proveer de tecnología y al mismo tiempo de los usos para mejora y prevención de consecuencias, con la finalidad de erradicar el analfabetismo se pueda ocupar herramientas en el buen uso.

En el caso de otros países, tenemos, por ejemplo, a:

> A)ALEMANIA. Para hacer frente a la delincuencia relacionado con la informática y con efectos a partir del 1 de agosto de 1986, se adoptó la Segunda Ley contra la Criminalidad Económica del 15 de mayo de 1986 en la que se contemplan los siguientes delitos:
> 1. Espionaje de datos. 2.- Estafa Informática. 3.- Falsificación de datos probatorios. 4.-Alteración de Datos. 5.- Sabotaje Informático. 6.- Utilización abusiva de cheques o tarjetas de crédito.
> Cabe mencionar que esta solución fue también adoptada en los Países Escandinavos y en Austria.
> Alemania también cuenta con una Ley de Protección de Datos, promulgada el 27 de enero de 1977, en la cual, en su numeral primero menciona que "el cometido de la protección de datos es evitar el detrimento de los intereses dignos de protección de los afectados, mediante la protección de los datos personales contra el abuso producido con ocasión del almacenamiento, comunicación, modificación y cancelación (proceso) de tales datos. La presente ley protege los datos personales que fueren almacenados en registros informatizados, modificados, cancelados o comunidades a partir de registros informatizados"…
> B)AUSTRIA. Ley de reforma del Código Penal del 22 de diciembre de 1987, la cual contempla los siguientes delitos:
> 1.-Destrucción de Datos… se regulan no sólo los datos personales sino también los no personales y los programas.
> 2.-Estafa Informática… se sanciona a aquellos que con dolo causen un perjuicio patrimonial a un tercero influyendo en el resultado de una elaboración de datos automática a través de la confección del programa, por la introducción, cancelación o alteración de datos o por actuar sobre el curso del procesamiento de datos.
> C)CHILE. Cuenta con una ley relativa a Delitos Informáticos, promulgada en Santiago de Chile el 28 de mayo de 1993, la cual en sus cuatro numerales menciona:
> Artículo 1°"El que maliciosamente destruya o inutilice un sistema de tratamiento de información o sus partes o componentes, o impida, obstaculice o modifique su funcionamiento, sufrirá la pena de presidio menor en su grado medio a máximo".

Artículo 2°"El que con el ánimo de apoderarse, usar o conocer indebidamente de la información contenida en un sistema de tratamiento de la misma, lo intercepte, interfiera o acceda a él, será castigado con presidio menor en su grado mínimo a medio".
Artículo 3°"El que maliciosamente revele o difunda los datos contenidos en un sistema de información, sufrirá la pena de presidio menor en su grado medio. Si quien incurre en estas conductas es el responsable del sistema de información, la pena se aumentará en un grado".
Artículo 4°"El que maliciosamente revele o difunda los datos contenidos en un sistema de información, sufrirá la pena de presidio menor en su grado medio. Si quien incurre en estas conductas es el responsable del sistema de información, la pena se aumentará en un grado".
D)ESTADOS UNIDOS... en 1994 del Acta Federal de Abuso Computacional. Que modificó al Acta de Fraude y Abuso Computacional de 1986. Dicha acta define dos niveles para el tratamiento de quienes crean virus estableciendo para aquellos que intencionalmente causan un daño por la transmisión de un virus, el castigo de hasta 10 años en prisión federal más una multa y para aquellos que lo transmiten sólo de manera imprudencial la sanción fluctúa entre una multa y un año de prisión…
California, en 1992 adoptó la Ley de Privacidad en la que se contemplan los delitos informáticos pero en menor grado que los delitos relacionados con la intimidad…
E)FRANCIA. Las disposiciones penales están contempladas en sus numerales del 41 al 44, los cuales contemplan lo siguiente: Artículo 41" El que hubiere procedido o mandado proceder a la realización de tratamientos automatizados de información nominativa sin que hubieran sido publicados los actos reglamentarios previstos en el artículo 15 o formuladas las denuncias previstas en el artículo 16, supra, será castigado con pena de privación de libertad de seis meses a tres años y con pena de multa de 2 000 a 200 000 francos, o con una sola de estas dos penas. Asimismo, el tribunal podrá ordenar la inserción de la sentencia, literalmente o en extracto, en uno o varios periódicos diarios, así como su fijación en tablón de edictos, en las condiciones que determinare y a expensas del condenado".
Artículo 42"El que hubiere registrado o mandado registrar, conservando o mandando conservar informaciones nominativas con infracción de las disposiciones de los artículos 25, 26 y 28, será castigado con pena de privación de libertad de uno a cinco años y con pena de multa de 20 000 a 2 000 000 francos…
Artículo 43."El que habiendo reunido, con ocasión de su registro, de su clasificación, de su transmisión o de otra forma de tratamiento, informaciones nominativas cuya divulgación tuviere como efecto atentar contra la reputación o la consideración de la persona o la intimidad de la vida privada; hubiere, sin autorización del interesado y a sabiendas, puesto tales informaciones en conocimiento de una persona que no estuviere habilitada para recibirlas a tenor de las disposiciones de la presente ley o de otras disposiciones legales, será castigado con pena de privación de libertad de dos a seis meses y con pena de multa de 2 000 a 20 000 francos, o con una de las dos penas.
El que por imprudencia o negligencia, hubiere divulgado o permitido divulgar informaciones de la índole de las que se mencionan en el párrafo anterior, será castigado con pena de multa de 2 000 a 20 000 francos.
Artículo 44 "El que, disponiendo de informaciones nominativas con ocasión de su registro, de su clasificación, de su transmisión o de otra forma de tratamiento las

hubiere desviado de su finalidad, según la misma hubiera sido definida, bien en el acto reglamentario previsto en el artículo 15, supra, o en las denuncias formuladas en aplicación de los artículos 16 y 17, bien en una disposición legal, será castigado con pena de privación de libertad de uno a cinco años y con multa de 20 000 a 2000 000 francos".

F)ITALIA. En un país con importante tradición criminalista, como Italia, nos encontramos tipificados en su Código Penal los siguientes delitos:

a)Acceso Abusivo. Se configura exclusivamente en caso de sistemas informáticos y telemáticos protegidos por dispositivos de seguridad (contraseñas o llaves de hardware) que indiquen claramente la privacidad del sistema y la voluntad del derechohabiente de reservar el acceso a aquél sólo a las personas autorizadas. La comisión de este delito se castiga con reclusión de hasta tres años, previendo agravantes.

b)Abuso de la calidad de operador de sistemas. Este delito es un agravante al delito de acceso abusivo y lo comete quien tiene la posibilidad de acceder y usar un sistema informático o telemático de manera libre por la facilidad de la comisión del delito.

c)Introducción de virus informáticos. Es penalmente responsable aquel que cree o introduzca a una red programas que tengan la función específica de bloquear un sistema, destruir datos o dañar el disco duro, con un castigo de reclusión de hasta dos años y multas considerables.

d)Fraude Informático.- Cuando por medio de artificios o engaños, induciendo a otro a error, alguien procura para sí o para otros un injusto beneficio, ocasionando daño a otro. También se entiende como tal la alteración del funcionamiento de sistemas informáticos o telemáticos o la intervención abusiva sobre datos, informaciones o programas en ellos contenidos o pertenecientes a ellos, cuando se procure una ventaja injusta, causando daño a otro. La punibilidad de este tipo de delito es de meses a tres años de prisión, más una multa considerable.

e)Intercepción abusiva.- Es un delito que se comete junto con el delito de falsificación, alteración o supresión de comunicaciones telefónicas o telegráficas. Asimismo, es la intercepción fraudulenta, el impedimento o intrusión de comunicaciones relativas a sistemas informáticos o telemáticos, además de la revelación al público, mediante cualquier medio, de la información, de esas publicaciones; este delito tiene una punibilidad de 6 meses a 4 años de prisión. Asimismo, se castiga el hecho de realizar la instalación de equipo con el fin anterior.

f)Falsificación informática. Es la alteración, modificación o borrado del contenido de documentos o comunicaciones informáticas o telemáticas. En este caso, se presupone la existencia de un documento escrito (aunque se debate doctrinariamente si los documentos electrónicos o virtuales pueden considerarse documentos escritos). En este caso, la doctrina italiana tiene muy clara la noción de "documento informático", al cual define como cualquier soporte informático que contenga datos, informaciones o programas específicamente destinados a elaborarlos.

g)Espionaje Informático.-Es la revelación del contenido de documentos informáticos secretos o su uso para adquirir beneficios propios, ocasionado daño a otro.

h)Violencia sobre bienes informáticos. Es el ejercicio arbitrario, con violencia, sobre un programa, mediante la total o parcial alteración, modificación o cancelación del

mismo o sobre un sistema telemático, impidiendo o perturbando su funcionamiento.
i)Abuso de la detentación o difusión de Códigos de acceso (contraseñas).
j)Violación de correspondencia electrónica, la cual tiene agravantes si causare daños.
Por su parte, la Constitución de la República Portuguesa, hace mención sobre la utilización informática, la cual fue aprobada por la Asamblea Constituyente el 2 de abril de 1976, y la cual menciona:
Artículo 35:"Utilización de la Informática. 1. Todos los ciudadanos tienen derecho a conocer lo que constare acerca de los mismos en registros mecanográficos, así como el fin a que se destinan las informaciones, pudiendo exigir la rectificación de los datos y su actualización. 2.La informática no podrá ser usada para el tratamiento de datos referentes a convicciones políticas, fe religiosa o vida privada, excepto cuando se tratare del proceso de datos no identificables para fines estadísticos. 3.Queda prohibida la atribución de un número nacional único a los ciudadanos…
En México, Internet no se ha regulado de manera expresa, como tampoco en el resto de los países latinoamericanos. Su uso gira en torno a cierto Código Ético y la tendencia Institucional es que será un fenómeno "autorregulable".
A pesar de los índices de crecimiento del uso de la computadora y de Internet, México enfrenta un problema social consistente en lo que denominamos "analfabetismo informático", del cual el Poder Legislativo no está exento, por lo que muchos congresistas no entienden el concepto y la estructura de Internet. Asimismo, nos atrevemos a afirmar que tanto los jueces como los magistrados que forman parte del Poder Judicial tienen hoy día la misma carencia. Es difícil prever el pronunciamiento de los tribunales federales o de la Suprema Corte de Justicia Mexicanos en un caso cuya resolución se base esencialmente en un conflicto por el uso de Internet, por lo cual no se tiene conocimiento de la existencia de tesis ni jurisprudencia algunas que se refieran a los medios electrónicos en general y a Internet en especial…
se considera pertinente recurrir a aquellos tratados internaciones de los que el Gobierno de México es parte en virtud de que el artículo 133 Constitucional establece que todos los tratados celebrados por el Presidente de la República y aprobados por el Senado serán Ley Suprema de toda la Unión.
El único estado de la República que contempla en su legislación los delitos informáticos es el Estado de Sinaloa... Código Penal Estatal.
Título Décimo. "Delitos contra el Patrimonio" Capítulo V. Delito Informático.
Artículo 217.-Comete delito informático, la persona que dolosamente y sin derecho:
"I.-Use o entre a una base de datos, sistemas de computadoras o red de computadoras o a cualquier parte de la misma, con el propósito de diseñar, ejecutar o alterar un esquema o artificio con el fin de defraudar, obtener dinero, bienes o información; o II.- Intercepte, interfiera, reciba, use, altere, dañe o destruya un soporte lógico o programa de computadora o los datos contenidos en la misma, en la base, sistemas o red. Al responsable del delito informático se le impondrá una pena de seis meses a dos años de prisión o de noventa a trescientos días de multa.[63]

[63]Poder Judicial de Michoacán, *Capitulo IV. Legislación en diferentes países sobre los delitos informáticos*, Biblioteca artículos electrónicos, , 2024, de:

El analfabetismo informático tan latente en México no preocupa sólo por la población sino como se muestra y desde los Tribunales, dependencias de gobierno, funcionarios públicos hasta la Suprema Corte de Justica de la Nación (SCJN) y la inexistencia de precedentes jurídicos y legales, así como la jurisprudencia respecto a delitos informáticos como si a falta de ello no sucedieran y menos con pronunciamiento y actuación.

No se trata de *tapar el sol con un dedo* e insinuar que a falta de leyes, vacíos o pronunciamiento (jurisprudencia) por el máximo Tribunal Constitucional en México, hace que vivamos en un país donde esto no ocurra porque sería revictimizar a quienes han padecido los delitos *cibernéticos* valorando (por lo menos eso se percibe) que prevalecen otros problemas a priorizar.

