Análisis de los delitos cibernéticos en el estado de Puebla a la luz del derecho nacional e internacional

Romero Aponte, Elba Jahana Thanayri

2021-01

********UNIVERSIDAD IBEROAMERICANA PUEBLA**

Estudios con Reconocimiento de Validez Oficial Por Decreto Presidencial del 3 de abril de 1981

ANÁLISIS DE LOS DELITOS CIBERNÉTICOS EN EL ESTADO DE PUEBLA A LA LUZ DEL DERECHO NACIONAL E INTERNACIONAL

TESINA

Que para obtener el título de Licenciado en

DERECHO

Presenta

Elba Jahana Thanayri Romero Aponte
Ivana Vásquez Contreras
Marifer Ortiz Ballhaus

Directora del Trabajo de Titulación:
Mtra. Ana María Estela Ramírez Santibañez

San Ándres Cholula, Puebla Otoño 2020

A mis padres, por todo su esfuerzo y apoyo incondicional para lograr terminar mis estudios.
A mis demás seres queridos, que siempre han estado de mi mano dándome fuerzas para seguir adelante.
A todos, con todo mi amor y cariño.

-Elba

A mi mamá, por su amor, por motivarme, apoyarme y darme la fortaleza para seguir adelante.
A mi papá, por todo su apoyo, amor y esfuerzo, gracias por siempre creer en mi y enseñarme que con trabajo y constancia todo se puede lograr.
A mis abuelos por ser unos pilares en mi vida, siempre dándome amor incondicional.

- Ivana

A mi papá, por su excepcional apoyo en mis estudios desde que era niña, por todo el esfuerzo y sacrificio para brindarme educación de calidad, por forjarme de valores como la constancia y la dedicación, y enseñarme a dar todo de mí; así mismo, por apoyarme en mis decisiones e impulsarme a seguir mis sueños.

A mi mamá, por su amor incondicional, por guiarme con rectitud y valores en la vida, por ser un ejemplo de fuerza y valentía, por siempre creer en mí, por enseñarme a conducirme con fe cada día.

Padres, son mi fortaleza e inspiración, les estoy eternamente agradecida y les amo con todo mi corazón.

A todos mis familiares por su cariño, sus consejos, por ser un sostén y llenarme de esperanza y alegría.

A Dios por sus infinitas bendiciones, por iluminar mi vida con unos maravillosos y ejemplares padres, por la salud y la sabiduría que hasta hoy me ha dado, las cuales me permitieron culminar esta valiosa etapa de mi vida.

-Marifer

SIGLAS Y ABREVIATURAS

CNI: Centro Nacional de Inteligencia

INTERPOL: Organización Internacional de Policía Criminal

INEGI: Instituto Nacional de Estadística y Geografía

ONU: Organización de las Naciones Unidas

TICs: Tecnologías de la Información

ÍNDICE

INTRODUCCIÓN

El presente trabajo de investigación se realizó debido a la emergente necesidad de una respuesta a las nuevas conductas ilícitas que se están generando en la sociedad debido a la globalización y el acelerado desarrollo de las TICs. Como resultado de lo anterior, el uso del internet ha quedado desmesurado, al ser una red mundial en la que los usuarios acceden a ella cada instante, sin saber los riesgos que ello implica debido a que no cuentan con una verdadera protección en su vida personal, patrimonial y en general en su esfera jurídica.

En el primer capítulo, para comenzar a adentrarnos al tema a tratar, se definen los delitos cibernéticos y las modalidades que existen de estos, así como la afectación que han generado al desarrollo de cada individuo y a la sociedad en general.

En el segundo capítulo se investigaron las diferentes leyes que existen en materia de delitos cibernéticos a nivel internacional y a nivel nacional, dando pauta a un análisis comparativo entre la regulación que le dan los países extranjeros a dichos ilícitos y los alcances que hasta ahora le han dado en nuestro país.

En el tercer y último capítulo decidimos enfocarnos particularmente al Estado de Puebla analizando su Código Penal, el cual es la única ley que prevé tales delitos, en donde a pesar de estar supuestamente regulados se encuentran meras deficiencias sobre la materia y por ende en su regulación; es por ello, que vimos la necesidad de dar a conocer los delitos cibernéticos que frecuentemente están sucediendo en el Estado y cómo estos no van más allá del conocimiento informativo del público, dejando a un lado y coartando la transparencia que se le da al seguimiento de dichos delitos.

¿Cómo se manejaría la sociedad si los delitos cibernéticos se determinarán de forma más precisa en los códigos penales de los estados mexicanos?, revisando el caso en

concreto de Puebla, se demuestra que es necesario un cambio y una reforma para contar con una legislación completa la cual daría lugar a una plena certeza jurídica de los ciudadanos.

CAPÍTULO I

LOS DELITOS CIBERNÉTICOS

1.1 DEFINICIÓN

Los delitos cibernéticos, también conocidos como delitos informáticos, han tenido muchas definiciones a lo largo de la historia, muchos autores han dado su mayor esfuerzo por definirlo, Nidia Callegari define al delito informático como *"aquel que se da con la ayuda de la informática o de técnicas anexas".*[1] Este concepto tiene el inconveniente que no abarca que también lo informático puede ser el objeto de la infracción y no solo ser un medio de la comisión del delito.[2]

Davara Rodríguez lo define como *"La realización de una acción que, reuniendo las características que delimitan el concepto de delito, sea llevada a cabo utilizando un elemento informático y/o telemático, o vulnerando los derechos del titular de un elemento informático, ya sea hardware o software"* [3]*.*

Mientras que, Julio Téllez Valdés conceptualiza al delito informático como *"Una forma típica y atípica, entendiendo por la primera a "las conductas típicas, antijurídicas y culpables en que se tienen a las computadoras como instrumento o fin" y por las segundas "Actitudes ilícitas en que se tienen a las computadoras como instrumento o fin".*[4]

---

[1] CALLEGARI, Nidia "Delitos Informáticos y Legislación" 2015, p. 113.https://egov.ufsc.br/portal/sites/default/files/6054-12231-1-sm.pdf

[2] *Cfr.* ACURIO DEL PINO, Santiago," Delitos informáticos: generalidades", 2016, pp.10-14, https://www.oas.org/juridico/spanish/cyb_ecu_delitos_inform.pdf

[3] RODRIGUEZ DAVARA, Miguel Angel. Manual de Derecho Informático. *Revista Chilena de Derecho Informático*, 2002, pp.177-180

[4] TÉLLEZ VALDÉS, Julio *Los Delitos informáticos. Situación en México, Informática y Derecho* Nº 9, i UNED, Centro Regional de Extremadura, Mérida, 1996, pp. 10-11.

Como ya se destacó, existen diferentes enfoques doctrinales al momento de hablar de delitos cibernéticos, ya que no existe solo una forma específica de realizar este tipo de delitos, sino, múltiples maneras.

Como bien establece el derecho penal, se necesitan dos sujetos para la existencia de un delito, en este caso, contamos con un sujeto activo que son aquellas personas que cometen los delitos informáticos y que cuentan con habilidades para el manejo de los sistemas informáticos o realizan dichos actos desde lugares estratégicos donde pueden acceder a información de carácter confidencial. Por otra parte, el sujeto pasivo es la persona titular del bien jurídico que el legislador protege y sobre la cual recae la actividad típica del sujeto activo. Estos pueden ser individuos, instituciones crediticias, gobiernos, etcétera que usan sistemas automatizados de información, generalmente conectados a otros.[5]

Es importante conocer a los sujetos de este delito ya que al tener una certeza del modus operandi del activo se podrían prever las acciones que conllevan a la comisión del delito, brindando así una seguridad jurídica al sujeto pasivo.

De acuerdo con la ONU, pocos instrumentos legales internacionales o regionales definen el delito cibernético, toda vez que el término da lugar a diferentes interpretaciones en donde el Convenio sobre Ciberdelincuencia del Consejo de Europa, ni la Convención de la Liga de los Estados Árabes ni el proyecto de Convención de la Unión Africana lo definen. encontrando que, El Acuerdo de la Comunidad de los Estados Independientes y el Acuerdo de la Organización de Cooperación de Shanghái lo contemplan en términos generales dejando de forma ambigua sus objetivos, características y el modus operandi de estos mismos.[6]

Por tanto, se infiere que en materia internacional no existe una definición en concreto, por lo consiguiente su regulación ha sido un arduo trabajo. Las consecuencias que conlleva la existencia del Internet y el cómo esto nos facilita la entrada a las redes internacionales ha dado lugar a que se cometa un sin fin de delitos informáticos y que

[5] *Cfr.* ACURIO DEL PINO, Santiago, *op. cit.* pp. 15-19

[6] *Cfr.* "Estudio exhaustivo sobre el delito cibernético", *United Nations Office on Drugs and Crime,* 2013, p.14 https://www.unodc.org/documents/organized-crime/cybercrime/Cybercrime_Study_Spanish.pdf

estos se queden impunes; por consecuencia, el derecho internacional en su mejor intento de dar un encuadre a este tipo de delito establece que, “Es cualquier acción ilegal en que una computadora es herramienta u objeto del delito". "Cualquier incidente asociado con tecnología de cómputo en que una víctima sufre o puede sufrir pérdida y una intromisión intencional, propiciando o pudiendo propiciar una ganancia".[7]

En un sentido amplio, es cualquier conducta criminal que en su ejecución utilice el uso de la tecnología electrónica por medio de dispositivos como computadoras o cualquier otro dispositivo electrónico como un método, fin o medio, para la realización de dichos delitos.

Es así que, los delitos informáticos son una subespecie de los delitos electrónicos que tiene como denominador común el uso de la computadora para realizar actividades criminales que, en un primer momento, los países han tratado de encuadrar en figuras típicas de carácter tradicional tales como robo, fraude, falsificaciones, daños, estafa, sabotaje, entre otros. Sin embargo, debe destacarse que el uso de las computadoras ha propiciado, a su vez, la necesidad de regulación por parte del derecho para sancionar conductas.[8]

Como señala Camacho Losa, en todas las facetas de la actividad humana existen el engaño, las manipulaciones, la codicia, el ansia de venganza, el fraude, en definitiva, el delito. Desgraciadamente es algo consustancial al ser humano y así se puede constatar a lo largo de la historia.[7]

Es evidente, la falta de regulación y lagunas que existen sobre los delitos cibernéticos, es por ello que estos son de actual trascendencia, pues dichas conducta antisociales y antijurídicas afectan de manera directa al entorno social, en especial a las nuevas generaciones que dependen completamente del uso del internet y las redes sociales, por lo que son un sector vulnerable, que se convierte en las principales víctimas de los delitos que se señalan en el presente estudio.

[7] ACURIO DEL PINO, Santiago, *op. cit.* p. 7

[7] DELGADO GRANADOS, María de Lourdes, “Delitos informáticos, delitos electrónicos”, Orden Jurídico, p.5, información visible en: http://www.ordenjuridico.gob.mx/Congreso/pdf/120.pdf [Fecha de consulta: 02 de octubre de 2020]

[8] Información visible en: https://centrosconacyt.mx/objeto/delitosinform/ [Fecha de consulta: 04 de Octubre 2020]

1.2 TIPOS DE DELITOS CIBERNÉTICOS

Los delitos cibernéticos con el paso del tiempo han ido desarrollándose y ampliando sus modalidades, existe una gran variedad de crímenes de este tipo en la actualidad, debido al avance de la tecnología, y la fácil disponibilidad de las personas para acceder a ellos.

La doctrina propone diversas clasificaciones de tipos de delitos cibernéticos, por lo que haremos mención de algunas de ellas:

Julio Téllez Valdés los clasifica como: [8]

- Instrumento o medio: se encuentran aquellas conductas que se valen de las computadoras como método, medio o símbolo en la comisión del ilícito.