Sin embargo, es importante mencionar el avance en cuanto a la legislación, por ejemplo; en el estado de Sinaloa y tipificar el delito informático que muestra una paradoja porque si bien se ha enfatizado ser un lugar donde el crimen organizado (utilizado mediáticamente) se encuentra presente (es decir, un Estado con leyes y prácticas aparentemente que imponen los cárteles), nos hace cuestionar ¿cómo son quienes han dado un paso adelante en ello? ¿Cómo es posible que en la Ciudad de México (CDMX) teniendo legislación en materia de género, la situación sea diferente y no se cuente con leyes al respecto?

No se trata de competir respecto a qué Estado en el caso de México avanza más o se queda atrás en materia de delitos informáticos, sino en que las leyes se unifiquen en todo el país y el mundo, es por ello que la Suprema Corte de Justicia de la Nación (SCJN) debe ser quien actué en dicha mejora para que no se den este tipo de delitos en cuanto a su legislación, jurisprudencia y pronunciamiento que de igual forma en los litigios en Tribunales, sean estos delitos sancionados y no un tema aislado y que difícilmente llegue a juicio.

---

https://www.poderjudicialmichoacan.gob.mx/tribunalm/biblioteca/almadelia/Cap4.htm

Según datos recientes del Servicio Secreto de los Estados Unidos, se calcula que los consumidores pierden unos 500 millones de dólares al año debido a los piratas que les roban de las cuentas online sus números de tarjeta de crédito y de llamadas. Dichos números se pueden vender por jugosas sumas de dinero a falsificadores que utilizan programas especiales para codificarlos en bandas magnéticas de tarjetas bancarias y de crédito, señala el Manual de la ONU.

Otros delincuentes de la informática pueden sabotear las computadoras para ganarle ventaja económica a sus competidores o amenazar con daños a los sistemas con el fin de cometer extorsión. Los malhechores manipulan los datos o las operaciones, ya sea directamente o mediante los llamados «gusanos» o «virus», que pueden paralizar completamente los sistemas o borrar todos los datos del disco duro. Algunos virus dirigidos contra computadoras elegidas al azar; que originalmente pasaron de una computadora a otra por medio de disquetes «infectados»; también se están propagando últimamente por las redes, con frecuencia camuflados en mensajes electrónicos o en programas "descargados" de la red.

En 1990, se supo por primera vez en Europa de un caso en que se usó a un virus para sonsacar dinero, cuando la comunidad de investigación médica se vio amenazada con un virus que iría destruyendo datos paulatinamente si no se pagaba un rescate por la «cura».

Los delinquentes cibernéticos al acecho también usan el correo electrónico para enviar mensajes amenazantes especialmente a las mujeres. De acuerdo al libro de Barbara Jenson «Acecho cibernético: delito, represión y responsabilidad personal en el mundo online», publicado en 1996, se calcula que unas 200.000 personas acechan a alguien cada año.

Singapur, por ejemplo, enmendó recientemente su Ley sobre el Uso Indebido de las Computadoras, de acuerdo con la CNET de Singapur. Ahora son más severos los castigos impuestos a todo el que interfiera con las «computadoras protegidas» es decir, las que están conectadas con la seguridad nacional, la banca, las finanzas y los servicios públicos y de urgencia así como a los transgresores por entrada, modificación, uso o intercepción de material computadorizado sin autorización.

Hay países que cuentan con grupos especializados en seguir la pista a los delincuentes cibernéticos. Uno de los más antiguos es la Oficina de Investigaciones Especiales de la Fuerza Aérea de los Estados Unidos, creada en 1978. Otro es el de Investigadores de la Internet, de Australia, integrado por oficiales de la ley y peritos con avanzados conocimientos de informática. El grupo australiano recoge pruebas y las pasa a las agencias gubernamentales de represión pertinentes en el estado donde se originó el delito.

Pese a estos y otros esfuerzos, las autoridades aún enfrentan graves problemas en materia de informática. El principal de ellos es la facilidad con que se traspasan las fronteras, por lo que la investigación, enjuiciamiento y condena de los transgresores se convierte en un dolor de cabeza jurisdiccional y jurídico. Además, una vez capturados, los oficiales tienen que escoger entre extraditarlos para que se

> les siga juicio en otro lugar o transferir las pruebas y a veces los testigos al lugar donde se cometieron los delitos.[64]

Lo cual nos lleva a preguntarnos si existen fechas anteriores al año en curso (2025) en donde se tenía presente la importancia respecto a lo *cibernético* ¿qué sucedió para que en el caso de México sigamos en este analfabetismo *cibernético*? Que más allá de la falta de acceso por parte de la población a educación, tecnología en zonas marginadas y comunidades indígenas, lo cierto es que el analfabetismo y falta de interés se da también en el Poder Judicial, autoridades y representantes que no conocen, no les interesa y no han hecho porque se erradique esto, de igual forma brindar mecanismos legales para protección a víctimas y castigo a agresores porque puede ser muy conveniente mantener a la población en un Estado *zombie* donde la víctima siga siendo quien tiene la culpa.

Además del desinterés en que los delitos *cibernéticos* no ocurran, también tenemos el factor económico, a todo lo que implica dinero en recursos, tan sólo para destinar tecnología a la policía *cibernética*, lo cual nos hace preguntarnos ¿cómo concientizar a la población y a las autoridades, si la población no puede pensar libremente porque su prioridad es encontrar la forma de tener la canasta básica y difícilmente podrán ver a lado de cifras de víctimas?

Las autoridades deben tomar acciones al respecto e implementar y cumplir leyes, también como población nos hemos deslindado de nuestra educación y propia vida. ¿Por qué lo anterior? porque hemos olvidado que la educación comienza desde cada hogar, acción y no sólo palabra, hemos borrado el ejemplo para formar niños, jóvenes y futuros adultos respetuosos de cualquier forma de vida, despersonalizando el entorno, la mente a vivir y escapar en la que la tecnología facilita todo, pero no en la conciencia y en la formación de buenas personas (esto

[64]Naciones Unidas, *Décimo Congreso de las Naciones Unidas sobre Prevención del Delito y Justicia Penal, Salvador, Brasil*, Décimo Congreso de las Naciones Unidas sobre Prevención del Delito y Tratamiento del Delincuente, del 12 al 19 de abril de 2010, de: https://www.un.org/es/conf/xcongreso/prensa/2088hs.shtml#:~:text=Los%20denominados%20delincuentes%20cibern%C3%A9ticos%20se,fines%20pornogr%C3%A1ficos%20y%20el%20acecho.

en relación con no fomentar la violencia) sin deslindarnos en que la educación no llega por cursos o discursos, sino en el ejemplo.

Por otra parte, podemos imaginar contar con mejores leyes y gobernantes para evitar los delitos *cibernéticos*, pero no tendrían porque existir leyes más severas si no hubiera delitos o quién los realice. La formación de personas mediante educación es una tarea desde casa, desde el respeto por nuestras comunidades indígenas, la vida de los animales y todo ser vivo.

Que la educación no sea sinónimo de quien acude a la escuela porque son tareas distintas en las que la formación y respeto es indispensable sea desde los hogares.

3.1. POSICIONAMIENTO RESPECTO A LOS DELITOS CIBERNÉTICOS EN EL ÁMBITO NACIONAL E INTERNACIONAL

La vida en el mundo ha cambiado drásticamente gracias a la tecnología, podemos *viajar* en tiempo mediante videos o videollamadas, pasando de la imaginación y lo desconocido a realidades y sitios del otro lado del continente, lo cual hemos dejado de imaginar para viajar, vivir y conocer otras culturas, realidades, trabajos o estudios mediante la tecnología.

Es por ello que la tecnología debe ser usada para mejora y no para cometer delitos, por ejemplo; en Aeropuertos Internacionales como el de Brasil la tecnología ha ayudado a la detección oportuna de droga en equipajes, cámaras capaces de tener una visión oportuna por situaciones posteriores de prueba y sustancias ilícitas por medio de *scanner* y *rayos x* por personas que han ingerido droga por dinero o coacción o no, también en detectar dinero no reportado o tráfico de especies y materiales como hierbas que en otros países y ciudades son medicamentos no permitidos, excediendo lo legalmente permitido, así como lectores de huellas o fotografías para quienes son buscados en otros países por haber cometido algún delito y que los países aliados se ven para cooperar internacionalmente a ayudar a encontrar criminales. Por ejemplo:

> La Organización para la Cooperación y el Desarrollo Económico establece como delito informático "cualquier comportamiento antijurídico, no ético o no autorizado, relacionado con el procesado automático y/o transmisiones de datos". Para Téllez Valdés son "actitudes contrarias a los intereses de las personas en que se tiene a las computadoras como instrumento o fin, y las conductas típicas, antijurídicas y culpables en que se tienen a las computadoras como instrumento o fin". De estas definiciones, se interpreta que los dispositivos tecnológicos, como las computadoras, son percibidos como el vehículo, no como el bien jurídico a proteger ni como el sujeto activo.
>
> Para Aceytuno, los ciberdelitos integran numerosas actividades efectuadas por una variedad de agentes, comprende factores personales, como la ideología, y fenómenos internacionales, como la globalización o la expansión de internet. Para otros autores también son delitos cibernéticos o electrónicos porque están relacionados con computadoras y redes de internet; porque la acción típica y antijuridica se comete a través de mecanismos informáticos y/o dispositivos electrónicos; y porque se lleva a cabo utilizando un elemento informático, o vulnerando derechos del titular de un elemento informático, ya sea hardware o software. En función de esto, se considera al cibercrimen como:

el conjunto de conductas relativas al acceso, apropiación, intercambio y puesta a disposición de información en redes telemáticas, las cuales constituyen su entorno comisivo, perpetradas sin el consentimiento o autorización exigibles o utilizando información de contenido ilícito, pudiendo afectar a bienes jurídicos diversos de naturaleza individual o supraindividual.

El ciberdelito implica: 1) conductas relacionadas con el procesamiento, tratamiento y transmisión ilícita de información sin consentimiento del titular; 2) el uso de la red, dispositivos o medios electrónicos, sistemas o programas informáticos, para la transmisión, modificación o mal uso de información y datos personales; y 3) afectar bienes personales dignidad, intimidad, identidad o bienes colectivos seguridad nacional, orden público. En los delitos informáticos se distinguen los elementos subjetivo y objetivo; en el subjetivo está el dolo o voluntad deliberada de cometer el delito sabiendo que es incorrecto, la culpa o la preterintención; en el objetivo, está la acción que afecta tanto a los componentes de hardware (elementos físicos) y software (programas o sistemas) como a los instrumentos principales para perpetrar el delito o consumar el acto ilícito o antijurídico.

También se observa el sujeto activo y pasivo; el activo es quien realiza toda o una parte de la acción delictiva a través del manejo de sistemas informáticos o lugares estratégicos pueden ser personas que ingresan a un sistema informático sin intenciones delictivas, que recién se inician en la informática o empleados; y el pasivo o víctima es el titular del bien jurídico sobre el cual incurre la conducta de acción u omisión pueden ser individuos, instituciones o gobiernos que usan sistemas automatizados de información.

La Organización de las Naciones Unidas (ONU) reconoce como delitos informáticos: 1)el fraude o engaño económico con intención de conseguir un beneficio mediante sistemas informáticos; 2)la manipulación o sustracción de datos; 3)la manipulación o modificación de programas computacionales, inserción de nuevos programas o rutinas sin autorización del titular; 4)las falsificaciones informáticas, alteración de datos de documentos almacenados en forma computarizada; 5)los instrumentos como medios para cometerlos, desde computadoras, fotocopiadoras, memorias de almacenamiento de datos…

A nivel mundial se han realizado esfuerzos para reglamentar las nuevas infracciones que trajo el avance tecnológico. El Salvador realizó reformas penales buscando actualizar las herramientas para combatir estos delitos, y que las autoridades facultadas consideren como evidencia para procesos penales todos los documentos digitales, mensajes electrónicos, imágenes, videos u otros datos almacenados, recibidos o transmitidos por canales digitales o dispositivos electrónicos.

Francia implementó la Ley 88-19, sobre el acceso fraudulento a un sistema de elaboración de datos, sanciona a quien acceda, suprima, altere o modifique datos contenidos o su funcionamiento del sistema, a quien falsifique documentos informatizados con intención de causar un perjuicio y procesa a quien intencionadamente y con menosprecio de los derechos de los demás introduzca datos en un sistema de tratamiento automático de datos, suprima o modifique los Alemania con la Segunda Ley contra la Criminalidad Económica de 1986, sanciona cancelar, inutilizar o alterar datos, inclusive en modalidad de tentativa, el espionaje de datos, la estafa informática, la falsificación de datos probatorios o modificaciones y falsedades documentales.

Alemania adoptó en 1986 la Segunda Ley contra la Criminalidad Económica, sanciona el espionaje de datos, la estafa informática, la falsificación de datos probatorios o modificaciones complementarias del resto de falsedades documentales como el engaño en el tráfico jurídico mediante la elaboración de datos, falsedad ideológica o uso de documentos falsos; considera ilícito cancelar, inutilizar o alterar datos inclusive en modalidad de tentativa; así como la destrucción, deterioro, inutilización, eliminación o alteración de un sistema de datos.

Austria reformó su Código Penal en 1987, sanciona la destrucción de datos personales, no personales y programas; sanciona a quienes con dolo causen un perjuicio patrimonial a un tercero, por la introducción, cancelación o alteración de datos o por actuar sobre el curso del procesamiento de datos.

México ratificó en 2005 el Estatuto de Roma, y desde 2017 el Senado de la República ha solicitado la adhesión al Convenio de Budapest; desde 2019 se han presentado al menos 15 iniciativas en el H. Congreso de la Unión para sancionar delitos informáticos, pero no existe una ley que los reconozca y tampoco se han hecho las reformas necesarias para implementar medidas y procedimientos que los sancionen o mitiguen.

El bien jurídico protegido en estos delitos es la información (mensajes, imágenes, sonidos), los derechos que esta conlleva son los que se ven afectados por las conductas ilícitas que se realizan a través de los recursos tecnológicos, ya sea por su difusión, tratamiento o modificación, porque atenta contra derechos humanos, bienes jurídicos básicos intimidad, imagen, dignidad, libertad sexual, propiedad intelectual- y bienes jurídicos colectivos propiedad industrial, mercado, seguridad nacional y orden público…

En México los delitos informáticos no se encuentran tipificados en un ordenamiento específico, pero existen algunas definiciones en el ámbito federal y local; por ejemplo, la Ley Federal del Derecho de Autor tipifica la copia ilegal de programas de cómputo y la Ley Federal de Protección a la Propiedad Industrial tipifica la copia ilegal de topografías, como diseños industriales.

El Código Penal para el Distrito Federal castiga el espionaje; los ataques a las vías de comunicación, la violación de correspondencia; la comunicación de contenido sexual con personas menores de 18 años de edad o que no tienen capacidad para comprender el significado del hecho o que no tienen la capacidad para resistirlo; la pornografía y la violación a la intimidad sexual a través de medios digitales.

De igual forma, castiga delitos en materia de derechos de autor, el acceso ilícito a sistemas y equipos de informática, y a quien descifre o decodifique señales de telecomunicaciones, a quien transmita la propiedad, uso o goce de aparatos, instrumentos o información que permitan descifrar o decodificar señales de telecomunicaciones; a quien fabrique, comercialice, adquiera, instale, porte, use u opere equipos que bloqueen, cancelen o anulen las señales de telefonía celular, de radiocomunicación o transmisión de datos.

Tras la pandemia hubo un crecimiento de delitos informáticos en México. Un estudio de Grupo Fractalia señala que aunque internet ya era parte de la vida cotidiana para diversas actividades, el comercio electrónico tuvo un crecimiento de 108% y el uso de herramientas digitales se duplicó en los primeros meses de la pandemia. En este período, la facturación de tiendas en líneas incrementó 60% y aumentaron las amenazas cibernéticas, pues para el último trimestre de 2020

existían 75% más de probabilidades de ser víctima de un ciberdelito en comparación con 2019.

Las cifras de estos delitos de 2019 a 2021 pasaron de 300.3 millones en 2019 a 120 mil millones en 2021, un incremento de casi 400 veces, y son los ataques de ingeniería social los más frecuentes, particularmente phishing y malware, los ataques a redes de los usuarios finales de los cuales, y más del 60% estuvieron dirigidos a la banca en línea. En este sentido, sobre la ciberseguridad en México, expertos consideran que:

Las restricciones de movimiento impuestas por la pandemia de coronavirus dispararon el ciberdelito, una industria grande, diversificada y con fines de lucro, con individuos o grupos que a menudo desempeñan funciones específicas, con una división del trabajo, en su propio mercado ilícito fácilmente disponible para impulsar la actividad en otros mercados ilícitos.

Algunas instituciones mexicanas también han sido vulneradas en sus sistemas informáticos, como la Secretaría de la Función Pública, la Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros, el Banco de México o el Servicio de Administración Tributaria. Sumado a esto, la Guardia Nacional ha detectado miles de sitios web que simulan ser del gobierno federal o con fines de comercialización, en los cuales se cometen fraudes, descargas de códigos maliciosos o robo de información sensible. Por ello, son necesarias medidas políticas, tecnológicas y estratégicas dirigidas a la ciberseguridad.

Las reformas en telecomunicaciones y la Estrategia Digital Nacional han priorizado la digitalización de actividades de gobierno y servicios públicos, sin abordar la ciberseguridad; y de acuerdo con el Reporte de Ciberseguridad de la OEA y el BID en 2020, el país tiene como desafío fortalecer las capacidades del Estado para garantizar la seguridad en el ciberespacio con base en una estrategia integral y generar recursos tecnológicos y humanos apropiados para las nuevas condiciones de ciberseguridad.

Con la finalidad de analizar los delitos informáticos en las entidades mexicanas, se toma como referencia el Convenio de Budapest y el Código Penal Federal. El primero distingue los delitos en cuatro categorías: los que atentan contra la confidencialidad, integridad o disponibilidad de la información; los que tienen a la tecnología como medio; los relacionados con el contenido; y los relacionados con infracciones a la propiedad intelectual. El segundo contempla los delitos contra la indemnidad de privacidad de la información sexual, contra el libre desarrollo de la personalidad y contra de las personas en su patrimonio, además de abordar la revelación de secretos y el acceso ilícito a sistemas y equipos de informática.

Con esta consideración y puesto que no existe definición especifica de delitos informáticos en el Código Penal Federal, se propone un concepto común y características para interpretarlos, clasificándolos en cuatro tipos penales protectores de los bienes jurídicos afectados: 1)De la confidencialidad, intimidad y la identidad: revelación de secretos, violación de correspondencia, acceso informático indebido, suplantación de identidad y violación a la intimidad; 2)de la libertad y seguridad sexual, libre desarrollo de la personalidad: hostigamiento, ciberacoso, pornografía infantil o de incapaces; 3)del patrimonio: fraude, robo y

> extorsión; 4)de la fe pública: falsificación y uso indebido de documentos, sellos, contraseñas y otros.[65]

Es alarmante que no exista en México y en general en el mundo leyes que combatan la *ciberdelincuencia* mediante la *ciberseguridad*, ya que en el Código Penal Federal debería, así como la Suprema Corte de Justicia de la Nación (SCJN) combate a los delitos *cibernéticos* y precedentes para los cuales el *ciberespacio* es ajeno a la realidad por lo que puede actuar en impunidad olvidando que las consecuencias como el patrimonio, intimidad, seguridad y libertad de las personas.

Tan sólo la pérdida de patrimonio, robo y fraudes en las víctimas conlleva daños irreparables y más si se trata de una vida para poder comprar algo, años de trabajo y sacrificio o delitos como la pornografía infantil y trata de personas tan lucrativos para los criminales capaces de destrozar la vida de las personas, en donde el Estado y leyes deben velar por ellos(as) no ser indiferentes e inviolables.

La seguridad en todos los aspectos de la vida, intimidad, libertad y a la cual el Estado de derecho (donde se supone nos encontramos) debería tener presente actuar a la par del avance de la tecnología, porque no sólo se ve afectado el comercio internacional con maneras sofisticadas de operar por parte de la piratería, contrabando y demás sino desde lo micro (personal) a lo macro (como país) en poder tener la libertad de publicar algo en redes sociales y no sea utilizado con otros fines, sin protección y la no revictimización como por ejemplo la pornovenganza, porque vale la pena como sociedad cuestionarnos ¿qué puede llevar a una persona a exponer a otra y peor cuando se trata de una persona con la cual se tuvo algún vínculo sentimental o familiar, para terminar siendo como el viejo refrán *dormir con el enemigo* y actuar con total libertad desde el *ciberespacio* por la falta de leyes e interés en las autoridades incompetentes?

---

[65]Miryam Georgina Alcalá Casillas, *Delitos informáticos en México. Reconocimiento en los ordenamientos penales de las entidades mexicanas, PAAKAT: revista de tecnología y sociedad*, rev. tecnol. soc. vol.13 no.24 Guadalajara, Epub, versión On-line ISSN 2007-3607, 16-Oct-2023, Computer crimes in Mexico. Recognition in the criminal laws of the Mexican entities, Universidad Michoacana de San Nicolás de Hidalgo, Universidad Autónoma de Baja California, México, SCIELO, *op.cit*.

Más allá de los vacíos legales en tipos penales, es alarmante la *psique* en que muchas personas se encuentren dañados, porque entonces las leyes en nada valdrán si el fin por ejemplo de un psicópata es hacer daño, lo cual vulnera aún más ser víctima y se señale como si se supiera que se convive o era el futuro agresor.

Podemos entender desde las aulas de las Universidades por ejemplo la exposición de *bullying* (acoso escolar) entre compañeros(as) colegas y las mismas autoridades sobre quien pude ser víctima y a quien se le ignora, se le juega y condena, pero es en estos lugares donde podemos hacer la diferencia sin olvidar la empatía y la lucha de poder, desde el conocimiento, combatir y exigir terminen los delitos *cibernéticos*.

Las Universidades no sólo como formadoras de futuros abogados, litigantes, jueces, magistrados o cualquier puesto a desempeñar, sino con empatía desde el respeto y conciencia para situaciones de defensa de quienes pudieron ser víctimas de *ciberdelitos*, haciendo justicia mediante las leyes e impartir clases que aborden estos temas que incluso en el litigio puede ser tan *nuevo* e inexistente que no estemos preparados para ello.

El tratado internacional que condena los delitos *cibernéticos* como fue el de Budapest (Hungría) es una acción que, si bien los países en lo local no han generado para que sea universal, en lo internacional, es un precedente para aplicar en lo local y sea general la regulación, prevención y penas a los *ciberdelitos* que principalmente se tiene conocimiento gracias a los Tratados Internacionales.

> La crisis propiciada a principios de 2020 por la pandemia del COVID-19 ha puesto de relieve nuestra dependencia de una infraestructura vital que, para la gran mayoría de los ciudadanos, resulta invisible o su existencia pasa prácticamente desapercibida.
> Nuestra vida diaria gira alrededor de actividades cada vez más digitalizadas y, por consiguiente, más sensibles a amenazas cibernéticas. Cadenas de suministro de alimentos, transporte, pagos y transacciones financieras, actividades educativas, trámites gubernamentales, servicios de emergencia, y el suministro de agua energía, entre un sinnúmero de actividades, operan en la actualidad a través de tecnologías digitales…
> La ciberseguridad es crítica para nuestra prosperidad y seguridad. Las actividades cibernéticas maliciosas no sólo amenazan las economías, sino también el

> funcionamiento mismo de nuestras democracias, libertades y valores. Nuestra seguridad futura depende de que sepamos transformar la capacidad para protegernos contra las amenazas cibernéticas: tanto la infraestructura civil como la capacidad militar dependen de sistemas digitales seguros. [66]

La *ciberseguridad* es indispensable incluso para sitios *web* en donde son páginas exclusivas para búsqueda de empleo, porque no se trata de un tema exclusivo para empresas, en lo financiero, pornovenganza y corporaciones o relaciones de pareja, estamos frente a personas con o sin poder adquisitivo (víctimas).

Por ejemplo, en el caso de búsqueda de trabajo y el contraste con la realidad totalmente opuesta en la que años de estudio y sacrificios no sólo no son remunerados por situaciones laborales en cuanto a la falta de oportunidades, el salario, *toparse con posibles estafas* o trata de personas y esclavitud laboral (o de cualquier índole y en todas sus modalidades) en supuestos sitios de internet que la modernización de estos *ciberdelincuentes* para captación de víctimas u obtención de datos como fraudes es una constante en la que las personas se enfrentan y realmente no existe un prevención ni se erradica que mínimamente se tenga la tranquilidad de poder intentar el acceso a medios para laborar sin que existan este tipo de situaciones.