- Como fin u objeto: Se encuadran las conductas dirigidas en contra de la computadora, accesorios o programas como entidad física.

Por otra parte, Ronaldo Alvarado y Ronald Morales establecen una más completa: [9]

Delitos contra la Integridad -

Daño informático.

- Falsificación informática.
- Fraude informático.

[8] TÉLLEZ VALDÉS, Julio, *Derecho Informático*, 4ª ed., México, Mc Graw-Hill, 2008, p.190

[9] ALVARADO, Rolando y MORALES, Ronald, *Cibercrimen*, s.f., España, Ius ediciones, 2012, p. 17 y 18

Delitos contra la Disponibilidad

- Violación a la Disponibilidad.

Delitos contra la Confidencialidad -

Espionaje informático.

- Acceso ilícito.
- Reproducción de dispositivos de acceso.

- Interceptación ilícita.

Delitos de pornografia infantil

Delitos contra la Propiedad Intelectual e Industrial

Si bien, la Organización Internacional de Policía Criminal (INTERPOL) enlista una diversidad de modalidades relacionadas con el contexto actual y el uso de las redes sociales, las cuales se mencionan a continuación:[10]

- Ataques contra sistemas y datos informáticos
- Usurpación de la identidad
- Distribución de imágenes de agresiones sexuales contra menores
- Estafas a través de Internet Intrusión en servicios financieros en línea
- Difusión de virus Botnets
- Phishing
- Acceso a material inadecuado
- Acoso
- Sexting
- Ciberbullying
- Cibergrooming

---

[10] *Cfr.* LOREDO GONZALEZ, Jesús Alberto, "Delitos informáticos: su clasificación y una visión general de las medidas de acción para combatirlo", Universidad Autónoma de Nuevo León, 2013, p. 45 y 46, información visible en: http://eprints.uanl.mx/3536/1/Delitos_informaticos.pdf [Fecha de consulta: 20 de octubre de 2020]

Es necesario comprender los delitos más importantes que se cometen por medio del internet, por lo que se desarrollarán y definirán a continuación una lista de los ciberdelitos más comunes en la sociedad.

El *ciberfraude*, es la producción de un perjuicio patrimonial mediante la manipulación o alteración de datos o programas de sistemas informáticos.[11]

Dentro de estos, existen distintos tipos, e.g. (por ejemplo): *los datos falsos o engañosos (Data diddling)*, conocido también como introducción de datos falsos, es una manipulación de datos de entrada al computador con el fin de producir o lograr movimientos falsos en transacciones de una empresa; *manipulación de programas o Caballos de Troya,* el cual consiste en insertar instrucciones de computadora de forma encubierta en un programa informático para que pueda realizar una función no autorizada al mismo tiempo que su función normal; *técnica del Salami (Salami Technique),* donde a partir de transacciones financieras se retira una cantidad imperceptible de una cuenta y se transfieren a otra.[12]

El phishing, es una modalidad de fraude informático diseñada con la finalidad de robarle la identidad al sujeto pasivo. El delito consiste en obtener información tal como números de tarjetas de crédito, contraseñas, información de cuentas u otros datos personales por medio de engaños. Este tipo de fraude se recibe habitualmente a través de mensajes de correo electrónico o de ventanas emergentes.[13]

El *sabotaje informático***,** es el acto de borrar, suprimir o modificar sin autorización funciones o datos de computadora con intención de obstaculizar el funcionamiento normal del sistema. Las técnicas que permiten cometer sabotajes informáticos son la *bombas lógicas (logic bombs)*, es una especie de bomba de tiempo que debe producir daños posteriormente, esta puede utilizarse como instrumento de extorsión y se

[11] MAYER LUX, Laura y OLIVER CALDERÓN, Guillermo, "El delito de fraude informático: concepto y delimitación", Revista chilena derecho tecnológico, 2020, vol.9, n.1, información visible en: https://scielo.conicyt.cl/scielo.php?pid=S0719-25842020000100151&script=sci_arttext [Fecha de consulta: 20 de octubre 2020]
[12] ACURIO DEL PINO, Santiago, *op. cit.* p. 23
[13] *Idem.* p. 24

puede pedir un rescate a cambio de dar a conocer el lugar en donde se halla la bomba.[14]

Ciberbullying, 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.[15]

Ciberterrorismo, es el acto de hacer algo para desestabilizar un país o aplicar presión a un gobierno, utilizando métodos clasificados dentro de los tipos de delitos informáticos, especialmente los de Sabotaje, sin que esto pueda limitar el uso de otro tipo de delitos informáticos, además lanzar un ataque de terrorismo informático requiere de muchos menos recursos humanos y financiamiento económico que un ataque terrorista común.[16]

Fuga de datos (data leakage), también conocida como la divulgación no autorizada de datos reservados, es una variedad del espionaje industrial que sustrae información confidencial de una empresa.[17]

Suplantación de personalidad (impersonation), En este caso, el delincuente utiliza la suplantación de personas para cometer otro delito informático por medio de artimañas y engaños tendientes a obtener el acceso a los sistemas o códigos privados de programas generalmente reservados a una empresa u organización**.**[18]

[14] *Cfr. Idem.* p.25
[15] *Vid.* CORONA, Pablo, *¿Qué es el ciberbullying?*, Gobierno de México, 2016, información visible en: https://www.gob.mx/ciberbullying/articulos/que-es-el-ciberbullying [fecha de consulta: 05 Octubre 2020]

[16] ACURIO DEL PINO, Santiago, *op. cit.* p. 27
[17] *Ibidem*
[18] *Cfr. Ídem.* p. 28

*Acceso a material inadecuado***,** existe una red conocida como Deep Web (Internet profunda) es el conjunto de sitios que contienen material potencialmente peligroso para el usuario, no solo de índole sexual, también existen, videos snuff (grabaciones de asesinatos, violaciones, torturas y otros crímenes reales), mercado negro online (tráfico de armas, drogas, trata de personas, etc.), contratación de asesinos, no existen límites para la gravedad del contenido que se puede encontrar.[19]

Sexting, este término hace referencia al uso de móviles para mantener charlas de índole sexual, donde voluntariamente se genera contenido que implique una situación

erótica o sexual. Si bien en ningún momento se obliga a la persona a posar y la mayoría de las veces se busca mantener el anonimato, existe un riesgo de identificación lo que resultaría en serios problemas sociales, de acoso y/o extorsión.[20]

Pornografía infantil, cualquier representación, por cualquier medio, de un niño participando en actividades sexuales explícitas, sean reales o simuladas, o cualquier representación de las partes sexuales de un niño, cuya característica dominante sea la representación con fines sexuales.[23]

*Grooming***,** es el conjunto de estrategias que una persona adulta desarrolla para ganarse la confianza del menor a través del Internet con el fin último de obtener concesiones de índole sexual.[21]

1.3 AFECTACIÓN DE LOS DELITOS CIBERNÉTICOS EN NUESTRO DESARROLLO

A lo largo del último siglo, las relaciones sociales han sido un punto clave en nuestras vidas, estas relaciones también se han visto afectadas debido a la globalización y al gran avance del Internet y las TICs, ya que se han desencadenado una serie de

[19] LOREDO GONZALEZ, Jesús Alberto, *op. cit.* p. 47
[20] *Cfr.* IBARRA SÁNCHEZ, Ernesto, "Protección de niños en la red: sexting, ciberbullying y pornografía infantil", México, UNAM,Instituto de Investigaciones Jurídicas, p. 87, informacion visible en: https://archivos.juridicas.unam.mx/www/bjv/libros/8/3646/5.pdf [Fecha de consulta: 17 de octubre de 2020] [23] *Ídem.* p. 95
[21] *Ídem.* p. 88

conductas derivadas del uso indebido de estos, que a la postre han generado una multiplicidad de riesgos en el desarrollo de la esfera jurídica de la sociedad.[22]

Si bien, el Dr. Santiago Acurio del Pino menciona que los principales bienes jurídicos tutelados que son afectados por estos delitos son: el patrimonio, la reserva, la intimidad y confidencialidad de los datos, la seguridad o fiabilidad del tráfico jurídico y probatorio, así como el derecho de propiedad.[23]

> Por tanto diremos que el nacimiento de esta nueva tecnología, está proporcionando a nuevos elementos para atentar contra bienes ya existentes (intimidad, seguridad nacional, patrimonio, etc.), sin embargo han ido adquiriendo importancia nuevos bienes, *como sería la calidad, pureza e*

> *idoneidad de la información en cuanto tal y de los productos de que ella se obtengan; la confianza en los sistemas informáticos; nuevos aspectos de la propiedad en cuanto recaiga sobre la información personal registrada o sobre la información nominativa*.[24]

Por lo que consideramos que dichos delitos están adquiriendo una mayor fuerza en el ámbito jurídico, ya que en la actualidad no sólo se ven afectados los bienes jurídicos principales ya mencionados, correspondientes a las primeras generaciones de derechos humanos, sino otros de trascendencia novedosa, que son los de la cuarta generación.

Como se sabe, la mayoría de los delitos cibernéticos no son denunciados ni reportados a las autoridades correspondientes ya que, las víctimas de estos tienen una acepción negativa del sistema jurídico penal por lo que mucho menos podrían confiar en la eficacia de un proceso enfocado a este tipo de delitos, siendo así que ni siquiera tienen conocimiento de las autoridades cibernéticas existentes. Aunado a esto, existe una situación de desventaja, ya que los delitos informáticos son difíciles de perseguir, pues los sujetos activos actúan sigilosamente y desde el anonimato, ya

---

[22] *Cfr.* LOREDO GONZALEZ, Jesus Alberto, *op. cit.* p. 47

[23] ACURIO DEL PINO, Santiago, *op. cit.* p. 22

[24] MAGLIONA MARKOVICTH, Claudio Paul, *et al.*, *Delincuencia y Fraude Informático, Jurídica de Chile*, 1999, *op. cit.* ACURIO DEL PINO, Santiago,"Delitos informáticos: generalidades", 2016, p. 22, Información visible en: https://www.oas.org/juridico/spanish/cyb_ecu_delitos_inform.pdf [Fecha de consulta: 18 de octubre de 2020]

que cuentan con técnicas de cifrado, conocimientos y herramientas especiales para borrar todo rastro de su partición delictiva; asimismo que las autoridades no están suficientemente capacitadas para investigar estas conductas ilícitas y punir a los autores del delito.

La gravedad del asunto radica en los distintos sectores que pueden ser afectados por estos ataques, pues no sólo se basa en las innovaciones de los sistemas informáticos y de contenidos digitales, sino a la confrontación de los cambios morales para la convivencia social.

Hoy en día, nos enteramos en las noticias y en los diversos medios, sobre estos ciberataques, los cuales se han vuelto comunes en nuestro entorno, desde casos a gran escala, como a los particulares, en los que pueden dañar la vida de una persona, afectando su situación emocional y psicológica. También, dichas conductas

---

antisociales han evolucionado al ciberespacio, ya que con el avance tecnológico y el fácil acceso que tienen todas las personas de los mismos propicia un aumento de este tipo de casos en el mundo.

Es el caso, de los niños y adolescentes que cuentan con redes sociales y medios electrónicos, y que dedican mucho tiempo a estas tecnologías sin la supervisión de sus padres o un adulto, por ende, su ve completamente expuesta su vida, ya que al ser sujetos indefensos e inocentes son susceptibles a que los sujetos activos tiendan a manipularlos y engañarlos para extraerles información de diversa índole, fotos, videos, así como actos sexuales afectando su desarrollo personal y social. Mientras que, los adultos normalmente sufren de acoso, extorsión, estafas y fraudes cuando realizan compras en línea e ingresan sus tarjetas de crédito y con ello les roban sus datos para hacer dichos actos perjudicandolos principalmente en su patrimonio.