> El Convenio sobre ciberdelincuencia, firmado en Budapest Hungría el 23 de noviembre de 2001 y entrando en vigor el 01 de julio de 2004, es el primer tratado internacional que busca abordar los delitos informáticos y de Internet para armonizar las leyes nacionales, mejorar las técnicas de investigación y aumentar la cooperación entre las naciones. Es decir, es el primer instrumento multilateral jurídicamente vinculante para regular el ciberdelito, en el mismo sentido posteriormente surgió el Protocolo Adicional al Convenio sobre ciberdelincuencia, tipificando como delito la difusión de material racista y xenófobo a través de sistemas informáticos.
>
> Este convenio es el primer tratado internacional sobre delitos cometidos a través de Internet y otras redes informáticas, que se ocupa especialmente de las infracciones de los derechos de autor, el fraude informático, la pornografía infantil y las violaciones de la seguridad de la red. También contiene una serie de poderes y procedimientos como la búsqueda de redes informáticas y la interceptación. Su

[66]Ciberseguridad, Riesgos, *Reporte Ciberseguridad Avances y el camino a seguir en América Latina y el Caribe*, BID Mejorando Vidas, OEA más derechos para más gente, Banco Interamericano de Desarrollo, 2020, pp.10,24, de:
https://publications.iadb.org/publications/spanish/document/Reporte-Ciberseguridad-2020-riesgos-avances-y-el-camino-a-seguir-en-America-Latina-y-el-Caribe.pdf

> principal objetivo, establecido en el preámbulo, es aplicar una política penal común destinada a la protección de la sociedad contra el ciberdelito, especialmente mediante la adopción de la legislación adecuada y el fomento de la cooperación internacional.[67]

Como población hemos crecido en un entorno donde escuchar de violencia, muerte, tortura y trata de personas es *común*, tanto que generalmente resulta *común* ver a las víctimas con base en números como se ha realizado a lo largo de sexenios (en donde ya tan acostumbrados estamos como población a los casos en donde poco pueden sonar peor que otros), sin dimensionar la magnitud de cómo *el mundo va cambiando, así como las sociedades* y no nos suena alarmante tantos casos impunes, sin investigación, penas ni justicia. Lo cual en cuanto a delitos *cibernéticos* aún suena lejano, como si se tratará de un tema que especialmente se agrava por la falta de difusión, conciencia, alerta y tema de conversación para evitar sucedan.

Por ejemplo, se han realizado *experimentos sociales* donde se simulan citas a ciegas, como el que llevó a cabo *Blind Dates en Orange España* con el fin de que tres mujeres conocieran a varios hombres (quienes eran en realidad actores, pero las mujeres no) mediante *chat móviles* hasta quedar en uno (el cual ellas seleccionaban de acuerdo a preguntas que cada mujer hacía para ir descartando candidatos hasta quedarse con un hombre con quien tuvieran mayor afinidad) al final, la sorpresa fue que a quién las tres mujeres en diferente momento sin conocerse, eligieron fue al mismo hombre.

La persona mayor, pero con la capacidad de aparentar ser menor y poder ir adaptando sus respuestas a lo que se iba percatando era lo que cada mujer buscaba en un hombre. Dicho experimento buscó demostrar y evidenciar que *las redes sociales no son lo que aparentan* y que es muy fácil el engaño incluso en personas adultas y con mayor facilidad al igual que con menores de edad que se puede dar sin conocer a la persona porque cualquiera en esta máscara digital como

[67] *El estatus de México y el Convenio sobre la Ciberdelincuencia de Budapest*, En Revista Foro Jurídico, Jersain Llamas Covarrubias, septiembre 14, 2020, de: https://forojuridico.mx/el-estatus-de-mexico-y-el-convenio-sobre-la-ciberdelincuencia-de-budapest/

lo es una *red social* y el *ciberespacio* lo puede lograr, lo cual se puede terminar utilizando para cualquier delito como la trata de personas.

Organismos Internacionales como Naciones Unidas buscan aportar y difundir ante delitos denominados como *cibercrimen* para hacer referencia de los *ciberdelitos*, ante lo cual lo primero a lo que nos enfrentamos es a dar una definición general, que al ser *nuevos* la homologación comienza precisamente desde ello porque:

> No existe una definición internacional de ciberdelincuencia. En términos generales, el delito cibernético se puede describir como delitos ciberdependientes y delitos facilitados por medio de las tecnologías de información y comunicación…
> Los delitos facilitados por medio de las tecnologías de información y comunicación pueden ocurrir online y offline. Ejemplo de ellos son estafa en línea, explotación sexual infantil en línea, trata de personas, etc…
> Enfoque programático
> La estructura y el enfoque del Programa están diseñados para permitir un enfoque integral, a largo plazo y holístico para prevenir y combatir el delito cibernético en los países. El diseño modular tiene por objeto ofrecer un enfoque programático completo que se puede aplicar a nivel de país al tiempo que incorpora una perspectiva regional y global.
> 1.-Desarrollo de capacidades. El Programa Global sobre Delito Cibernético apoya el proceso de fortalecimiento de las habilidades, el conocimiento, las capacidades y los recursos de instituciones del sector justicia para contrarrestar y prevenir el delito cibernético.
> 2.-Apoyo al marco regulatorio. El Programa Global brinda asistencia normativa y legal a los Estados miembros y otras partes interesadas para prevenir y contrarrestar el delito cibernético mediante el establecimiento de procedimientos operativos estándar, pautas y legislaciones que se alinean con las prácticas y los estándares internacionales aplicables.
> 3.-Cooperación. El Programa Global fomenta las relaciones de colaboración entre los Estados miembros y el sector privado a nivel nacional e internacional para aumentar la eficiencia y eficacia de la respuesta de la justicia penal.
> 4.-Prevención. El Programa Global aumenta la conciencia sobre los riesgos del ciberdelito entre la sociedad para un mejor uso e interacción con la tecnología e Internet.
> Áreas de intervención
> 1.-Investigaciones cibernéticas. Trabajar para desarrollar y fortalecer las habilidades y capacidades de los profesionales de la justicia penal y los funcionarios encargados de hacer cumplir la ley sobre cómo prevenir, interrumpir, investigar, enjuiciar y juzgar los delitos ciberdependientes y los facilitados por medio de las tecnologías de la información y comunicación.
> 2.-Abuso y explotación sexual infantil en línea. Coordinar la detección y la respuesta entre todos los actores a los casos de abuso y explotación sexual infantil en línea y material de abuso sexual infantil, asegurando un enfoque centrado en la víctima.

> 3.-Análisis forense digital. Trabajar para desarrollar y fortalecer las habilidades y capacidades de los profesionales de la justicia penal para identificar, incautar, procesar, preservar y reportar evidencia digital.
> 4.-Evidencia digital. Trabajar para desarrollar y fortalecer las habilidades y capacidades de los profesionales de la justicia penal para identificar, comprender, solicitar, analizar, preservar y presentar evidencia digital.
> 5.-Activos virtuales. Reconociendo las características únicas de los activos virtuales, trabajar para desarrollar y fortalecer las habilidades y capacidades de los profesionales de la justicia penal y los agentes del orden público para investigar, rastrear y analizar los activos virtuales.
> 6.-Prevención. Trabajar para educar a las personas sobre el uso seguro de la tecnología para mitigar los riesgos de ser víctimas de delitos.[68]

Es importante no perder de vista que el avance acelerado de la tecnología debe contar con regulación, que si bien; en el plano legal falta mucho por hacer, podamos comenzar con no exponer nuestras vidas en ello, difundir y conversar sobre ello desde los hogares hasta las Universidades (específicamente en ellas porque son quienes forman a las futuras profesiones).

El abuso y explotación infantil no son temas *nuevos*, pero si se han diversificado y facilitado por las redes que operan para captación mediante tecnología, lo cual ha tenido gran auge en el acceso rápido y efectivo que se tiene para conocer a alguien, entablar una comunicación, conversación y citarse en persona para no regresar.

Las carencias en el hogar desempeñan un papel sumamente importante porque la ausencia de familia vulnera y suma a las carencias en la persona, así como falta de quién debería encontrarse para cuidar y ser responsable en caso de menores o en adultos que bien puede ser por trabajo o desconocimiento donde opera la delincuencia en una falsa comprensión, incluso en adolescentes, falsas ofertas laborales y poder adquisitivo (ya sea por las ganancias o por contactos e influencias) en que los *ciberdelincuentes* viven gracias a los vacíos legales, que pareciera está muy distante y lejano.

[68]Naciones Unidas, UNODC ROPAN, *Proyecto Nuevas Avenidas - Peacebuilding Fund Ciberdelito*, Programa Global de Ciberdelito, Programa Global de Ciberdelito, UNODC Oficina de las Naciones Unidas contra la Droga y el Delito, La declaración de Doha. Promover una Cultura de Legalidad, Educación para la Justicia, 2024, de: https://www.unodc.org/ropan/es/ciberdelito.html

El aporte de Naciones Unidas es avanzar no solamente en poner énfasis, acciones para atacar y prevenir los delitos *cibernéticos* que de igual forma no se limitan a la exposición o debate en ello, sino que ofrecen un enfoque para que se implementen acciones que estén dispuestos a cooperar para unificar y se vuelva universal que existen delitos que se cometen mediante la tecnología y lo que se sube a la red permanecerá siempre y por lo cual un tema aún todavía con un largo camino.

Tomar en cuenta el panorama en la era digital, evolución repentina y ferozmente acelerada tiene consecuencias que están en la vida real (no digital como en los *avatars*) tanto gobiernos como las leyes siguen pasando a último plano y es en la información, difusión, concientización y educación donde podemos ir avanzando.

3.2. SALUD MENTAL Y REPERCUSIONES.

La vida ha girado en torno a lo económico, darle valor y sentido de esta forma, hemos perdido como sociedad empatía para poder vivir desde la tranquilidad, honestidad, armonía, respeto entre todos (as) y para cualquier forma de vida (animal y vegetal). Es esto lo que ha dado paso a vivir para trabajar, despersonalizando el sentido mismo del trabajo que esta ligado a la falta de remuneración que hace aún más difícil la paz mental porque, aunque se quiera decir lo contrario, el valor del poder adquisitivo reina en todo y es lo que ha generado impunidad tan cotidiana, por ejemplo, en México que al ser empleos precarios, con malas condiciones laborales y de remuneración, las personas (jefes) pareciera tratar con máquinas y no con personas, peor aún intentar hacer ver que en el trabajo no importa el trato sino aguantar por un salario las peores condiciones.

¿Cómo intentar comprender el daño de los delitos *cibernéticos* y afectación a la vida de la víctima cuando las personas pareciera se ven unas a otras sin importar si no ayudar por lo menos no hacer mal? Las ciencias como la filosofía y psicología han tratado de darle sentido al bien y el mal, el derecho por su parte con leyes que tan difícil o imposible cumplir y la educación con ética donde se imponen años que con la creencia de que necesitamos leyes con penas más severas, como más años, aunque sea más una salida política que legalmente efectiva.

Si como sociedad se tuviera salud mental, muchos delitos serían hoy en día inexistentes, la tecnología estaría a favor de la humanidad y no facilitando impunidad ante delitos que las leyes aún no alcanzan.

Más allá de partidos políticos, debatir si el poder judicial debe o no elegirse por medio de voto, lo importante es poner sobre la mesa la necesidad de legislar y regular todo lo que abarca lo *cibernético* que las leyes no sólo existan como *un papel en una novela de ciencia ficción*, sino que sea en un Estado de derecho porque, por ejemplo:

> Las amenazas cibernéticas son cada vez más frecuentes, complejas y destructivas, y atentan contra derechos como la vida, la integridad, la salud, el patrimonio, los activos de información, la privacidad, la reputación; es más inciden en la opinión pública a través de información falsa, lo cual crea desinformación, perjudicando a niñas, niños, adultos, empresas, instituciones gubernamentales y relaciones internacionales.
>
> Por ello, el diputado Christian Von Roehrich de la Isla, de la fracción parlamentaria del PAN en el Congreso capitalino, presentó una iniciativa para crear la Ley de Ciberseguridad, la cual tiene por objeto garantizar la seguridad cibernética en la capital, y que sería una herramienta utilizada y aprovechada para la gobernabilidad.
>
> La propuesta de Ley de Ciberseguridad tiene 11 títulos integrados por 71 artículos que contemplan la estructura orgánica gubernamental que se deberá conformar a partir del momento de su promulgación.
>
> Prevé, además, la creación de la Fiscalía Especializada en Delincuencia Cibernética, la cual será la responsable de investigar los delitos cometidos en la materia, los aspectos que deberán observar las políticas públicas que involucren a las tecnologías de la información y comunicación, la rendición de cuentas de la cual serán responsables las autoridades competentes, la regulación de las relaciones entre el gobierno local y particulares cuando se observe que se puede ver vulnerada la ciberseguridad de los órganos de gobierno.
>
> En la argumentación de su propuesta, el legislador indicó que hoy en día resulta complejo medir y cuantificar las consecuencias directas e indirectas que puede tener un ataque cibernético a todas las actividades y servicios gubernamentales, sean infraestructuras críticas y/o servicios esenciales o no.
>
> Por lo que para las instituciones gubernamentales de la Ciudad de México y sus demarcaciones territoriales es prioridad la protección, en virtud de los servicios de gobierno que se prestan a la ciudadanía a través de los poderes Ejecutivo, Legislativo, Judicial y órganos autónomos.
>
> "Garantizar la seguridad cibernética de las instituciones gubernamentales es un asunto de seguridad pública que no puede postergarse más, y es el Congreso de la Ciudad de México quien debe hacer un esfuerzo histórico y sin precedentes para contar con la primera legislación en materia de ciberseguridad"...
>
> La propuesta fue turnada para su análisis y dictaminación a las comisiones unidas de Seguridad Ciudadana, y de Ciencia, Tecnología e Innovación.[69]

Las elecciones presidenciales en junio de 2024, pudieron ser bandera de preocupación y posterior ocupación para medidas desde lo legislativo en relación con los delitos *cibernéticos*, sin embargo; es triste el poco o nulo abordaje sobre temas que están afectando desde lo económico como son los fraudes hasta el acoso y posibles suicidios derivado de delitos *cibernéticos*.