Por otro lado, el sector empresarial periódicamente se ve afectado en la seguridad de sus sistemas informáticos y/o tecnológicos debido a las diversas técnicas informáticas que se utilizan para la comisión de los delitos como los robos de identidad o pérdidas financieras

Como ya se ha planteado, son diversas las afectaciones que causan los ciberdelitos, y para ejemplificar el impacto que este puede llegar a causarle a una persona, una institución, una empresa, un estado o un país.

Por consiguiente, se hará mención de algunos acontecimientos que han sido objeto de delitos cibernéticos en los últimos años:

Uno de los virus informáticos más poderosos del mundo fue denominado Stuxnet, el cual estaba orientado a reprogramar los sistemas de control industrial utilizados en tuberías de gas y diversas plantas de energía aprovechando las vulnerabilidades del sistema, con el fin de crear una ciberguerra en todo el mundo; consiguiendo sacar de operación a 1,000 centrifugadoras que Irán tenía destinadas a la purificación de Uranio. Por lo que en Junio del 2012 el presidente Barack Obama ordenó ataques informáticos contra las instalaciones iraníes por medio de este virus con el objetivo de frenar el programa nuclear de Irán.[25]

En 2020, la Guardia Civil Española en una operación llamada Boxman desarticuló a una banda de 13 hackers liderada por dos menores de edad en Granada los cuales habían ejecutado 47 estafas con datos bancarios robados, después de que compraron más de 777.750 contraseñas en la Internet profunda (*Deep web*) ya que realizaron compras con tarjetas de crédito ajenas desde diferentes provincias, aunque las víctimas residían en Alemania, Estados Unidos y España.[26]

A modo de conclusión, si tomamos en sentido opuesto los avances y el uso de las TICs en las naciones, estos han aperturado una infinidad de actos y situaciones delictivas nunca vistas ni imaginadas con anterioridad, lo que representa un riesgo inminente para esta generación en la que vivimos.

1.3.1 LOS DELITOS CIBERNÉTICOS EN LA PANDEMIA COVID-19

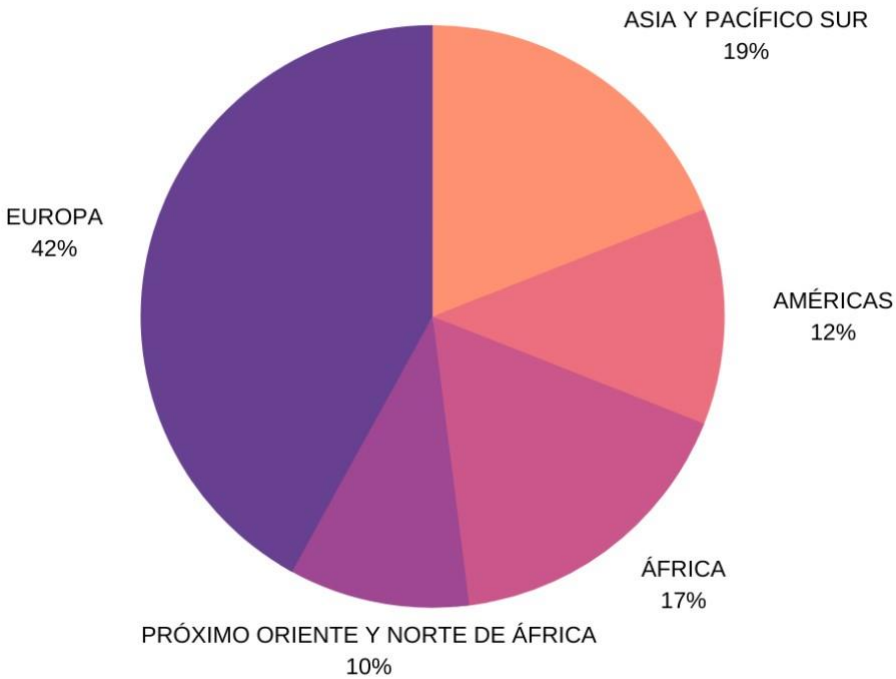
La pandemia que estamos viviendo actualmente causada por el virus COVID-19 ha tenido una repercusión importante, y un aumento mundial de ciberamenazas; en todas las partes del mundo, las autoridades están sometidas a una presión considerable

[25] LOREDO GONZALEZ, Jesús Alberto, *op. cit.* p. 48
[26] *Vid.* "Desarticulada en Granada una red de cibercriminal liderada p2or dos menores tras 47 estafas" en Periódico El País, 2020, información visible en: https://elpais.com/espana/2020-0819/desarticulada-en-granada-un-red-de-cibercrimen-liderada-por-dos-menores-tras-47-estafas.html [Fecha de consulta: 20 de octubre de 2020]

debido al aumento de la crisis sanitaria en el mundo y a la actividad delictiva que ha tenido como consecuencia del coronavirus.

> "Según la información facilitada por uno de los socios de INTERPOL del sector privado, entre enero y el 24 de abril de 2020 se detectaron 907 000 correos basura, 737 incidentes de tipo malware, y 48.000 URL maliciosas, todos ellos relacionados con la COVID-191. Los ciberdelincuentes están cambiando de objetivo, para maximizar el alcance del daño y los ingresos económicos, y, en vez de lanzar sus ataques contra particulares y pequeñas empresas, empiezan a centrarse en las grandes empresas, gobiernos, e infraestructuras esenciales, que juegan un papel fundamental en la respuesta al brote." [27]

A continuación, se muestran los países que más han sido vulnerados por la ciberdelincuencia durante la pandemia del COVID-19.



Encuesta mundial de INTERPOL sobre ciberdelincuencia

31

[27] INTERPOL, Secretaría General de INTERPOL 200, quai Charles de Gaulle 69006 Lyon Francia "Ciberdelincuencia: efectos de la covid-19", 2020 p.9, información visible en: https://www.interpol.int/es/Noticias-y-acontecimientos/Noticias/2020/Un-informe-de-INTERPOLmuestra-un-aumento-alarmante-de-los-ciberataques-durante-la-epidemia-de-COVID-19 [Fecha de consulta: 27 de octubre de 2020]

El continente europeo ha sido el que más ha sufrido ataques de la ciberdelincuencia con un 42%, por el contrario, el Próximo Oriente y el Norte de África obtuvieron 10%. Siendo de los continentes que menos ha presentado ataques de la ciberdelincuencia durante la pandemia al igual que el continente africano. Es notoria la gran diferencia que existe entre Europa y las demás regiones, ya que este al ser un continente donde la mayoría de los países que lo conforman son desarrollados, cuentan con una tecnología avanzada y con hackers de primer nivel; así mismo, durante la pandemia han llevado una absoluta ventaja en la distribución de fármacos y artículos sanitarios, lo que les genera mayores posibilidades de ataque por los demás países dominantes en ese rubro.

Los principales ciberdelitos que se han desarrollado durante la pandemia son:

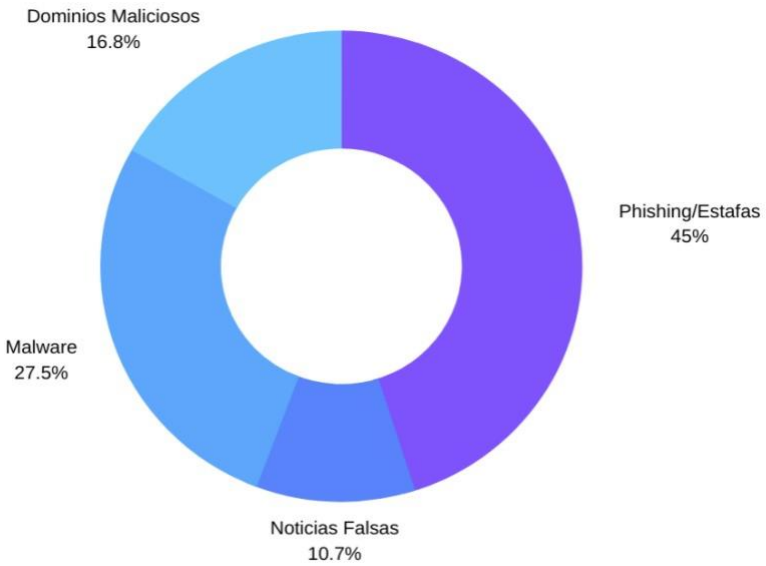
[31] Encuesta mundial de la interpol de ciberdelincuencia 2020, "Ciberdelincuencia: efectos del covid-19" p.4,información visible en: https://www.interpol.int/es/Noticias-y-acontecimientos/Noticias/2020/Uninforme-de-INTERPOL-muestra-un-aumento-alarmante-de-los-ciberataques-durante-la-epidemia-deCOVID-19 [Fecha de consulta: 27 de octubre de 2020]

- ❏ Las estafas por internet y el phising: Los autores de este delito aprovechan la pandemia para mandar a sus víctimas correos electrónicos relacionados con el COVID-19 haciéndose pasar por autoridades sanitarias gubernamentales, y así al momento en que abren el correo, los delincuentes aprovechan para mandar contenidos maliciosos y robar datos personales.

- ❏ Los malware: Los delincuentes con el fin de recolectar datos personales, datos bancarios o instalar programas espías; utilizan como señuelo datos del COVID19 y de esa manera infiltrarse y poder sustraer datos.

- ❏ Dominios Malignos: Se tratan de sitios web malignos, que se crean con el afán de actividades fraudulentas como por ejemplo la propagación de malware o phishing; estos sitios web contienen en sus nombres de dominio, palabras relacionados con la pandemia del COVID-19 y con una posible cura.

❑ Desinformación: Debido a la gran cantidad de desinformación y noticias falsas que se divulgan dentro de la sociedad, y la necesidad de que exista una posible cura para el COVID-19, se han facilitado la realización de ciberataques y así convertir a la sociedad en un blanco fácil para los ciberdelincuentes.[28]



Proporción de las principales ciberamenazas relacionadas con la COVID-19 calculada a partir de la información dada por los países miembros de la INTERPOL

33

[28] *Cfr.* INTERPOL, Secretaría General de INTERPOL 200, quai Charles de Gaulle 69006 Lyon Francia "CIBERDELINCUENCIA: EFECTOS DE LA COVID-19", 2020 p.5, información visible en: https://www.interpol.int/es/Noticias-y-acontecimientos/Noticias/2020/Un-informe-de-INTERPOLmuestra-un-aumento-alarmante-de-los-ciberataques-durante-la-epidemia-de-COVID-19 [Fecha de consulta: 27 de octubre de 2020]

De acuerdo con la información recabada por la INTERPOL, el ciberdelito que más amenaza presenta es el phishing y la estafa, el segundo con más amenazas es el malware y los que menos tienen amenazas son los dominios maliciosos y las noticias falsas. Es por ello que el phishing es el delito cibernético que más se ha propagado en estos últimos años y sobre todo en la pandemia ya que debido al confinamiento, las personas se han dedicado a hacer todo tipo de movimientos, compras, transacciones a través de sitios web.

De acuerdo con el diario El Economista, se reportó el 18 de septiembre del presente año, el caso de un grupo de hackers chinos que robó información de laboratorios españoles donde se dedicaban a la investigación de la vacuna para el COVID 19. La directora del CNI dijo que se han aumentado los asaltos a los sistemas informáticos en varios países que compiten por la obtención de un remedio frente a la pandemia.[34]

[33] INTERPOL, Proporción de las principales ciberamenazas relacionadas con la COVID-19 calculada a partir de la información dada por los países miembros 2020, p.8, información visible en: https://www.interpol.int/es/Noticias-y-acontecimientos/Noticias/2020/Un-informe-de-INTERPOLmuestra-un-aumento-alarmante-de-los-ciberataques-durante-la-epidemia-de-COVID-19 [Fecha de consulta: 27 de octubre de 2020]

[34] Vid., "Hackers chinos robaron información en España sobre vacuna contra Covid-19. 2020". El Economista, 2020, información visible en:https://www.eleconomista.com.mx/internacionales/Hackerschinos-robaron-informacion-en-Espana-sobre-vacuna-contra-Covid-19-20200918-0041.html [Fecha de consulta: 20 de octubre de 2020] REVISTA Y PUBLICACION PERIODICA

CAPÍTULO II

PRECEDENTES EN MATERIA DE DELITOS CIBERNÉTICOS

2.1 REVISIÓN DE LAS LEYES QUE EXISTEN PARA COMBATIR LOS DELITOS CIBERNÉTICOS EN EL MUNDO

A nivel internacional existen diversos ordenamientos jurídicos, convenios, leyes o tratados que contemplan los delitos informáticos o cibernéticos y los regulan de diversas maneras, dando ciertas pautas y referencias para que otros países miembros de las naciones unidas se hagan cargo de regular dichos delitos en sus propias leyes y jurisdicciones.

A continuación se muestra una tabla que contiene las diferentes leyes en materia de delitos informáticos en diversos países:

Tabla comparativa de delitos informáticos a nivel internacional[35]

Países	Leyes o Tratados
Alemania	Ley contra la criminalidad económica del 15 de mayo de 1986 y, la ley de protección de datos del 27 de enero de 1977.
Francia	Ley sobre Fraude Informático No. 88-19 creada el 5 de enero de 1988, también conocida como “Loi Godfrain”.
Estados Unidos de Norteamérica	Acta Federal de Abuso Computacional de 1994

[35] Tabla es de elaboración propia con información tomada de las siguientes fuentes: https://biblioteca.cejamericas.org/bitstream/handle/2015/1723/cl-bcn-delitosinformaticos.pdf?sequence=1&isAllowed=y; https://www.poderjudicialmichoacan.gob.mx/tribunalm/biblioteca/almadelia/Cap4.htm; https://obtienearchivo.bcn.cl/obtienearchivo?id=repositorio/10221/20864/5/FINAL%20_%20Informe%20_%20Cibercrimen%20en%20EEUU_v5.pdf [Fecha de consulta: 09 de noviembre de 2020]

	Ley de Privacidad de California Ley de Fraude y Abuso Informático Ley de Usurpación de Identidad Ley USA PATRIOT 9 Ley PROTECT de 2003 Ley de Protección de los Niños de Internet Ley NET de 1998 Ley de Copyright del Milenio Digital Ley de Decencia en las Comunicaciones

Italia	Código Penal de Italia
Austria	Ley de Reforma del Código Penal del 22 de diciembre de 1987.
Chile	Ley 19.223 “Relativa de Delitos Informáticos” de 1993 Ley 20.009 (2005) Ley 18.168 (2002)
España	Código Penal de 1995

En el caso de Alemania, la Ley contra la Criminalidad Económica de 1986 contempla las siguientes figuras delictivas: espionaje de datos, estafa informática, falsificación de datos probatorios, alteración de datos, sabotaje informático y utilización abusiva de cheques o tarjetas de crédito. Así mismo, este país cuenta con la ley de protección de datos personales la cual contempla el abuso de almacenamiento, comunicación, modificación y cancelación de los datos personales.[29]

En Austria, la Ley de Reforma del Código Penal de 1987 establece los delitos de: destrucción de datos, el cual sólo contempla la destrucción de datos personales, no personales y programas; y la estafa informática.[30]

El Código Penal de Italia tipifica los siguientes delitos: acceso abusivo de sistemas informáticos y telemáticos, abuso de la calidad de operador de sistemas, introducción de virus informáticos, fraude informático, intercepción abusiva de telecomunicaciones, falsificación informática, espionaje informático, violencia sobre bienes informáticos,

[29] Información visible en: https://www.poderjudicialmichoacan.gob.mx/tribunalm/biblioteca/almadelia/Cap4.htm#4_3 [Fecha de consulta: 09 de noviembre de 2020]
[30] *Ibidem.*

abuso de la detentación o difusión de códigos de acceso y violación de correspondencia electrónica.[31]

Chile, en su Ley de Delitos Informáticos de 1993 dispone de cuatro artículos que sancionan al que actúe maliciosamente destruyendo, utilizando, apoderándose, interfiriendo, difundiendo y revelando datos contenidos en un sistema de información.[39]

En Estados Unidos, sus diferentes leyes contemplan numerosas figuras penales: fraude y acceso ilegal, usurpación de identidad y fraude, fraude y dispositivos de acceso, terrorismo, obscenidades, pornografía infantil, prohibición de dominios engañosos, prohibición de uso de recursos públicos para adquisición de ordenadores sin filtros, seducción de menores para propósitos sexuales, protección de copyright, difamación y, amenazas y acoso cibernético.[32]

En Francia, con la Ley de Modificación del Código Penal, número 88-19, del 5 de enero de 1988, relativa al fraude informático, se centra basicamente en los atentados contra los sistemas de tratamiento automatizado de datos e información nominativa que incluye el acceso fraudulento, sabotaje informatico, destruccion de datos y la falsificación de documentos.[33]

El Código Penal de España de 1995 distingue cinco grupos de delitos informáticos los cuales son: 1) sabotaje informático, 2) acceso ilícito a sistemas informáticos que incluye el espionaje electrónico, apoderamiento de datos, ficheros y programas y acceso ilegítimo para obtener un beneficio patrimonial, 3) protección de programas de ordenador que recaen en la propiedad intelectual, 4) utilización ilegítima de sistemas

---

[31] *Ibidem.* [39]

Ibidem.

[32] MEZA LOPEHANDIA, Matias, “Los delitos cibernéticos en la legislación estadounidense”, Biblioteca del Congreso Nacional de Chile, 2014, Chile, pp. 3-5, visible en: https://obtienearchivo.bcn.cl/obtienearchivo?id=repositorio/10221/20864/5/FINAL%20_%20Informe%20_%20Cibercrimen%20en%20EEUU_v5.pdf [Fecha de consulta: 09 de noviembre de 2020]

[33] CANALES, Patricia y LOISEAU, Virgine, “Delitos informáticos en la legislación de España, Francia, Alemania e Italia”, Santiago de Chile, Biblioteca del Congreso Nacional de Chile, 2004, pp. 31-35, visible en: https://biblioteca.cejamericas.org/bitstream/handle/2015/1723/cl-bcn-delitosinformaticos.pdf?sequence=1&isAllowed=y [Fecha de consulta: 09 de noviembre de 2020]

o elementos informáticos exclusivos de las terminales de comunicación y 5) vulneración de la intimidad.[34]

Actualmente, existen dos organismos internacionales que se dedican a vigilar, regular y controlar los delitos informáticos en el mundo: El Convenio de Budapest y las Naciones Unidas a través de la Comisión de Prevención del Delito y Justicia Penal.[35]

El Convenio de Budapest que entró en vigor en 2004, es el primer tratado internacional que busca combatir los delitos informáticos cometidos a través de Internet, mediante la armonización de leyes entre naciones, con el fin de aplicar una política penal común que mejore las técnicas de investigación y el enjuiciamiento de esos delitos, fomentando la cooperación internacional. [36]

Dicho tratado establece las infracciones de derechos de autor, fraude informático, la pornografía infantil, los delitos de odio y violaciones de seguridad de red. También contiene una serie de competencias y procedimientos, tales como la búsqueda de las redes informáticas y la interceptación legal.[37]

La Comisión de Prevención del Delito y Justicia Penal creada en 1992, es el órgano principal del sistema de las Naciones Unidas que se encarga de formular políticas innovadoras sobre las problemáticas actuales y recomendaciones sobre justicia penal, enfocadas en la trata de personas, crímenes transnacionales y el terrorismo.[38]

Para llevar a cabo lo anterior, realiza un foro cada cinco años con el propósito de intercambiar conocimientos y estrategias tanto nacionales como internacionales, junto con organismos auxiliares de la ONU en materia de seguridad, delincuencia organizada transnacional y corrupción.[39]

[34] *Idem*, p. 9

[35] ARGUELLES ARELLANO, María del Consuelo, “Retos de la legislación informática en México”, vol.20, n.4, Computación y sistemas, 2016, p.830, visible en: http://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S1405-55462016000400827 [Fecha de consulta: 10 de noviembre de 2020] FUENTE ELECTRONICA

[36] *Cfr.Ibidem*

[37] *Cfr.Ibidem*

[38] *Cfr, Ibidem*

[39] *Cfr. Ibidem*

2.2 ANÁLISIS DE LA LEGISLACIÓN EN MATERIA FEDERAL DE DELITOS CIBERNÉTICOS EN MÉXICO

En nuestra legislación mexicana existen grandes lagunas jurídicas respecto de los delitos cibernéticos, como ya se ha mencionado, no hay una delimitación expresa y unificada sobre las conductas particulares que han surgido a la par de la tecnología, y se ha omitido reformar los distintos códigos penales que existen para abarcar las distintas modalidades de delitos cibernéticos.

> El 17 de mayo de 1999 se publicó en el *Diario Oficial de la Federación* una reforma integral en materia penal a nivel federal relacionada con delitos informáticos, la cual incluía dentro de su marco jurídico distintas figuras delictivas que protegen la información contenida en los sistemas y equipos de cómputo, sin embargo, este ordenamiento ha quedado superado debido al crecimiento del uso de las tecnologías de información por casi todo tipo de individuo, perteneciente a cualquier clase social.[40]

Actualmente, pocas entidades federativas, dentro de sus códigos penales prevén y sancionan los delitos cibernéticos:

En el Código Penal para el Estado de México, en su artículo 174 establece la falsificación y utilización indebida de títulos al portador como los documentos de crédito público y documentos relativos al crédito, se prevé una sanción de cuatro a diez años de prisión y de ciento cincuenta a quinientos días de salario mínimo a quien incurra en estos delitos.[41]

En Jalisco, se tipifica en su artículo art. 170 bis del Código Penal para el Estado Libre y Soberano de Jalisco, el delito de falsificación de boletos, contraseñas, fichas, tarjetas u otros documentos que no estén destinados a circular y sirvan

---

exclusivamente para identificar a quien tiene derecho a exigir la prestación que en ellos se consigna y se le impondrán de tres a nueve años de prisión y multa por lo

---

[40] JIMÉNEZ ROJAS, Jesús Ramón, "Delitos informáticos en México", *Seguridad*, México, UNAM, 2018, núm. 26, información visible en: https://revista.seguridad.unam.mx/numero26/delitos-informticos-en-m-xico [Fecha de consulta: 09 de noviembre de 2020]

[41] *Cfr.* PIÑA LIBIEN, Hiram Raúl, "Delitos informáticos previstos y sancionados en el ordenamiento jurídico mexicano", p. 9, información visible en: http://www.ordenjuridico.gob.mx/Congreso/2doCongresoNac/pdf/PinaLibien.pdf [Fecha de consulta: 09 de noviembre de 2020]

equivalente de doscientos a cuatrocientos días de salario mínimo a quien incurra en este delito. Si el sujeto activo es empleado o dependiente del ofendido, las penas aumentarán en una mitad.[42]

El Código Penal para el Estado de Nuevo León en su artículo 242 Bis, se establece la sanción de tres a nueve años de prisión y multa de ciento cincuenta a cuatrocientas cincuenta cuotas al que produzca, reproduzca, introduzca al estado, enajene, aun gratuitamente, o altere, tarjetas de crédito o de débito, o la información contenida en estas, esqueletos de cheque o documentos utilizados para el pago de bienes y servicios o para disposición de efectivo.[43]

En el estado de Quintana Roo, en su Código Penal para el Estado Libre y Soberano de Quintana Roo en los artículos 189 y 189 Bis se tipifica la falsificación de documentos y uso de documentos falsos y prisión de seis meses a tres años y una multa de quince a noventa días a quien para obtener un beneficio o para causar un daño, falsifique o altere un documento público o privado; las penas aumentarán en el caso que el sujeto activo sea empleado o dependiente del ofendido.[44]

Dentro del Código Penal para el Estado de Sinaloa en el artículo 217, se tipifica un artículo con relación al delito informático y dentro de sus fracciones plantea las hipótesis respecto de quien Intercepte, altere, dañe o destruya una base de datos, sistema de computadoras o red, con el fin de defraudar, obtener dinero, bienes o información y un programa de computadora o los datos contenidos en la misma, en la base, sistema o red. Se prevé la sanción de seis meses a dos años de prisión y una multa de noventa a trescientos días de salario mínimo.[45]

En Veracruz, los delitos informáticos se encuentran en su Código Penal en el capítulo III que tiene por nombre delitos informáticos, el cual contempla sólo el artículo 181 que dice que quien cometa dicho delito respecto de bases de datos y sistemas de

[42] *Cfr. Idem*, p.10
[43] *Cfr. Idem*, p. 11
[44] *Cfr. Idem*, p.12
[45] *Cfr.* Idem, p. 13

computadoras, programas informáticos será sancionado de seis meses a dos años de prisión y multa hasta de trescientos días de salario.