[69]II Legislatura Congreso de la Ciudad de México, *Buscan crear la Ley de Ciberseguridad para la Ciudad de México*, 18 de julio de 2024, de:
https://congresocdmx.gob.mx/comsoc-buscan-crear-ley-ciberseguridad-ciudad-mexico-1936-1.html

Podríamos entender la falta de interés porque el narcotráfico ha servido para atribuir cualquier muerte a daños colaterales, no a falta de investigación, prevención y sanción. Esto entonces es una salida fácil y de justificación para *normalizar* la violencia, pero no querer voltear a ver que los delitos *cibernéticos* abarcan muchos delitos, que únicamente para y el crimen organizado.

Cuando dejamos de ser vistos como personas, para convertirnos en números y estadísticas, difícilmente podremos entender la importancia de la salud mental, que da espacio al vacío en la sociedad y las leyes, lo cual es importante tomar en cuenta para que el cuidado así como prevención sea desde la casa y de normalizar hablar de temas como por ejemplo, los de índole sexual, que no tienen como fin exponer sino explicar para prevenir y sobre todo que la familia sea el círculo de seguridad frente a cualquier situación (alzar la voz y la ley de la mano) no la razón para huir (en lo físico) o en la realidad por carencias emocionales, como económicas o que sea donde comiencen los delitos y sea normalizado.

Los juicios de *Nuremberg* intentaron dar una lección a la humanidad que aún importa que la tipicidad de los atroces delitos no estuviera en la ley no era motivo para no juzgarlos y dar el ejemplo al mundo que no se podían pasar por alto ni permitir por no estar en ese tiempo en las leyes al momento de su acción, porque quién podría imaginar se darían tan lamentables acontecimientos.

En cuanto a que los delitos que en ese tiempo no existían y por lo tanto falta de sanción, sin importar el tiempo, por la gravedad, afectación y evitar se repitan, se condenó a algunos de los lideres Nazis sin importar que en ese tiempo se tuviera o no el tipo penal porque los delitos no deben contar con herramientas legales donde el tiempo juegue a su favor, para impunidad, sumado al nulo interés por avanzar en ello siendo un ejemplo que aunque pase el tiempo, las leyes y el derecho harán justicia, que no exista un delito sobre una víctima, ni impunidad sobre el poder de cualquier tipo.

Estos juicios siembran como precedente que, sin importar el tiempo, el daño en la víctima y la reparación de ello son lo que debe prevalecer más allá de que si en el momento en que se cometieron aún no existía una definición, tipo penal y pena como los casos y consecuencias que tal vez hoy tengamos las graves cifras, pero que en un futuro será normal hablar de ello. En ese entonces y hoy en día sigue retumbando como bandera de verdad y justicia dichos juicios que deben servir para que quienes cometan delitos no queden impunes como se están dando en la actualidad con los delitos c*ibernéticos*.

3.3. ALCANCES, LÍMITES Y RIESGOS DE LOS AVANCES TECNOLÓGICOS

Es difícil imaginar que llegaría o estaríamos cerca de la famosa caricatura los *supersónicos*, en relación al avance digital y tan acelerado que hoy en día tenemos, no solamente por los medios de transporte, la medicina y las ciencias en general sino por la tecnología presente en todos los aspectos, como por ejemplo; el depósito a nómina, la forma de adquirir o vender un producto desde casa o cualquier parte (paqueterías) y comprar algo pero más porque esta vida tan lejana también puede volverse contra nosotros mismos. Muestra de ello, es la regulación para evitar que en el caso de las paqueterías sea tan fácil cobrar seguros, dar por perdido un paquete o simulación en una mafia(s) con ganancias a costa de la innovación.

La ley no ha alcanzado a la tecnología, pero la tecnología si a quién busca formas sofisticadas de obtener algo, los delitos no solo representan terrible forma en que la evolución no ha sido precisamente para mejorar, sino muestra un aspecto que no se ha querido ver y darnos cuenta que nos ha rebasado y no estamos preparados, tampoco tenemos las herramientas para repercusiones y menos sea de atención urgente a un tema que se puede observar desde todos los ámbitos.

Muestra de lo anterior es la trata de personas, los delitos *cibernéticos* como el acoso y hostigamiento que las Instituciones del Estado no cuentan ni con tecnología ni interés para perseguir esto, ayudar a las víctimas y menos en prevenir ni mostrar verdadero problema de índole psiquiátrico para quienes pagan las consecuencias de la impunidad apoyados en la tecnología.

La vida psicológica en la población ha sido tan devaluada y con prejuicios como quién se atiende psicológicamente es porque este loco(a) como si estuviéramos haciendo referencia a dinero, como si la vida no valiera al lado de poder, influencias y peor aún, a costa del sufrimiento de tantas personas como de cualquier ser vivo.

El poder adquisitivo y la tecnología se han vuelvo sinónimo, por ejemplo, en redes sociales que perder la vida por una fotografía(*selfie*) que pudo generar millones de

vistas y *like* lo valen y pese a casos así, las personas lo siguen realizando, sin pensar o entender que las redes sociales *no deben ser la vida real*, que tanto para quienes son seguidores, como quienes han tratado de generar que la vida sea lo que aparentemente muestran las redes sociales, como si cualquier otra forma de vida fuera de ellas prácticamente hiciera invisible a las personas porque los *tiktoker*[70] ganan más que quién tiene una carrera (incluso un grado como maestría o doctorado) dando el mensaje que es más importante ese *mundo virtual* y creando impunidad en una sociedad donde faltan valores en el *ciberespacio*.

Pareciera que la tecnología nos ha dado herramientas para las cuales el ser humano y las leyes aún no están listos, pero demasiado tarde para dar marcha atrás y replantear cómo debió ser la evolución de las leyes a la par a la tecnología o si en realidad la tecnología era lo que se necesitaba para que las personas estuvieran mejor, sin priorizar en temas como educación, salud mental y leyes porque la individualización del hombre (las personas, no a un género es específico) también se ha acelerado por la tecnología.

El sociólogo (polaco) *Zygmunt Bauman* nos habla de la individualidad en la que el ser humano ha respondido ante el avance de los tiempos y la diferente manera de reaccionar ante los cambios, ya sea de forma independiente aceptando nuestro destino o con miedo lo cual traería como consecuencia que posiblemente no estamos preparados y la despersonalización en el otro o sociabilización que son parte del ser humano para el desarrollo porque la modernidad e independencia hace que las personas vayan dejando de interactuar, no permite de igual la empatía hacia el otro, en que podamos entender la falta de actuación ante un delito e impunidad tan latente en el país.

[70]Se les denomina de esta forma a las personas que utilizan la aplicación de *tik tok* para subir o realizar contenido y compartirlo en dicha plataforma.

El hombre ha buscado su libertad tan individual y satisfacción de forma tan rápida que se ha olvidado que vive y necesita a la sociedad y su entorno. Como se menciona en la vida líquida de *Bauman*, pasamos de pertenecer de lo social a lo individual, es por ello que la sociedad líquida (para referirse a la modernidad) no tiene un camino:

> La «vida líquida» es la manera habitual de vivir en nuestras sociedades modernas contemporáneas. Esta vida se caracteriza por no mantener ningún rumbo determinado, puesto que se desarrolla en una sociedad que, en cuanto líquida, no mantiene mucho tiempo la misma forma. Y ello hace que nuestras vidas se definan por la precariedad y la incertidumbre constantes. Así, nuestra principal preocupación es el temor a que nos sorprendan desprevenidos, a no ser capaces de ponernos al día de unos acontecimientos que se mueven a un ritmo vertiginoso, a pasar por alto las fechas de caducidad y vernos obligados a cargar con bienes u objetos inservibles, a no captar el momento en que se hace perentorio un replanteamiento y quedar relegados…
> la vida líquida es una vida precaria y vivida en condiciones de incertidumbre constante. Las más acuciantes y persistentes preocupaciones que perturban esa vida son las que resultan del temor a que nos tomen desprevenidos, a que no podamos seguir el ritmo de unos acontecimientos que se mueven con gran rapidez, a que nos quedemos rezagados, a no percatarnos de las fechas «de caducidad», a que tengamos que cargar con bienes que ya no nos resultan deseables, a que pasemos por alto cuándo es necesario que cambiemos de enfoque si no queremos sobrepasar un punto sin retorno. La vida líquida es una sucesión de nuevos comienzos, pero, precisamente por ello, son los breves e indoloros finales sin los que esos nuevos comienzos serían imposibles de concebir los que suelen constituir sus momentos de mayor desafío y ocasionan nuestros más irritantes dolores de cabeza. Entre las artes del vivir moderno líquido y las habilidades necesarias para practicarlas, saber librarse de las cosas prima sobre saber adquirirlas.[71]

De igual forma, en lo psicológico o salud mental de las personas nos muestra una sociedad *zombie* donde la vida vale tan poco o nada que es indispensable que el derecho actúe para seguir regulando las conductas que desafortunadamente se han intentado minimizar a través del tiempo porque la despersonalización por el otro o problemas sociales ya no tienen sentido sobre la propia por lo que, si en casos la vida propia no lo tiene, menos la de cualquier otra persona.

[71]Zygmunt Bauman, *Vida líquida*, ESPA PDF, Título original: *Liquid life*, 2005 Traducción: Albino Santos Mosquera Diseño/Retoque de cubierta: Mario Eskenazi Editor digital: diegoan ePub base r1.2, pp.2,5-6, de:https://circulosemiotico.wordpress.com/wp-content/uploads/2012/10/vida-liquida-zygmunt-bauman.pdf

Podríamos cuestionar ¿por qué mencionar la sociología o la psicología y no simplemente hablar de leyes, artículos e Instituciones? La respuesta es porque cuando nos limitamos únicamente a ver a las víctimas o las acciones como legales o ilegales los delitos *cibernéticos* perdemos de vista que han entrado a nuestras vidas como un virus para el cual no existe cura, no existen *consecuencias* visibles y ni conciencia por ser algo nuevo, desconocido y porque otras ciencias de la mano de las leyes mucho pueden ayudar o atacar y prevenir, no sólo a implementar penas que en muchos casos pueden o no cumplirse y no reparar el daño en la víctima.

La sociología y la psiquiatría como ciencias nos permiten ayudar a mejorar leyes, entender y ayudar a la víctima desde una perspectiva más humana para la prevención y ser mejor sociedad donde ni siquiera sea necesario más penas, más centros de reclusión que existen Estado con impunidad en la aplicación de las leyes para no visibilizar en lo *cibernético* y cómo la tecnología nos ha rebasado. Porque como se menciona en *el hombre en busca de sentido de Viktor Frankl* el hombre desde una perspectiva de ser humano necesita ser quien tome las riendas de su vida y encuentre sentido a una vida que parece sin sentido aún en las peores situaciones (como en los campos de concentración).

El derecho necesita ir de la mano de una sociedad que ha evolucionado a pasos gigantes por la tecnología, que si bien nos ha brindado mejora, también está rebasando a la sociedad y al derecho.

Las leyes se encuentran presentes en cualquier momento de la vida sin embargo; se siguen cometiendo delitos por lo cual se tienen que continuar creando más leyes, con más años, que impliquen reparación de daño monetario porque siguen apareciendo o continuando delitos, en una sociedad donde ya existan delitos *cibernéticos*, pero hablar de una era digital cuando existe analfabetismo nos lleva a preguntarnos ¿qué está fallando? ¿las leyes, los legisladores, los servidores públicos o la sociedad? es por ello que es pertinente mencionar la salud mental en una *vida líquida* que por una parte avanzamos en un aspecto tecnológico, pero no

es esto lo que parece dar sentido a la vida para mejora, porque al parecer debería priorizar en salud mental y después en la tecnología.

Actualmente, en cuanto a la evolución de los delitos *cibernéticos* recientemente tenemos al *Cryptojacking* que es:

> El cryptojacking es un tipo de ciberdelito que consiste en el uso de manera subrepticia de la potencia de los ordenadores para generar criptomoneda.
> Esto suele ocurrir cuando, sin darse cuenta (por ejemplo, al hacer clic en un enlace desconocido enviado por e-mail o al visitar un sitio web infectado), un usuario instala un programa con secuencias de comando maliciosas que permiten al ciberdelincuente acceder al ordenador o a cualquier otro dispositivo de la víctima que esté conectado a Internet. A continuación los ciberdelincuentes utilizan programas llamados "mineros de monedas" para generar o extraer criptodivisas.
> Al tratarse de divisas digitales, para crearlas solo es necesario disponer de programas informáticos y de la potencia de los ordenadores. Las criptomonedas que más solemos ver extraídas a partir de ordenadores personales son las llamadas Monero.
> El cryptojacking puede parecer un delito inofensivo, puesto que lo único que se "hurta" es la potencia del ordenador de la víctima, pero lo cierto es que se utiliza con fines delictivos y sin el conocimiento ni consentimiento de dicha víctima, en beneficio del delincuente que crea divisas de manera ilícita. Al haber un elevado número de dispositivos infectados se generan grandes cantidades de criptomonedas, de modo que es considerado por los ciberdelincuentes como un delito lucrativo.
> Las principales repercusiones de esta minería ilícita se notan en el rendimiento. Además, pueden entrañar mayores gastos para las empresas y los particulares afectados, ya que esta actividad consume mucha electricidad y potencia de los ordenadores.[72]

Lo que podría ser un paso grande en cuanto avances, casi como fue la noticia al mundo cuando se anunció que *el hombre había llegado a la luna* (que está en duda si en realidad ocurrió cuando se dijo, cómo se mencionó o la veracidad de imágenes, que no significa que no lo sea en cuanto a ser un avance científico) las criptomonedas podrían simular avance pero de dinero en el mundo financiero y capitalista en cuanto a monedas o dinero digitales sin los bancos como intermediarios y esto puede significar riesgo, así como la falta de regulación y la

[72]INTERPOL. International police (policía internacional), *Cryptojacking: ¿Qué es el cryptojacking (minería ilícita de criptomonedas)? ¿Cómo funciona?*, 2024, de: https://www.interpol.int/es/Delitos/Ciberdelincuencia/Cryptojacking

presunción de hablar de lavado de dinero por tratarse de no ser rastreable y la facilidad para moverse en un mundo donde las leyes son inoperantes.

Este dinero *cibernético*, también denominado *bitcoin, ripple* o *leticoin*, (*criptomonedas*) puede utilizarse con fines delictivos, donde no cuentan con conocimiento las Instituciones ni la población, sólo falta de oportunidades en la adquisición de conocimiento, información o dispositivos electrónicos, cuando vorazmente ya se encuentran inmersos en este mundo *cibernético* que viene a apoyar la brecha de desigualdad tan presente.

> Gobiernos y sociedad civil deben forjar un vínculo que permita fortalecer la educación digital, fundamental para prevenir delitos cibernéticos desde el contexto preventivo, sobre todo cuando sabemos del incremento en las interacciones de las y los usuarios en aplicaciones y plataformas que utilizan internet y que conllevan grandes riesgos para su privacidad, aseveró Luis Gustavo Parra Noriega, Comisionado del Instituto de Transparencia, Acceso a la Información Pública y Protección de Datos Personales del Estado de México y Municipios (Infoem).
> Durante su participación en el panel digital a distancia, realizado por el Ayuntamiento de Puebla, en el marco del Día Municipal de la Protección de Datos Personales, Parra Noriega destacó que el uso de las nuevas tecnologías ha modificado la manera de socializar, no sólo para la población joven o adulta, sino también para niñas, niños y adolescentes, quienes aprenden rápidamente a utilizar los dispositivos para adentrarse en el mundo digital, pero que sin una guía pueden arriesgar su propia vida al exponerse a los delitos que ocurren en el ciber espacio.[73]

La educación debe prevalecer tanto en prevenir como informar porque lo *cibernético* y delitos tienen consecuencias reales en las personas, no sólo de cierta edad pese al conocimiento y prácticamente nacer con el uso de la tecnología (que podríamos pensar menores) sino *adultos* pueden contar con mayores herramientas así como la propia experiencia para no ser *blancos débiles*, sin embargo; por desconocimiento de la tecnología pueden ser presas fáciles, es por ello la importancia de enseñar desde el hogar y ser red de apoyo entre familia la desinformación, porque la falta de ello puede ser refugio para *supuestos amigos*

[73]Instituto de Transparencia, Acceso a la Información Pública y Protección de Datos Personales del Estado de México y Municipios (INFOEM), Educación digital, fundamental para prevenir delitos cibernéticos, *Educación digital, fundamental para prevenir delitos cibernéticos*, Estado de México, 31 de enero de 2022, de:
https://www.infoem.org.mx/es/contenido/noticias/educaci%C3%B3n-digital-fundamental-para-prevenir-delitos-cibern%C3%A9ticos

virtuales, citas en redes en un mundo donde cualquiera puede crear una realidad inexistente o simulada para un fin criminal.

> Los delincuentes cibernéticos a menudo emplean enfoques técnicos y sociales para cometer delitos. Es difícil prevenir algunos tipos de ciberdelitos. No obstante, los usuarios de la tecnología pueden tomar ciertas medidas para protegerse (en cierta medida) de los ciberdelitos.[74]

Tenemos el *código morse* (clave internacional mediante señales) compuestas por guiones y puntos que tienen como fin la sustitución de números o letras y de gran utilidad para la comunicación, *Samuel Morse* fue quien creó en 1830 estos códigos y a nivel internacional en 1851 ya con mezcla de diferentes lenguas (tanto del continente Americano como el Europeo). Este código es también usado mediante sonidos, lo que ya desde tiempo atrás podíamos ver en estos primeros pasos de *ciberespacio* en el que evolucionaría con códigos ya cifrados e internet.

Desafortunadamente, al no haber rastro, la *web* es cuna de *ciberdelincuentes*, que pueden actuar desde una casa donde sólo se necesita una computadora o dispositivos electrónicos, para desencadenar terrorismo porque el *hackeo* a instituciones o páginas *web*, donde se cometen delitos como la tortura llega a involucrar no sólo a quien comete el delito, sino a todos los usuarios que pagan por matar, torturar que puede ser transmitido en todo el mundo y desde cualquier parte.

Al terminar estos *espectáculos atroces*, la vida para los usuarios continua en su *normalidad*, para la víctima en una cifra más y para quienes actúan bajo este terrorismo *cibernético* sigue en la búsqueda de otra víctima, una forma más sádica para llenar el morbo de una sociedad ya dañada, con ganancias desde la comodidad de su casa (o cualquier lugar) donde lo necesario sólo es actúan en el *ciberespacio* y satisfacer a un vació social lapidado de impunidad sin verdad ni justicia y carente de todo sentido en una sociedad vacía, donde ya nadie ve el sufrimiento ajeno como importante.

---

[74]Oficina de las Naciones Unidas contra la Droga y el Delito (UNODC), *Prevención de la ciberdelincuencia*, The Doha Declaration: Promoting a Culture of Lawfulness, 2020, de: https://www.unodc.org/e4j/es/cybercrime/module-1/key-issues/cybercrime-prevention.html

CONCLUSIONES DEL CAPÍTULO

Hablar de violencia (tanto de hombres como de mujeres) y cualquier forma que dañe la vida de las personas no debe ser sólo un tema de preocupación para las autoridades del país (jueces y legisladores) sino también para la sociedad en términos de atención psicológica para que no se normalice esto.

Los delitos *cibernéticos* tan poco abordados como prioridad para legislar, prevenir y sancionar son un problema legal y psicológico, donde las víctimas no tienen mecanismos a su alcance ni justicia, porque la ley no parece estar de lado de quienes sufren delitos y menos del tipo *cibernético*. Tampoco se han actualizado las leyes conforme ha avanzado la tecnología, incluso ha resultado benéfico para quienes tan fácilmente se esconden detrás de un medio electrónico destrozar la vida de las personas, quedando impune, sin herramientas, tipificación, sanción y justicia para las víctimas porque son aparentemente *imperceptibles* cuando realmente es lo contrario.

Si bien se ha comenzado a hablar más de ello, la realidad poco o nada ha cambiado ya sea porque aparentemente no hay presupuesto, interés, ni leyes a favor de que se castigue y erradiquen estos delitos, que no sólo acaban con la vida, dignidad y derechos humanos de la víctima por el daño en la psique podría ser irreversible como en casos de suicidio a raíz de ello, incluso desde la niñez (por ejemplo, el *ciberbullying*).

El acoso, hostigamiento y demás delitos de carácter *cibernético* que sufre la persona agredida deben terminar se debe, fomentar interés real en jueces, autoridades y no se siga pensando sólo en más tecnología como *teléfonos inteligentes* (que pueden ser usados con fines contrarios a mejorar la educación o conocimiento de la ciencia) pero sin consecuencias que posiblemente que ya rebasan a las leyes y al mismo ser humano.

Hoy en día las redes sociales son determinantes para la difusión de información (comunicación y conocimiento a distancia) sin embargo; también han sido una herramienta para violentadores, infractores y personas mentalmente mal o simulan serlo para causar sufrimiento, así como exparejas que utilizan el mundo digital para destruir la vida de la víctima y tan justificables con víctimas reales, sin justicia y desechables en una sociedad donde vale más lo individual que lo colectivo por el bien general.

CONSIDERACIONES FINALES

La tecnología se ha vuelto una herramienta indispensable incluso para saber qué hora es, revisar el calendario y tener el control de cuentas bancarias por medio de aplicaciones, mensajes o correos instantáneos en alerta por realizar compras y (como modo de seguridad) evitar la impresión de *tickets* físicos y c*ódigos qr* que podemos adquirir desde una entrada al cine o paquetes para recibir o entregar.

La vida dio un giro de 180 grados a raíz de la contingencia del COVID-19, la incertidumbre, miedo y desesperanza tanto por el virus, como por la pérdida de empleos (por lo tanto la economía) y las nuevas formas de comunicación cambio la perspectiva y despersonalización de ver al otro como persona, tener más tiempo en casa utilizando la tecnología de la era digital.

Afortunadamente gracias a la tecnología en las comunicaciones (de forma virtual) así como gran parte de los empleos continuaron su rumbo hacia una realidad diferente, así como para las audiencias, que si bien ya teníamos el cambio por los juicios orales, no tuvimos (como población) tiempo de pensar, cuando ya nos encontramos frente a una realidad en la cual tanto jóvenes (quienes ya nacieron con la normalidad en la tecnología) como adultos (por ejemplo litigantes, jueces, magistrados educados en el antiguo sistema) sólo tenían dos opciones: adaptarse y aprender o quedar prácticamente excluidos(as) en *otro mundo* obsoleto, por las tecnologías y prepararnos para enfrentar una nueva época que de igual forma trajo consigo delitos en un *evolución* de modalidad que son *cibernéticos*.

Desafortunadamente, para las leyes aún son invisibles en delitos *cibernéticos* y poco tomados con seriedad para entender la necesidad de actuar no sólo en temas financieros, sino en la capacidad de contar con personas capacitadas y con equipo para auxiliar desde la red en prevención y poder actuar en caso de delitos con equipo necesario para dar seguimiento (como computadoras, redes y tecnología mejor de quienes cometen delitos).

Los delitos *cibernéticos* no son ajenos a la vida real y diaria de las personas, forman parte de la población, representan la realidad de las víctimas y la falta de justicia de la cual el país y el mundo está cansado del desinterés. La tecnología utilizada para cometer delitos no es futuro, sino presente por lo que la actuación implica serlo también; el buen uso de la tecnología representa avances significativos desde la medicina, como el conocimiento e interacción con lugares ajenos, pero el mal uso ha representado víctimas con secuelas aparentemente sutiles que derivan del mismo desinterés por otra persona.

No se trata de contextualizar los delitos *cibernéticos* en cuanto a machismo (que en todo el mundo existe en mayor o menor medida) porque en la trata de personas existen casos de (también virtual) mujeres que pudieron incluso ser inicialmente víctimas y con el paso del tiempo adquirir papeles claves para captación, sometimiento o gancho a nuevas víctimas que resulta una maniobra perfecta porque difícilmente se podría desconfiar de alguien que en teoría debería ser empática con la otra mujer (que de igual forma en relación con niños u hombres) y podría ser casi imposible imaginar que sea quien también comete delitos.

Nuestra propuesta de investigación se centra en la necesidad de universalizar en todo el país leyes que combatan los delitos *cibernéticos*, que no se trate sólo de que algunos estados que cuenten con tipos penales y otros no, deben las leyes proteger a los ciudadanos, no ser negligentes con las víctimas y ni siquiera tener un tipo penal, no se estén capacitados en el conocimiento de estos delitos y actuar mediante la ley con tecnología. Sería absurdo pensar que la única forma de atacar delitos *cibernéticos* es mediante denuncia, pero sin jurisdicción, sin actuación por desconocimiento o por falta incluso de una computadora o equipo necesario para la policía *cibernética*.

Que las autoridades competentes, protejan a la población y los litigios en torno a delitos *cibernéticos*, sin tener como problema principal la falta de conocimiento y empatía respeto a secuelas de estos delitos.

Con esta investigación comprobamos que aún falta mucho por hacer en materia de leyes, regulación, tipificación, difusión, prevención, combate, preparación tanto a autoridades competentes como a quienes imparten educación y aparato judicial, pero el interés porque no haya más víctimas, sino su protección es el primer paso a la regulación en contra de los delitos *cibernéticos*.