El Estado de Puebla contempla un capítulo denominado delitos informáticos, sobre el cual se va profundizar en el siguiente capítulo de este estudio.

En el Código Penal Federal, los delitos cibernéticos vienen tipificados en los siguientes artículos:

En el artículo 202, se tipifica el delito de pornografía de personas menores de edad y de incapaces, a quien procure, obligue o induzca, a una o varias de estas personas a realizar actos de índole sexual o de exhibicionismo corporal, con el objeto de grabarlos, fotografiarlos o exhibirlos a través de anuncios impresos o de transmisión por medio de internet; se prevé la sanción de siete a doce años de prisión y una multa de ochocientos a dos mil días de salario mínimo a quien incurra en este delito.[46]

Del artículo 211 Bis al 211 Bis 7, se encuentran regulados el delito de revelación de secretos y el acceso ilícito a sistemas y equipos de informática (hacking informático) protegidos por algún mecanismo de seguridad, siendo estos de particulares, del Estado o de instituciones del sistema financiero con su respectiva sanción y multa.[47]

El artículo 424 Bis tipifica los delitos en materia de Derechos de Autor, el cual establece que a quien fabrique con fin de lucro un dispositivo o sistema cuya finalidad sea desactivar los dispositivos electrónicos de protección de un programa de computación; estos son sancionados con una multa de dos mil a veinte mil días de salario mínimo y de tres a diez años de prisión. Aunado a esto, la Ley Federal del Derecho de Autor regula todo lo relativo a la protección de programas de computación, bases de datos y los derechos autorales relacionados a estos, por lo que el uso ilícito de los mismos conlleva a sanciones establecidas en dicha ley.[48]

Derivado de lo anterior, se infiere que ciertos Estados de México, contemplan en sus Códigos Penales algún capítulo relativo a los delitos informáticos pero no radica esencialmente en el tema, pues estos derivan al ser clasificados con otro nombre que impide el esclarecimiento de los mismos. Así mismo, en ellos sólo establecen de uno

[46] *Cfr. Idem p. 14*
[47] *Ibidem*
[48] *Ibidem*

a tres artículos que mencionan o se centran básicamente en el acceso ilícito a bases de datos, sistemas de computadoras y programas, ya sean del Estado, de un particular o de sistemas financieros. Por otra parte, hay una gran cantidad de Estados que todavía no regulan este tipo de conductas de manera precisa, tales como: Baja California, Aguascalientes, Campeche, Coahuila, Oaxaca, Guerrero, Guanajuato, Michoacán, Colima, Hidalgo, entre otros; pues estos los mencionan de forma ambigua y dentro de otra conducta penal.

2.3 COMPARACIÓN DE LAS DIFERENTES LEYES QUE EXISTEN EN MATERIA DE DELITOS CIBERNÉTICOS A NIVEL INTERNACIONAL CON LA LEGISLACIÓN MEXICANA

Alemania, el país donde se ha ponderado con especial cuidado la conveniencia político-criminal de penalizar determinadas conductas relativas a la informática, queriendo colmar una laguna legal inaplazable, no sólo consistieron en la modificación de algún precepto ya existente, sino que se introdujeron una serie de nuevos tipos penales relativos a la delincuencia informática: el espionaje de datos, estafa mediante ordenador o fraude informático, falsificación de datos probatorios. [49]

Caso contrario al de México, en el cual los legisladores han omitido la adaptación de los códigos penales para introducir nuevas figuras delictivas, ya que sólo mencionan a los medios electrónicos de forma secundaria dentro de los tipos penales comunes

y ya existentes.

En España optaron por seguir con los esquemas dogmáticos penales tradicionales incorporando las nuevas figuras delictivas relacionadas con lo informático y vinculado a las nuevas TICs, mediante una técnica legislativa de equivalencia. Por lo que, en su código penal han modificado o ampliado algunos elementos o requisitos de los delitos ya existentes. [58]

[49] CANALES, Patricia y LOISEAU, Virgine, *op.cit*. p. 45 [58]
Cfr. Idem, p. 44

Ahora bien, México ha seguido la misma pauta de España toda vez que, en la mayoría de los códigos penales de los Estados han preferido continuar reformando artículos

ya existentes respecto de figuras delictivas en las que mencionan que pueden cometerse por algún medio tecnológico o informático.

En Italia, el legislador estableció las disposiciones sobre delito informático en el Código Penal, usando la técnica legislativa de la extensión, esto es, elaboró una figura especial, paralela e inspirada en otras existentes, pero con relación a bienes nuevos como los sistemas informáticos, los datos y el software.[50]

El legislador francés utilizó la técnica legislativa especial, esto es, la conducta la criminalizó por medio de una disposición penal, o juego de disposiciones de la misma clase, castigando las especialidades de un particular uso indebido, o abuso informático. Así, ha introducido los llamados delitos informáticos, mediante la tipificación, artículo por artículo, de determinadas acciones que han sido objeto de sanción penal. Sin embargo han dejado sin una regulación específica a delitos como el fraude electrónico. [60]

En lo que concierne a México, en distintos Estados de la República, han optado por seguir la técnica que utiliza Francia, tal es el caso de Tabasco, el cual contempla en su código penal el título decimotercero bis llamado Delitos Contra La Seguridad En Los Medios Informáticos y Magnéticos, tipificando de manera especial y específica las figuras jurídicas de: 1) Acceso sin autorización, 2) Daño informático, y 3) Falsificación informática.

Por lo que respecta a Chile, en su Ley 19.223 “Relativa a Delitos Informáticos” sólo contempla cuatro artículos en los que regula los sistemas de tratamiento de información; La Ley 20.009 regula la responsabilidad para el caso de robo, hurto o extravío de tarjetas de crédito y La Ley 18.168 regula de manera general las telecomunicaciones, a pesar de ello, sigue siendo un país que no regula todas las demás figuras jurídicas de delitos informáticos. Contrastandolo con México, se

[50] *Cfr. Ibidem* [60]
Cfr. Ibidem

encuentra en el mismo plano, toda vez que regula en sus diferentes códigos penales esas figuras y no las idóneas para dichos delitos.[51]

Con respecto a una investigación en la que se analizaron los delitos cibernéticos en países de Latinoamérica, que cuentan con una legislación completa al establecer siete figuras jurídicas como son: la interceptación ilícita, atentado contra la integridad de los datos, atentado contra la integridad del sistema, abuso de los dispositivos, falsedad informática, fraude o estafa informática y pornografia infantil; los resultados del ranking de países con más sanción penal son Puerto Rico, República Dominicana y Venezuela, obteniendo un 100% y contemplando las siete figuras delictivas; por lo que México quedó situado en el 9º lugar obteniendo un 75% en su protección penal.[52]

Haciendo incapie en Venezuela, se considera como el único país en America Latina que posee una ley especial sobre Delitos Informáticos, la cual contiene 33 artículos y están clasificados en 5 capítulos a saber: Contra sistemas que utilizan TICs; Contra la propiedad; Contra la privacidad de las personas y las comunicaciones; Contra niños y adolescentes; Contra el orden económico.[53]

Las Naciones Unidas logró un gran avance en materia de delitos cibernéticos, ya que en su 11º Congreso sobre "Prevención del delito y justicia penal", discutió las recomendaciones que deberían tomar los países miembros para tomar las medidas correspondientes que logren combatir los delitos informáticos, las cuales son las siguientes:[54]

1. La creación de una cultura de seguridad en la navegación de Internet, la aplicación de estrategias para la detección y combate hacia los delitos cibernéticos y buscar soluciones a las necesidades de cada país.

[51] TEMPERINI MARCELO, Gabriel Ignacio, "Delitos informáticos en Latinoamérica: Un estudio de derecho comparado. 1ra. Parte", información visible en: http://conaiisi.unsl.edu.ar/2013/82-553-1-DR.pdf [Fecha de consulta: 10 de noviembre de 2020]

[52] Vid. anexo 2

[53] *Cfr.* TEMPERINI MARCELO, Gabriel Ignacio *op. cit.*

[54] TORRES RUIZ, Pedro,"Aspectos generales de los delitos informáticos y el combate a los mismos", p.8, información visible en: http://ordenjuridico.gob.mx/Congreso/2doCongresoNac/pdf/TorresRuiz.pdf [Fecha de consulta: 19 de octubre de 2020]

2. La necesidad de que el Sistema de Naciones Unidas juegue un papel preponderante mediante convenios o tratados internacionales, para asegurar el correcto funcionamiento y protección del Internet.

3. La renovación de las leyes internas de todos los países participantes, para combatir a los delitos informáticos.

4. Capacitar a los profesionales de la justicia como son los jueces, abogados, y magistrados, a través de planes de estudio que incluyan el tema del crimen cibernético.

5. Incrementar y mejorar las herramientas básicas actuales para el intercambio de información, así como las medidas en la lucha contra el crimen cibernético basándose en los criterios de la INTERPOL.

6. Todos los países miembros deberán de contar con una política de evaluación del crimen cibernético, esta se debe basar en un esquema de eficacia y eficiencia.

Como se ha vislumbrado, México carece de un seguimiento a las pautas emitidas por las Naciones Unidas, aún siendo miembro de dicho organismo internacional, por lo que es importante que se reformen nuevamente los ordenamientos tanto local como federal, pues como ya se ha visto el cuerpo normativo hasta el dia de hoy no ha sido suficiente para prevenir y reprimir esta conducta ilícita, y no abarca todas las modalidades del delito informático. Se considera que es menester la creación de figuras jurídico penales que específicamente regulen esta nueva modalidad delictiva, toda vez que, no se debe olvidar que en materia penal no es aplicable la analogía, sino que el delito debe estar perfectamente tipificado en un ordenamiento legal, según se desprende del Artículo 14 constitucional.[55]

[55] TÉLLEZ VALDÉS, Julio, “Delitos Informáticos: Situación en México”, Informática y derecho: Revista iberoamericana de derecho informático,Nº 9-11, 1996,vol. I, p.461, visible en: https://dialnet.unirioja.es/servlet/articulo?codigo=248768 [Fecha de consulta: 10 de noviembre de 2020]

CAPÍTULO III

DELITOS CIBERNÉTICOS EN EL ESTADO DE PUEBLA

3.1 ANÁLISIS DEL CÓDIGO PENAL DEL ESTADO DE PUEBLA EN MATERIA DE DELITOS CIBERNÉTICOS

En el Estado de Puebla, los delitos cibernéticos se encuentran contemplados en su Código Penal en el capítulo vigésimo quinto denominado “Delitos Informáticos” que van del artículo 475 a 478 de dicho ordenamiento, los cuales se mencionan a continuación:

Artículo 475. Se impondrá prisión de uno a cinco años, multa de cincuenta a quinientos días de salario 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 o técnicos o por funcionario o empleado público o cuando el secreto revelado o publicado sea de carácter industrial.