También es necesario que los delitos *cibernéticos* sean universales, tanto en el nombre del delito, significado, penas e interés por parte de jueces quienes legislan e imparten justicia, así como de la misma población.

Las víctimas de violencia digital tienen estigmas incluso desde que deciden poner una denuncia o compartir esto con alguien de su confianza porque se les intenta minimizar a *simplemente bloquea lo que paso o no hagas caso porque será más tu exposición, el tiempo lo cura todo*, porque no hablamos únicamente de algo que sólo ocurre en la red, se trata de violencia que se encuentra inmersa en ella y repercute en la vida de la(s) persona(s), se trata de violencia digital que no es menor que otros casos porque ni siquiera debe haber comparación entre delitos prácticamente evaluar cuál si o no es grave, porque si esto fuera así sólo habría algunos delitos y no todos los actuales y futuros.

Es importante que se erradique y castigue todo tipo de violencia, por ejemplo; el *ciberbullying* que no es ni siquiera de interés en la *ciberseguridad* por parte de las autoridades competentes, ya que el analfabetismo *cibernético* esta de la mano del desinterés constante, que al intentar exponer sufrir de *ciberacoso* se reduce a que es algo en internet y no se logra entender que no se queda sólo en redes.

Desafortunadamente, se ha entendido que la *ciberseguridad* sólo ha estado presente en el sector empresarial, como por ejemplo instituciones financieras como bancos (que han abordado y avanzado más en el combate a protegerse por delitos *cibernéticos*) en cuanto a los avisos de privacidad y protección de datos, pero no

examinado en víctimas de otro tipo de delitos de índole *cibernético* y en otros aspectos como el acoso, hostigamiento, intimidación, difamación, amenazas, etc.

La pandemia de COVID-19 aceleró utilizar medios digítales e inocentemente, podemos pensar que empezar a compartir de forma más normal fotos por ejemplo a familiares o personas a quien por contingencia no había esa cercanía, se olvidó que la publicación de las mismas no estaban seguras en la *red*.

Por ejemplo, tenemos los *metadatos*[75] y la inteligencia artificial que pueden incluso engañar al hombre porque se pueden dar dos situaciones: la primera es utilización de inteligencia digital para crear a una persona, una vida y obtener algo a cambio y la segunda, sustraer fotos reales de una persona, adaptarlas a otro lugar, cambiarle la ropa (incluso desnudarlas) y realizar tanto creación de videos con la cara de un persona mediante esta tecnología y la víctima no tener conocimiento que se realiza este tipo de actos en su contra y las repercusiones en su vida cuando no es verdad y los delincuentes con ganancias del mal uso de imagen de una persona.

Nos encontramos frente a lo que podríamos denominar como una nueva forma de esclavitud pero de índole digital porque el chantaje hacia una persona que no sea aparentemente difundida (que esto puede ser que ya estén circulando en la *red* imágenes, videos o publicaciones falsas por contar sólo con la cara de la víctima o en ciertas situaciones con el robo de material de índole comprometedor pero privado al cual estas personas obtengan acceso sin autorización) en *chats*, foros de carácter sexual sin entender que la víctima como en la trata de personas y otros delitos esté amenazada(o) incluso ni siquiera tener respeto y empatía para detenernos a pensar por un momento el no ser partícipes de ver, compartir o difundir esto porque al no haber nadie que no haga, ni lo consuma(de igual forma por chisme o morbo) no habrá porque existan estos escenarios tan lamentables.

[75]Forma para referirse a la información de datos, como los archivos.

No ser empáticos, desencadena el aumento de delitos porque se juzga a la víctima en no sólo bloquear atacantes, cuando las mismas pueden ni siquiera tener conocimiento de qué hacer, incluso denunciar puede no proceder (pese a que sea continuado en el tiempo y espacio) tampoco existen reglamentos o protocolos ante tales situaciones, amplio desconocimiento y desinterés por parte de autoridades competentes para apoyar a víctimas.

De igual forma no existe una policía en la que lo *cibernético* actúe eficazmente, si bien se dice en lo teórico que existe, la realidad es que no se lleva a cabo y menos se voltea a ver como algo grave, urgente y de emergencia. porque quien atiende un homicidio es quien (sin conocimiento, ni empatía) atiende a una víctima de carácter *cibernético*, más no especialización en cada rama y delito.

Hablar de policía *cibernética* es intentar dar pistas de prevención, como por ejemplo no acceder a correos sospechosos, no ingresar a páginas que pudieran pedir datos, no responder a llamadas que piden deposito de dinero y realmente más en torno a tener cuidado, no a actuación ante un delito, tecnología para combatir el delito y menos penas que contemplen la necesidad de una policía *cibernética* verdadera.

Comúnmente cuando se sabe de este tipo de delitos es porque la víctima lo está pasando o ya lo paso, quedando como *aprendizaje* (o no) la mala experiencia no en justicia por parte de la autoridad y apoyo de la sociedad y sus cercanos

De igual forma tanto autoridades competentes como población podemos ayudar en no tener contacto con quienes se verifique es acosador, hostigador o realice cualquier tipo de delito, porque ante la ausencia de la ley, la exposición pública del delincuente es una herramienta de lucha que ayuda y hace visible una realidad que ha rebasado a las leyes.

Debemos como sociedad ser una red de apoyo en la que no se permita que una persona hable mal de otra(o) ver, publicar o compartir material que revictimice (pese a leyes) y menos juzgar si alguien fue víctima porque distorsionar y dudar de quien padeció un delito (en este caso *cibernético*) y sobre todo de connotación sexual, nos vuelve cómplices, pero peor aún interactuar y convivir tan sólo con quién es capaz de hablar de alguien con quien se compartió un tiempo (familiar, amigo, expareja, excompañero, excolaborador, etc.) de su vida *gaslighting* [76]y ser alimento de este violentador(a) porque creer que algún delito no nos puede ocurrir es la puerta a la impunidad.

Concluimos que mediante el análisis de la legislación actual esta no es suficiente para poder prevenir, combatir ni erradicar los delitos *cibernéticos*, porque muchos de ellos ya han rebasado a las leyes y nuestras autoridades, al estar en un estado de derecho, paradójicamente el derecho no protege, como si se tratara de delitos en una realidad virtual ajena al día a día.

[76]Término que hace referencia a la historia de una mujer y su esposo que, mediante sucesos provocados por él, intenta hacerla pasar a ella como loca y como si no sucedieran, cuando en realidad él los provocaba para hacer ver y creer que ella estaba mal e inventaba cosas, lo cual era falso porque él estaba detrás de esta dolosa intención.

FUENTES CONSULTADAS

-Acosta, Maria Gabriela (Universidad Técnica de Ambato, Ecuador), Benavides, Merck Milko(Universidad Central del Ecuador, Ecuador) García, Nelson Patricio (Corte Provincial de Justicia de Tungurahua., Ecuador), Delitos informáticos: Impunidad organizacional y su complejidad en el mundo de los negocios Cybercrime: Impunity organizational and its complexity in the business of the world, Revista Venezolana de Gerencia, Universidad del Zulia, vol. 25, núm. 89, 2020, Universidad del Zulia, de:
https://www.redalyc.org/journal/290/29062641023/html/#:~:text=La%20falta%20de%20atenci%C3%B3n%20(descuido,lo%20es%2C%20el%20espionaje%20inform%C3%A1tico.

-Acurio del Pino, Santiago (Profesor de Derecho Informático de la PUCE), Delitos Informáticos: Generalidades, Profesor de Derecho Informático de la PUCE, 2024, pp.30-33, de:
https://www.oas.org/juridico/spanish/cyb_ecu_delitos_inform.pdf

-Alcalá Casillas Miryam Georgina, Delitos informáticos en México. Reconocimiento en los ordenamientos penales de las entidades mexicanas, PAAKAT: revista de tecnología y sociedad, rev. tecnol. soc. vol.13 no.24 Guadalajara, Epub, versión On-line ISSN 2007-3607, 16-Oct-2023, Computer crimes in Mexico. Recognition in the criminal laws of the Mexican entities, Universidad Michoacana de San Nicolás de Hidalgo, Universidad Autónoma de Baja California, México, SCIELO,de:
https://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S2007-36072023000100005

-Análisis jurídico-criminológico del stalking a partir de un estudio de sentencias1 Victoria Fernández-Cruz2 y José R. Agustina Universitat Internacional de Catalunya – Barcelona, International e-Journal of Criminal Sciences Artículo 3, Número 14 (2019), Supported by DMS International Research Centre, ISSN: 1988 7949, pp.2-3, de:
file:///C:/Users/javis/Downloads/21275-265-81962-1-10-20191204.pdf

-Bauman Zygmunt, *Vida líquida*, ESPA PDF, Título original: *Liquid life*, 2005 Traducción: Albino Santos Mosquera Diseño/Retoque de cubierta: Mario Eskenazi Editor digital: diegoan ePub base r1.2, pp.2,5-6, de:
https://circulosemiotico.wordpress.com/wp-content/uploads/2012/10/vida-liquida-zygmunt-bauman.pdf

-Cassou Ruiz Jorge Esteban, *Delitos informáticos en México*, pp.226-228, de:
https://escuelajudicial.cjf.gob.mx/publicaciones/revista/28/Delitos_inform%C3%A1ticos.pdf

-Código de Ética para la Prevención de la Violencia Digital Contra las Mujeres. Uso y consumo seguro de los servicios de telecomunicaciones, Gobierno de México, Secretaría de Economía, Instituto Nacional de las Mujeres (INMUJERES) y Procuraduría Federal del Consumidor (PROFECO), p.5, de:
http://cedoc.inmujeres.gob.mx/documentos_download/CodigoEticaProfecoInmujeresRev080922.pdf

-Código Penal para el Distrito Federal, Publicado en la Gaceta Oficial del Distrito Federal el 16 de julio de 2002, Cámara de Diputados del H. Congreso de la Unión, Secretaría General, Secretaría de Servicios Parlamentarios. Última reforma publicada en la Gaceta Oficial de la Ciudad de México el 29 de julio de 2020, pp. 47,49-50, de:
https://www.congresocdmx.gob.mx/media/documentos/9cd0cdef5d5adba1c8e25b34751cccfdcca80e2c.pdf

-Código Penal para el distrito Federal, Publicada en la Gaceta Oficial de la Ciudad de México el 16 de julio de 2002, texto vigente, Última reforma publicada en la G.O. CDMX el 19 de febrero de 2024, Gobierno de la Ciudad de México, Asamblea Legislativa del Distrito Federal, II Legislatura, p.58, de: https://data.consejeria.cdmx.gob.mx/images/leyes/codigos/CODIGO_PENAL_PARA_EL_DF_10.2.pdf

-Código Penal Federal, 2024, Nuevo Código Publicado en el Diario Oficial de la Federación el 14 de agosto de 1931, Últimas reformas publicadas DOF 17-04-2024, Cámara de Diputados del H. Congreso de la Unión, Secretaría General, Secretaría de Servicios Parlamentarios, pp.68-69, de: https://www.diputados.gob.mx/LeyesBiblio/pdf/CPF.pdf

-Diputadas y Diputados Locales Estado de México, Comunicado 2256, 24 de Octubre 2023, Poder Legislativo del Estado de México, *Hasta 12 años de cárcel por difundir imágenes de cadáveres: Congreso*, 2024, de: https://www.legislativoedomex.gob.mx/boletin/a93a2214-e15f-42f7-b250-6e31a67ff785

-Duran Pamplona Jonathan, Principales características, modos de perpetración y vulneración de la seguridad informática a través de la modalidad carding, Universidad Nacional Abierta y a Distancia "UNAD" Escuela de Ciencias Básicas, Tecnología e Ingeniería (ECBTI) Especialización en Seguridad Informática Bogotá, Colombia, 2020, p.25, de: https://repository.unad.edu.co/bitstream/handle/10596/34366/jduranpa.pdf?sequence=1&isAllowed=y

-El País, La mujer que denunció a su exesposo por atacar sexualmente a sus hijas gana un amparo con el que podrá reabrir el caso, México - 06 OCT 2021. de: https://elpais.com/mexico/2021-10-06/la-mujer-que-denuncio-a-su-exesposo-por-atacar-sexualmente-a-sus-hijas-gana-un-amparo-con-el-que-podra-reabrir-el-caso.html

-Gobierno de la Ciudad de México, Secretaria de las Mujeres, *Manual de Contenidos: Laboratorio de Análisis Multidisciplinario sobre Ley Olimpia*, Frente Nacional Sorodidad, Defensoras Digitales .Org, pp.5-7, de: https://semujeres.cdmx.gob.mx/storage/app/media/ViolenciaDigital/Manual_Contenidos_Lab_Ley_Olimpia.pdf

-Gobierno de la Ciudad de México, Jefatura de Gobierno, Publica Martí Batres "Ley Malena" que tipifica la "Violencia Ácida" como Delito y Garantiza Justicia a las Víctimas, 19 febrero 2024, de: https://jefaturadegobierno.cdmx.gob.mx/comunicacion/nota/publica-marti-batres-ley-malena-que-tipifica-la-violencia-acida-como-delito-y-garantiza-justicia-las-victimas

-Evaluación Nacional de Riesgos de Lavado de Dinero y Financiamiento al Terrorismo, noviembre 2023, Secretaría de Hacienda y Crédito Público, p.52, de: https://www.pld.hacienda.gob.mx/work/models/PLD/documentos/enr2023.pdf

-Fajardo Caldera, Ma Isabel; Gordillo Hernández, Marta; Regalado Cuenca, Ana Belén *Sexting: Nuevos Usos de la Tecnología y la Sexualidad en Adolescentes,* International Journal of Developmental and Educational Psychology, vol. 1, núm. 1, 2013, pp. 521-533 Asociación Nacional de Psicología Evolutiva y Educativa de la Infancia, Adolescencia y Mayores Badajoz, España, International Journal of Developmental and Educational Psychology ISSN: 0214-9877, Asociación Nacional de Psicología Evolutiva y Educativa de la Infancia, Adolescencia y Mayores, pp. 523, 524-525, de: https://www.redalyc.org/pdf/3498/349852058045.pdf

-Fiscalía General de Justicia Ciudad de México, Unidad de Inteligencia Cibernética, Policía de Investigación de la Ciudad de México, Glosario de Delitos Cibernéticos, de: https://www.fgjcdmx.gob.mx/storage/app/media/Unidad%20de%20Inteligencia%20Cibernetica/delitos-ciberneticos.pdf

-Fiscalía General de Justicia Ciudad de México, Unidad de Inteligencia Cibernética, Policía de Investigación de la Ciudad de México, Glosario de Delitos Cibernéticos, op.cit.