Artículo 476. 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 de multa. Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, se le impondrán de tres meses a un año de prisión y de cincuenta a ciento cincuenta días multa.

Artículo 477. 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 dos años de prisión y de doscientos a seiscientos días multa.

Artículo 478. Al que estando autorizado para acceder a sistemas y equipos de informática del Estado, indebidamente modifique, destruya o provoque pérdida de información que contengan, se le impondrán de dos a cuatro años de prisión y de trescientos a novecientos días multa. Al que estando autorizado para acceder a sistemas y equipos de informática del Estado, indebidamente copie información que contengan, se le impondrán de uno a dos años de prisión y de ciento cincuenta a cuatrocientos cincuenta días multa.

A quien estando autorizado para acceder a sistemas, equipos o medios de almacenamiento informáticos en materia de seguridad pública, indebidamente obtenga, copie o utilice información que contengan, se le impondrá pena de dos a cinco años de prisión y multa de quinientos a mil días de salario mínimo general vigente. Si el responsable es o hubiera sido servidor público en una institución de seguridad pública, se impondrá además, hasta una mitad más de la pena impuesta, destitución e inhabilitación por un plazo igual al de la pena resultante para desempeñarse en otro empleo, puesto, cargo o comisión pública.

Como podemos ver, los delitos cibernéticos en el Código Penal para el Estado Libre y Soberano de Puebla se regulan solamente en cuatro artículos los cuales hacen referencia a sistemas informáticos respecto del Estado o de un mecanismo de seguridad y cuando se den revelación de un secreto por parte de un prestador de servicios profesionales o servidor público, en donde se les asigna la sanción o multa que tendrán los sujetos que realicen dichas conductas.

Por otra parte, se infiere que se regulan de manera indirecta los delitos informáticos de:

- Extorsión en el art. 292 Bis, Comete el delito de extorsión el que con ánimo de conseguir un lucro o provecho, amenazare a otro *por cualquier medio* con la finalidad de causar daños morales, físicos o patrimoniales, que afecten al amenazado o a persona física o jurídica con quien éste tuviere relaciones de cualquier orden que lo determinen a protegerlos.

- Amenazas en el art. 290 Frac I “Al que *por cualquier medio* amenace a otro con causarle un mal en su persona, honor, bienes o derechos o en la persona, honor, bienes o derechos de su cónyuge, …”
- Fraude art. 402, Frac. XIX “XIX.- Al que dolosamente y con el propósito de procurarse un lucro ilícito, para sí o para un tercero, dañe o perjudique el patrimonio de otro, *mediante el uso indebido de mecanismos cibernéticos*, que provoque o mantenga un error, sea manipulando datos de entrada a un equipo de informática con el fin de producir o lograr movimientos falsos en transacciones de una persona física o moral, sea presentando como ciertos hechos que no lo son, o deformando o disimulando hechos verdaderos; y,
- Pornografía Infantil art 222.- La posesión de una o más fotografías, filmes, videos o *cualquier otro medio impreso o electrónico*, que contenga imágenes de las que se refiere el artículo 220, se sancionará con prisión de uno a cinco años y multa de cien a quinientos días de salario, siempre y cuando se demuestre que el poseedor tenía conocimiento de que las imágenes son de las personas a que se refiere el artículo 220 del presente Código; y los artículos relativos a este.

Sin embargo, estos están contemplados de manera general y no específica en lo que compete en la materia de delitos cibernéticos.

3.2 COMPARACIÓN DE LOS DELITOS CIBERNÉTICOS EN PUEBLA CON LOS ESTADOS CIRCUNDANTES A ESTE

A fin de lograr ver cómo las entidades federativas circundantes a Puebla regulan los delitos cibernéticos en sus códigos penales, sirve como parteaguas para conocer si Puebla cuenta con lo mismo o lo mínimo necesario para enfrentar las nuevas realidades delictivas que se cometen en el ciberespacio.

Hidalgo

En el Estado de Hidalgo dentro del capítulo de “Falsificación de documentos y uso de documentos falsos” en el artículo 256 Bis regula los delitos cometidos contra los equipos electrónicos y su información de cintas magnéticas de tarjetas o documentos para el pago de bienes y servicios o efectivo. Por último, en el artículo 370 de dicho ordenamiento, contempla el delito de usurpación de identidad cometida por cualquier medio.

Tlaxcala

En Tlaxcala en su Código Penal, en el título décimo cuarto en un único capítulo contempla los “Delitos contra la seguridad en los medios informáticos” el cual tiene cinco artículos que van del artículo 316 al 320 del mismo, los cuales en resumidas cuentas regulan los delitos cometidos contra los sistemas informáticos e información y datos confidenciales de entidades públicas y regímenes financieros.

Por otro lado, el artículo 399 de dicho ordenamiento regula el delito de falsificación de documentos por medios o equipos electrónicos cuando se trate de información contenida en cinta de tarjetas, títulos o documentos para el pago de bienes o servicios; el artículo 282 sanciona la usurpación de identidad cuando sea cometida por cualquier medio; y el artículo 355 nos dice de los delitos cometidos contra los menores de edad cuando se trate de que por cualquier medio se les procure, propicie promueva o induzca a realizar actos de exhibicionismo corporal, lascivos o sexuales, consumo de drogas, prácticas sexuales o otros delitos.

Guerrero

En el Estado de Guerrero en su Código Penal, se encuentran previstos los delitos de Pornografía de personas menores de edad en el artículo 173; Usurpación de identidad equiparada en el artículo 240 Ter; Divulgación de imágenes y videos íntimos sexuales en el artículo 187 y Simulación de documentos equiparado en el artículo 344.

Tales delitos mencionados, se encuentran regulados de forma que cuando sean cometidos por cualquier medio electrónico o tecnológico, Internet y demás TIC´s tengan su respectiva sanción.

Veracruz

Mientras que, el Estado de Veracruz en su Código Penal cuenta con el capítulo III denominado “Delitos Informáticos” con un artículo el cual regula los delitos informáticos en perjuicio de bases de datos, sistemas o programas informáticos cuando se altere, utilice o destruya información de los mismos.

También, contempla en su artículo 173 bis el delito de extorsión cometido vía telefónica o por cualquier medio electrónico.

Oaxaca

El Estado de Oaxaca contiene en el título vigésimo séptimo un capitulo único llamado "Delitos contra la seguridad informática y electrónica" el cual contempla las figuras de defraudación informática, intrusión informática, comercialización de programas que violen mecanismos de seguridad de equipos informáticos, destrucción de sistemas informáticos por medio de algún virus; por otra parte, al que divulgue o altere de manera ilícita información clasificada de sistemas informáticos de instituciones de seguridad pública.

Ahora bien, la legislación de este Estado introduce de forma secundaria los delitos cibernéticos dentro de otros tipos penales, haciendo mención de que estos son cometidos por cualquier o algún medio electrónico, tales como: la Pornografia infantil en su art. 195, frac. III; en el apartado de delitos contra la dignidad y el desarrollo de las personas menores de edad o de quienes no tienen la capacidad para comprender el significado del hecho; suplantación de identidad digital en el art. 232 Bis A; el secuestro exprés cometido por medios electrónicos en el art. 348 Bis y la extorsión cometida por cualquier medio electrónico en el art. 383 frac. IV.

Morelos

El Estado de Morelos regula en su capítulo VIII en el artículo 148 quarter a los delitos informáticos, atendiendo solo al que use, intercepte, altere o destruya programas de computadoras, bases de datos, o que mediante el uso de la red del internet realice actos en contra de las personas o cosas con el fin de perturbar la paz pública y atentar contra el orden constitucional.

Por otra parte dentro del mismo ordenamiento se regulan ciertas figuras que incluyen a los delitos cibernéticos en su modo de comisión a la hora de ocupar medios electrónicos, siendo estos los delitos de: violación de la intimidad personal en el art. 150 Bis; ciberacoso sexual en el art. 158 Bis; la suplantación de identidad en el art. 189 Bis; así como la suplantación de identidad de menores de edad e incapaces para comprender el significado del hecho.

Estado de México

El Estado de México no contempla un capítulo o apartado sobre los delitos informáticos, sin embargo, aplica la misma metodología de los estados anteriormente mencionados en los cuales incluye características de ciertas modalidades de los delitos cibernéticos adheridos a otros tipos penales como: la utilización de imágenes y/o voz de personas menores de edad o personas que no tienen la capacidad para comprender el significado del hecho para la pornografía, el hostigamiento y acoso sexual, delitos contra el correcto funcionamiento de las instituciones de seguridad pública y órganos jurisdiccionales, y de la seguridad de los servidores públicos y particulares, la falsificación y utilización indebida de títulos al portador, documentos de crédito público y documentos relativos al crédito.

A continuación, se muestran dos tablas que concluyen con el estudio realizado a los Códigos Penales de las entidades federativas circundantes al Estado de Puebla.

Tabla comparativa de los códigos penales que contemplan un capítulo acerca de los delitos cibernéticos[66]

	Hidalgo	**Tlaxcala**	**Guerrero**	**Oaxaca**	**Morelos**	**Edo. de México**	**Veracruz**	**Puebla**
Contempla un capítulo denominado “Delitos informáticos”				X	X		X	X

[66] Tabla es de elaboración propia con información tomada de las siguientes fuentes:

Código Penal para el Estado de Hidalgo

Código Penal para el Estado Libre y Soberano de Tlaxcala

Código Penal para el Estado de Guerrero

Código Penal para el Estado Libre y Soberano de Oaxaca

Código Penal para el Estado de Morelos

Código Penal para el Estado de México

Código Penal Para El Estado Libre y Soberano De Veracruz De Ignacio De La Llave

Código Penal Del Estado Libre y Soberano De Puebla [Fecha de consulta: 14 de Diciembre de 2020]

Tabla comparativa de los delitos cibernéticos tipificados dentro de los códigos penales [67]

	Hidalgo	**Tlaxcala**	**Guerrero**	**Oaxaca**	**Morelos**	**Edo. de México**	**Veracruz**	**Puebla**
Usurpación y/o suplantación de identidad	X	X	X	X	X			
Falsificación de documentos	X	X	X			X		
Pornografía infantil			X	X				X
Delitos contra la seguridad de sistemas informáticos		X		X	X		X	
Violación de la intimidad personal			X		X	X		
Acoso/Cibera coso sexual					X	X		
Delitos contra menores de edad que no comprenden el significado del hecho		X		X		X		

Extorsión y/o amenazas				X			X	X

[67] Tabla es de elaboración propia con información tomada de las siguientes fuentes:
Tabla es de elaboración propia con información tomada de las siguientes fuentes:
Código Penal para el Estado de Hidalgo

Código Penal para el Estado Libre y Soberano de Tlaxcala

Código Penal para el Estado de Guerrero

Código Penal para el Estado Libre y Soberano de Oaxaca

Código Penal para el Estado de Morelos

Código Penal para el Estado de México

Código Penal Para El Estado Libre y Soberano De Veracruz De Ignacio De La Llave

Código Penal Del Estado Libre y Soberano De Puebla [Fecha de consulta: 14 de Diciembre de 2020]

Secuestro exprés				X				
Fraude								X

3.3 DEFICIENCIAS DE LA LEGISLACIÓN ACTUAL EN PUEBLA

Expuesto lo anterior, se puede concretar que el capítulo referente a los Delitos Cibernéticos en la legislación de Puebla está acotado únicamente a dos modalidades, las cuales vienen siendo el sabotaje informático y la fuga de datos, haciendo hincapié en que dichas figuras atañen a sistemas o equipos de informática protegidos por algún mecanismo de seguridad, a los que forman parte del Estado, y en el caso de funcionarios públicos que infrinjan de tal manera la ley en materia de seguridad pública. Empero, esto nos deja claro como el sistema jurídico penal del Estado carece de una concisa regulación en materia de delitos cibernéticos toda vez que, excluye de legislar tales figuras delictivas de manera específica, dejando a un lado la protección jurídica que deben de tener para una eficaz impartición de justicia.

Así como se plasmó en el tema anterior, en el que se ve como en el Código Penal del Estado de Puebla se encuentran distribuidos diversos delitos que hacen alusión a los delitos cibernéticos con base en la mención de “mediante el uso o por cualquier medio”. Sin embargo, esto desde nuestro punto de vista le deja una amplia interpretación vaga tanto a los juzgadores al momento de encuadrar el delito en el

supuesto normativo, así como a los ciudadanos al momento en que se vuelven víctimas de estos delitos y buscan la necesidad de obtener justicia por los hechos cometidos en su contra.

> En la entrevista realizada a la doctora en Derecho Cynthia Solis remarca que el problema de fondo es entender cuál es la naturaleza de los delitos informáticos y, por otro, capacitar a los ministerios públicos, policía cibernética y a los jueces. Destacó que ya existe un convenio inter-policías, que se hizo en 2017. Esto implica que prácticamente todos los estados de la República ya cuentan con policía cibernética.
>
> Por otro lado, hace énfasis en que, en el derecho penal, es requisito que la ley específica describa la conducta para luego comprobar que cada punto se cumplió. "Entonces, si la conducta no está descrita como tal, a detalle y con la redacción que está prevista en el Código, no puedes hacer nada. Si te falta un elemento, no hay delito que perseguir y dejan libres a los ciberatacantes".[56]

Como sustento de lo anterior la Suprema Corte de Justicia de la Nación emitió un criterio jurisprudencial que hace referencia a la exacta aplicación de la ley en materia penal:

> **"PRINCIPIO DE LEGALIDAD PENAL EN SU VERTIENTE DE TAXATIVIDAD. ANÁLISIS DEL CONTEXTO EN EL CUAL SE DESENVUELVEN LAS NORMAS PENALES, ASÍ COMO DE SUS POSIBLES DESTINATARIOS**
>
> ***El artículo 14, de la Constitución Política de los Estados Unidos Mexicanos, consagra la garantía de exacta aplicación de la ley en materia penal al establecer que en los juicios del orden criminal queda prohibido imponer, por simple analogía y aun por mayoría de razón, pena alguna que no esté decretada por una ley exactamente aplicable al delito de que se trata. Este derecho fundamental no se limita a ordenar a la autoridad jurisdiccional que se abstenga de interpretar por simple analogía o mayoría de razón, sino que es extensivo al creador de la norma. En ese orden, al legislador le es exigible la emisión de normas claras, precisas y exactas respecto de la conducta reprochable, así como de la consecuencia jurídica por la comisión de un ilícito; esta descripción no es otra cosa que el tipo penal, el cual debe estar claramente formulado. Para determinar la tipicidad de una conducta, el intérprete debe tener en cuenta, como derivación del principio de legalidad, al de taxatividad o exigencia de un contenido concreto y unívoco en la labor***

[56] OCHOA, Maricela, "Delitos Informáticos en México, ¿Que dice la ley?",IT Masters MAG, 2020, información visible en: https://itmastersmag.com/noticias-analisis/delitos-informaticos-en-mexico-quedice-la-ley/ [Fecha de consulta: 25 de noviembre de 2020]

de tipificación de la ley. Es decir, la descripción típica no debe ser de tal manera vaga, imprecisa, abierta o amplia, al grado de permitir la arbitrariedad en su aplicación. Así, el mandato de taxatividad supone la exigencia de que el grado de determinación de la conducta típica sea tal, que lo que es objeto de prohibición pueda ser conocido por el destinatario de la norma...”[57]

A modo de conclusión del criterio jurisprudencial, se destaca la importancia de contar con normas concretas en materia penal, en las cuales el delito debe ser preciso y exacto para que no se preste a interpretaciones propias del juzgador que incurran en arbitrariedades.

Aunado a ello, existe una exorbitante carencia de resultados palpables en estadísticas y en plataformas de transparencia del Estado que permitan dar a conocer el seguimiento a los procedimientos de justicia penal para combatir dichos delitos y si realmente se logra resarcir el daño causado a las víctimas.

Por otra parte, derivado del convenio inter-policías de 2017 se creó la la Policía Estatal Cibernética, que es una Subsecretaría de Inteligencia e Investigación de la Secretaría de Seguridad Pública del Estado de Puebla, sus principales funciones son:[58]

- Patrullaje Web
- Brindar orientación por distintos canales de comunicación ya sea vía telefónica, correo electrónico y redes sociales a los ciudadanos víctimas de algún delito cibernético o conducta inapropiada.
- Coadyuvar en la Prevención del Delito mediante boletines informativos, de alerta, tutoriales, y consejos de seguridad a través de las cuentas oficiales del

[57] Tesis 1a. CXCII/2011 (9a.) Semanario Judicial de la Federación y su Gaceta, Décima Época, Octubre de 2011, Página: 1094.

[58] Información visible en: http://ssp.puebla.gob.mx/index.php/delitos-ciberneticos [Fecha de consulta: 25 de octubre de 2020]

Grupo de Atención, además de ofrecer pláticas dirigidas a estudiantes, padres de familias y autoridades municipales.

Si bien, la policía cibernética implica un avance en materia de seguridad pública del Estado, se entiende que las funciones de esta misma están enfocadas meramente a la prevención del delito, mas no en dar la debida persecución del mismo, pues indagando en la página web de dicha institución pública, esta maneja publicaciones informativas dirigidas al público en general por medio de la redes sociales *facebook y twitter* en la cual suben diversos boletines e infografías para que los usuarios de internet sean precavidos al proteger sus datos personales, mensajes, claves de acceso, al realizar operaciones financieras en línea, y prevenciones al acceder a sitios web. Dentro de su contenido informativo, hacen alusión a la denominación específica de ciertas conductas delictivas como lo son el smishing, phishing, ciberfraude y vishing; no obstante, no existe una concordancia con la legislación actual penal

---

respecto de la tipificación que contemplan sobre los delitos informáticos relacionada con las figuras delictivas cibernéticas que maneja la Policía Cibernética de Puebla en sus publicaciones preventivas.

Por otra parte, estos medios a través de los cuales se pretenden combatir los delitos, son ineficaces partiendo del hecho de que solo los usuarios de facebook y twitter que siguen a la página de dicha institución podrán visualizar ese tipo de contenidos de prevención, de forma paralela y como consecuencia del impacto que tenga la difusión de la página, será el resultado de una sociedad informada y consciente de los medios de acceso a la justicia en materia de estos nuevos delitos.

Derivado de lo anterior, según los últimos datos recabados por el INEGI en 2015, el Estado de Puebla cuenta con 6,168,883 millones de habitantes de los que 13,145 son usuarios que siguen la página de facebook de la policía cibernética y 4,890 son seguidores de la página de twitter de esta misma institución. Siendo así, que la primera de estas representa el 0.21% y la segunda representa el 0.07% del total de la población que sigue a dichas páginas, es evidente que hay una nula difusión de la existencia de la policía cibernética en redes sociales, lo cual va dejando atrás a la

mayoría de la población que no conoce de la existencia de esta misma y no puede tomar medidas precautorias para salvaguardar sus derechos. [59]

3.3.1 CASOS CONCRETOS DE DELITOS CIBERNÉTICOS EN EL ESTADO DE PUEBLA

Es importante, mencionar la realidad que se vive en el Estado de Puebla con el desarrollo de los delitos cibernéticos y como estos cada vez aumentan más. Es por ello que se darán a conocer unos casos y los delitos que se cometen con mayor frecuencia.

De acuerdo con el diario Milenio, los delitos cibernéticos en el estado de Puebla incrementaron un 28 por ciento, del mes de marzo al mes de abril, siendo los delitos de cyberbullying, ciberextorsión y ciberfraude, los que con mayor frecuencia denuncian; así lo detalla Juan Carlos Pérez Vallejo, director de la Policía Estatal Cibernética, el cual mencionó que son los fines de semana cuando se cometen el mayor número de incidentes cibernéticos, donde se ha detectado que se activan las páginas web, en especial el delito grooming (engaño pederasta), es por ello que aseguró que en coordinación con el área de Comunicación Social se realiza la publicación de boletines para informar sobre el tema, y que los padres de familia tengan mayor cuidado con sus hijos que son el sector vulnerable.[60]

[59] Párrafo de elaboración propia con información tomada de las siguientes fuentes:CiberPolicía Pue | Facebook, (1) CiberPolicía Pue (@CiberPoliciaPue) / Twitter, Número de habitantes. Puebla (inegi.org.mx), [Fecha de consulta: 25 de noviembre de 2020]

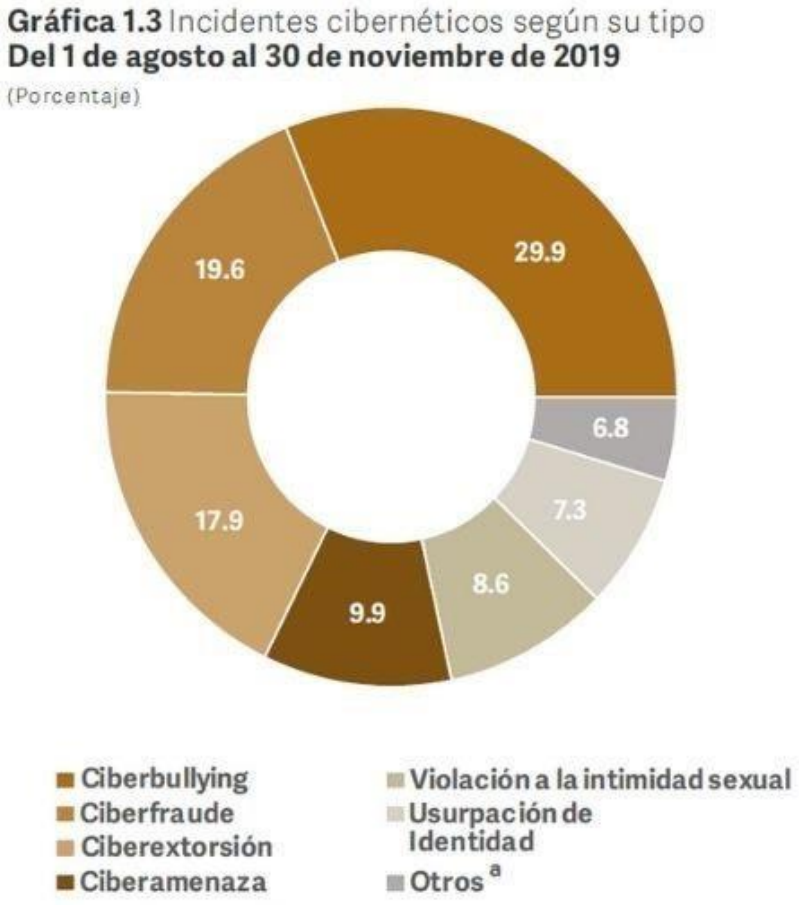
[60] GARCÍA, Elvia, “Aumentan 28% delitos cibernéticos en Puebla; al dia hay 15 reportes”, Milenio, 2020, Puebla, información visible en: https://www.milenio.com/policia/aumentan-28-los-delitosciberneticos-en-puebla