-Guía para Prevenir el Pharming, Secretaria de Hacienda y Crédito Público, Instituto Federal de Telecomunicaciones, pp.1-2, de:
https://ciberseguridad.ift.org.mx/files/guias_y_estudios/guia_prevenir_pharming_vf1.pdf

-Hernández Prados, Ma Ángeles; Solano Fernández, Isabel Ma, Ciberbullying, un Problema de Acoso Escolar, RIED. Revista Iberoamericana de Educación a Distancia, vol. 10, núm. 1, 2007, pp. 17-36, Asociación Iberoamericana de Educación Superior a Distancia, Madrid, Organismo Internacional, ISSN: 1138-2783, pp.23-25, de: https://www.redalyc.org/pdf/3314/331427206002.pdf

-Instituto de Formación Profesional y Estudios Superiores, Fiscalía General de Justicia de la Ciudad de México, *Ley Ingrid*, 2024, de:
https://ifpes.fgjcdmx.gob.mx/storage/app/media/2020/comunicacion/infografias/Ley_ingrid_.pdf

-Instituto Nacional de Estadística, Geografía e Informática (INEGI), comunicado de prensa núm. 404/23 13 de julio de 2023 página 1/21, comunicación social módulo sobre ciberacoso 2022, pp.1,3., de: https://www.inegi.org.mx/contenidos/saladeprensa/boletines/2023/MOCIBA/MOCIBA2022.pdf

-Instituto Nacional de Tecnologías de la Comunicación INTECO, Guía Legal Sobre Ciberbullying y Grooming, Observatorio de la Seguridad de la Información, Área Jurídica de la Seguridad y las TIC, p.4, de:
https://tumovilseguro.unam.mx/pluginfile.php/181/mod_label/intro/guia_legal_sobre_ciberbullying_y_grooming.pdf

-INTERPOL, Ciberdelincuencia, La ciberdelincuencia traspasa fronteras y evoluciona a gran velocidad, 2024, de: https://www.interpol.int/es/Delitos/Ciberdelincuencia

-INTERPOL. International police (policía internacional), Cryptojacking: ¿Qué es el cryptojacking (minería ilícita de criptomonedas)? ¿Cómo funciona?, 2024, de:
https://www.interpol.int/es/Delitos/Ciberdelincuencia/Cryptojacking

-Instituto de Transparencia, Acceso a la Información Pública y Protección de Datos Personales del Estado de México y Municipios (INFOEM), Educación digital, fundamental para prevenir delitos cibernéticos, Educación digital, fundamental para prevenir delitos cibernéticos, Estado de México, 31 de enero de 2022, de:
https://www.infoem.org.mx/es/contenido/noticias/educaci%C3%B3n-digital-fundamental-para-prevenir-delitos-cibern%C3%A9ticos

-Ilustre Colegio de la Abogacía de Madrid, p.15, de:
https://web.icam.es/bucket/Faustino%20Gud%C3%ADn%20%20Nuevos%20delitos%20inform%C3%A1ticos.pdf

-Jersain Llamas Covarrubias. El estatus de México y el Convenio sobre la Ciberdelincuencia de Budapest, Foro Jurídico, septiembre 14, 2020, de:
https://forojuridico.mx/el-estatus-de-mexico-y-el-convenio-sobre-la-ciberdelincuencia-de-budapest/

-La violencia de género en línea contra las mujeres y niñas, Guía de conceptos básicos, OEA/CICTE, OEA/CIM/MESECVI, Secretario General Organización de los Estados Americanos (Arthur Weintraub), Secretario de Seguridad Multidimensional Organización de los Estados Americanos (Alison August Treppel) Secretaria Ejecutiva Comité Interamericano contra el Terrorismo (CICTE) Alejandra Mora Mora Secretaria Ejecutiva Comisión Interamericana de Mujeres (CIM) Equipo Técnico de la OEA Programa de Ciberseguridad Kerry-Ann Barrett Mariana Cardona Gabriela Montes de Oca Fehr Comisión Interamericana de Mujeres / Mecanismo de Seguimiento de la

Convención de Belém do Pará Luz Patricia Mejía Guerrero Alejandra Negrete Morayta, Katya N. Vera Morales, apoyo financiero del Gobierno de Canadá, p.50, de: https://www.oas.org/es/sms/cicte/docs/Guia-conceptos-basicos-La-violencia-de-genero-en-linea-contra-las-mujeres-y-ninas.pdf

-II Legislatura Congreso de la Ciudad de México, Buscan crear la Ley de Ciberseguridad para la Ciudad de México, 18 de julio de 2024, de: https://congresocdmx.gob.mx/comsoc-buscan-crear-ley-ciberseguridad-ciudad-mexico-1936-1.html

-Ley General de Acceso de las Mujeres a una Vida Libre de Violencia, Ley de Acceso de las Mujeres a una Vida Libre de Violencia de la Ciudad de México, Capítulo IV ter, De la violencia digital y mediática, de: https://www.ssc.cdmx.gob.mx/storage/app/media/Subsecretaria%20de%20Inteligencia%20e%20investigacion%20Policial/Policia%20Cibernetica/Imagenes/violencia%20digital/MARCO%20LEGAL.pdf

-Leyre Hernández Díaz, El Delito Informático, Investigadora en formación Beca pre-doctoral, Eguzkilore Número 23. San Sebastián diciembre 2009, Gobierno Vasco, pp. 227-228, 230, de: https://www.ehu.eus/documents/1736829/2176697/18-Hernandez.indd.pdf

-Loredo González Jesús Alberto y Aurelio Ramírez Granados, Delitos informáticos: su clasificación y una visión general de las medidas de acción para combatirlo, FCFM-UANL Facultad de Ciencias Físico Matemáticas Universidad Autónoma de Nuevo León San Nicolás de los Garza, Nuevo León, México, Investigación/ Seguridad en ti, Celerinet, enero-junio 2013, p.45.

-Naciones Unidas, Décimo Congreso de las Naciones Unidas sobre Prevención del Delito y Justicia Penal, Salvador, Brasil, Décimo Congreso de las Naciones Unidas sobre Prevención del Delito y Tratamiento del Delincuente, del 12 al 19 de abril de 2010, de: https://www.un.org/es/conf/xcongreso/prensa/2088hs.shtml#:~:text=Los%20denominados%20delincuentes%20cibern%C3%A9ticos%20se,fines%20pornogr%C3%A1ficos%20y%20el%20acecho.

-Ochoa Serafín Maricela, Delitos Informáticos en México. Conozca las leyes y las multas, DIGIXEM 360, Digital for Empowerment, 01 Dic 2023, de: https://www.itmastersmag.com/ciberseguridad/delitos-informaticos-en-mexico-que-dice-la-ley/

-Oficina de las Naciones Unidas contra la Droga y el Delito (UNODC), Prevención de la ciberdelincuencia, The Doha Declaration: Promoting a Culture of Lawfulness, 2020, de: https://www.unodc.org/e4j/es/cybercrime/module-1/key-issues/cybercrime-prevention.html

-Padilla Espinosa Miriam J., Universidad Nacional Autónoma de México (UNAM), Revista Seguridad |1 251 478, 1 251 477| Revista bimestral, Coordinación de Seguridad de la Información (UNAM CERT), Seguridad de la Información, Pescando Información Phishing, de: https://revista.seguridad.unam.mx/numero-02/pescando-informaci%C3%B3n-phishing#:~:text=El%20Phishing%20consiste%20en%20el,nombres%20de%20usuario%20y%20contrase%C3%B1as.

-Poder Judicial de Michoacán, Biblioteca artículos electrónicos, Capitulo IV. Legislación en diferentes países sobre los delitos informáticos, 2024, de: https://www.poderjudicialmichoacan.gob.mx/tribunalm/biblioteca/almadelia/Cap4.htm

-Protección Datos y Prevención de delitos, Agencia Española de Protección de Datos, p.2, de: https://www.aepd.es/guias/guia-proteccion-datos-y-prevencion-de-delitos.pdf

-Reporte Ciberseguridad, BID Mejorando Vidas, OEA más derechos para más gente, Banco Interamericano de Desarrollo, Ciberseguridad, Riesgos, Avances y el camino a seguir en América Latina y el Caribe. 2020, pp.10,24, de:
https://publications.iadb.org/publications/spanish/document/Reporte-Ciberseguridad-2020-riesgos-avances-y-el-camino-a-seguir-en-America-Latina-y-el-Caribe.pdf

-Revista Digital INESEM, Escuela de líderes Masters Online, Cursos y Postgrados, INESEM Business School,12/06/2024, De:
https://www.inesem.es/revistadigital/informatica-y-tics/para-que-sirve-la-deep-web/

-Sain Gustavo, Cibercrimen y Delitos Informáticos. Los nuevos tipos penales en la era de internet, ERREIUS, Dirección Nacional del Derecho de Autor. Hecho el depósito que marca la ley 11723, ISBN 978-987-4405-56-2, p.7, 2018, de:
https://www.pensamientopenal.com.ar/system/files/2018/09/doctrina46963.pdf

-Secretaria de las Mujeres, Gobierno de la Ciudad de México, Prevención y visibilización del ciberacoso contra las mujeres y niñas, ¿Qué es la violencia cibernética contra las mujeres?, 2024,de:
https://www.semujeres.cdmx.gob.mx/violencia-cibernetica-contra-mujeres/identificala

-Secretaria de las Mujeres, Gobierno de la Ciudad de México, Visibilización y prevención de la violencia cibernética contra las mujeres y niñas, 2024, de:
https://www.semujeres.cdmx.gob.mx/violencia-cibernetica-contra-mujeres

-Servicio de Noticias de la Mujer de Latinoamérica y el Caribe (SEMLAC), Aprueba congreso de Baja California la Ley Alina, que exime a las mujeres por actuar en legítima defensa, Sem México La mujer es notica, 27/08/2023, de:
https://semmexico.mx/aprueba-congreso-de-baja-california-la-ley-alina-que-exime-a-las-mujeres-por-actuar-en-legitima-defensa/

-Téllez Valdés Julio. Director de Estudios Superiores del Instituto de Investigación en Computación Electrónica (ICEL). Asesor de la Cámara Federal de Diputados en México, Doctor en Derecho, Informática y Derecho, *Los "Delitos Informáticos": Situación en México*, pp.462-464, de:
file:///C:/Users/javis/Downloads/Dialnet-LosDelitosInformaticos-248768.pdf

-United Nations (Naciones Unidas), UNODC ROPAN, Proyecto Nuevas Avenidas - Peacebuilding Fund, Ciberdelito, Programa Global de Ciberdelito, Programa Global de Ciberdelito, UNODC Oficina de las Naciones Unidas contra la Droga y el Delito, La declaración de Doha. Promover una Cultura de Legalidad, Educación para la Justicia, 2024, de:
https://www.unodc.org/ropan/es/ciberdelito.html

-Valencia Álvarez Armando. Revista de la Facultad de Derecho de la Universidad Veracruzana, Publicación semestral, número dos, Impacto de los delitos informáticos en la sociedad actual, abril 2020, pp.3-4, de:
https://www.uv.mx/derecho/files/2019/04/Revista-de-la-Facultad-de-Derecho-No-3-Impacto-de-los-delitos-informaticos-en-la-sociedad-actual.pdf