A la semana, 12 personas en el estado de Puebla son víctimas de un ciberdelito; el año pasado, la Policía Cibernética del Estado recibió 641 denuncias por estos tipos de delitos.[61]

En la siguiente gráfica se muestran los delitos cibernéticos que más se cometieron durante el mes de agosto a noviembre del 2019:[62]

[61] GÓMEZ, Paulina, "Cada semana 12 poblanos son víctimas de ciberdelitos", El sol de Puebla, 2019, Puebla, información visible en: https://www.elsoldepuebla.com.mx/policiaca/cada-semana-12-poblanos-son-victimas-de-ciberdelitospuebla-3261724.html [Fecha de consulta: 23 de noviembre de 2020]

[62] ESPEJO, Joskua, "Policía Cibernética de Puebla, sin atribución en 6 de cada 10 denuncias", Datamos, Noviembre 2020, información visible en: https://datamos.com.mx/2019/12/18/policiacibernetica-de-puebla-sin-atribucion-en-6-de-cada-10-denuncias/



De acuerdo con el artículo publicado en la revista Datamos:

> "Cuatro de cada 10 casos atendidos de agosto a noviembre por la policía cibernética del estado de Puebla fueron por ciberbullying, ciberextorsión, ciberfraude, ciberamenaza o la violación a la intimidad sexual; los seis restantes no se encuentran tipificados en el Código Penal, revela el Primer Informe de Gobierno de Miguel Barbosa Huerta, el cual detalla en el Eje 1 "Seguridad Pública, Justicia y Estado de Derecho" que cuando la queja no se trata de un delito tipificado sólo se orienta a los afectados, pese a que no puntualiza el número de casos atendidos"[63]

Otro de los delitos cibernéticos más cometidos es la violación a la intimidad sexual el cual se encuentra con un 8.6% de incidencia, sin embargo en el año 2012 en el Estado de Puebla, Olimpia Coral Melo quien en ese entonces tenía 18 años de edad, sufrió de ciberacoso debido a la difusión de un video íntimo teniendo relaciones sexuales con su novio. Olimpia, acudió con la autoridad del Estado de Puebla para que le brindaran ayuda, al llegar al Ministerio Público, le dijeron que no podía denunciar a

[63] *Ibidem*

nadie ya que no existía ningún delito que perseguir y que el único delito que podría encuadrar su situación sería el de ultrajes a la moral pública, se cita textualmente a Olimpia "Me dijeron que no podían hacer nada porque no hay en México peritos digitales y la policía cibernética es preventiva y no de acción, por lo tanto ellos no pudieron hacer nada". [64]

No conforme con la respuesta del ministerio público, Olimpia se convirtió en activista, fundando su Frente Nacional para la Sororidad, en conjunto con activistas y asociaciones civiles comenzaron su lucha por la prevención del ciberacoso; logrando que en el presente año, el Senado de la República aprobara la "Ley Olimpia" creada y propuesta desde el 2014, donde tipifica diversos delitos en relación con el acoso digital, enfocado en la difusión de contenido íntimo y sexual, con penas que van hasta los 6 años de cárcel.[65]

Gracias al avance legislativo de la Ley Olimpia, se pueden encuadrar delitos que antes no estaban tipificados en el Código Penal, y así poder sancionar a quienes realicen este tipo de actividades ilícitas como la difusión de contenido íntimo o sexual; un ejemplo es el caso de Brad Hunter, un hombre de nacionalidad australiana que se dedicaba a contactar mujeres por medio de aplicaciones de citas, para enamorarlas y persuadirlas a tener relaciones sexuales con el fin de grabarlas para publicarlo en su canal de Youtube; este hombre estuvo por diversos países haciendo esta artimaña, hasta que llegó a México; uno de los estados que visitó fue Puebla, donde lamentablemente varias mujeres fueron sus víctimas, las citaba en un departamento de la ciudad, y después de tener relaciones sexuales, las grababa y las subía a Youtube sin su consentimiento.[66]

[64] Cfr. DELGADO, Ángel, "Ley olimpia de 3 a 6 años de prisión a quien difunda packs", El universal, 2018, información visible en: https://www.eluniversal.com.mx/estados/ley-olimpia-de-3-6-anos-deprision-quien-difunda-packs [Fecha de consulta: 24 de noviembre de 2020]

[65] Cfr. FORBES, Staff, "Senado aprueba ley olimpia: 6 años de cárcel por acoso sexual digital", Forbes México, Noviembre 2020, información visible en: https://www.forbes.com.mx/politica-senado-ley-olimpia-hasta-6-anos-carcel-acoso-sexual-digital/ [Fecha de consulta: 24 de noviembre de 2020]

[66] Cfr. COLEOTE,Cinthya, "Rompen silencio víctimas poblanas de Brad Hunter" Excelsior agosto 2020, información visible en: https://www.excelsior.com.mx/nacional/rompen-el-silencio-victimaspoblanas-de-brad-hunter/1401076
[Fecha de consulta: 24 de noviembre de 2020]

Como bien se ha visto, surgió la necesidad de crear una ley específica para regular el delito de violación a la intimidad sexual por medios digitales. Toda vez que, el

Código Penal de la mayor parte de los estados no contemplaba dicha penalidad lo cual dejaba un vacío legal de estos y por ende un desamparo a la víctimas. Ahora, las víctimas de Brad Hunter con la Ley Olimpia podrán alzar la voz para exigir justicia ya que habrá un delito que perseguir.

Por el contrario, a consecuencia de la pandemia COVID-19 los delitos cibernéticos en el Estado de Puebla han incrementado un 30% a comparación del año pasado, ya que en el segundo trimestre del 2020, se registró un total de mil 164 denuncias. Los delitos que más se han presentado son el ciberfraude, la ciberextorsión y la ciberamenaza; Todo esto a raíz del confinamiento ya que las personas se ven obligadas a no salir de sus casas, lo que conlleva a que todo se realice por medio de internet y así se encuentran en un plano más vulnerable para ser víctimas de ciberdelitos.[67]

[67] Cfr. GÓMEZ, Paulina, “Dispara confinamiento a los ciberdelitos en Puebla; piden no caer en falsas ofertas”, El sol de Puebla julio 2020, información visible en:https://www.elsoldepuebla.com.mx/policiaca/dispara-confinamiento-los-ciberdelitos-en-pueblapiden-no-caer-en-falsas-ofertas-seguridad-policia-cibernetica-internet-pandemia-covid19-ciberfraudeciberextorsion-ciberamenaza-5491110.html [Fecha de consulta: 25 de noviembre de 2020]

CONCLUSIONES

Como ya se demostró a lo largo del presente estudio, se considera que la principal causa de no poder obtener una plena justicia cibernética es la insuficiencia que se tiene en la regulación de los delitos cibernéticos en México.

Derivado del estudio delimitado de los Estados circundantes al Estado de Puebla, los cuales son: Hidalgo, Tlaxcala, Guerrero, Veracruz, Oaxaca, Morelos y Estado de México se vislumbró que no todos cuentan con un apartado específico de los delitos cibernéticos en sus Códigos Penales. En ese mismo sentido, los que sí lo contemplan, establecen pocos artículos respecto del tema y se centran únicamente en modalidades como el acceso ilícito a bases de datos, sistemas de computadoras y programas, ya sean del Estado, de un particular o de sistemas financieros.

Sin embargo, en dichos Estados se destacó que algunos logran regular dentro de otros tipos penales partes alusivas a los delitos informáticos; es así que sólo el Estado de Oaxaca logra abarcar dentro de seis delitos generales a los informáticos, mientras que Tlaxcala, Guerrero, Morelos y Estado de México los contemplan dentro de cuatro tipos penales, situando a Puebla después de estos encuadrando tres delitos informáticos en los generales. Y por último, Veracruz e Hidalgo insertan dentro de dos tipos penales ciertas características correspondientes a la informática.

Es así que, los tipos penales de: usurpación y suplantación de identidad, falsificación de documentos, pornografia infantil, delitos contra la seguridad de sistemas informáticos, violación de la intimidad personal, acoso sexual, delitos contra menores de edad que no comprenden el significado del hecho, extorsión y amenzas, secuestro exprés y fraude integran dentro de su redacción la modalidad informática por medio del uso de las palabras “ por cualquier medio” o “medios informáticos”; de esta forma evitan regular de manera específica las figuras informáticas que se mencionan en el capítulo I de este trabajo. Por consiguiente, dichos Códigos no definen como tal los

delitos cibernéticos y las modalidades que se puedan suscitar, perdiendo la naturaleza de los mismos.

Sin embargo, consideramos que tales modalidades cuentan con características particulares en la comisión del delito, las cuales necesitan ser definidas y plasmadas en los ordenamientos jurídicos.

De los nueve delitos encontrados que hacen referencia a las modalidades informáticas en los diferentes códigos penales de las entidades federativas circundantes a Puebla, encontramos que el Código Penal de Puebla sólo regula tres de ellas, las cuales son: pornografía infantil, extorsión y amenzas, y fraude. Ahora bien, Puebla sí cuenta con un capítulo de delitos informáticos con cuatro artículos que se centran en el delito contra la seguridad de sistemas informáticos o mecanismos de seguridad del Estado, de un particular o de servidores públicos.

Es así que, es menester de los legisladores dar respuestas nacionales a la ciberdelincuencia en el aspecto normativo, en cuanto a la tipificación de las figuras cibernéticas en los Códigos Penales con su respectivo apartado para que exista una precisión de ello, y así las autoridades encargadas de hacer cumplir la ley y la justicia penal puedan investigar dichos delitos que cada día toman más trascendencia y consecuencias en la vida de las personas que sufren de ellos.

Por consiguiente, a la hora de que los juzgadores emitan una sentencia, puedan tener el fundamento jurídico concreto, garantizando así el debido procedimiento, encuadrando el delito en el tipo penal específico para cada modalidad, y por ende, otorgar la sanción correspondiente a cada delito. Todo ello se daría, si fuese el caso en que los delitos cibernéticos tuvieran una precisa regulación.

Por otra parte, vemos cómo la Policía Cibernética del Estado de Puebla es la autoridad encargada de combatir los delitos cibernéticos, sin embargo, se demostró en el trabajo que dicha institución, se enfoca más que nada en la prevención del delito, dejando la parte fundamental de la persecución del mismo con el fin de garantizar el acceso a la justicia en el Estado.

Por último, tomando en cuenta que otros países abordan los delitos cibernéticos en una legislación propia, México al ser un país en vías de desarrollo tiene que ir avanzando a la par del desarrollo, tanto de la sociedad y las TICs, generando

fundamentos jurídicos concretos y mecanismos de seguridad encargados de hacer frente a los nuevos ilícitos, los cuales requieren de una constante actualización en medios de pruebas digitales y técnicas de seguimiento del delito, así como de una capacitación completa hacia la Policía Cibernética de cada Estado y de los juzgadores en el conocimiento de la materia, y hacer efectivos los mecanismos judiciales de cooperación internacional de los que son parte.

REFERENCIAS:

-OBRAS GENERALES

ACURIO DEL PINO, Santiago," Delitos informáticos: generalidades", 2016, https://www.oas.org/juridico/spanish/cyb_ecu_delitos_inform.pdf

CANALES, Patricia y LOISEAU, Virgine, "Delitos informáticos en la legislación de España, Francia, Alemania e Italia", Santiago de Chile, Biblioteca del Congreso Nacional de Chile, 2004, visible en: https://biblioteca.cejamericas.org/bitstream/handle/2015/1723/cl-bcn-delitosinformaticos.pdf?sequence=1&isAllowed=y [Fecha de consulta: 09 de noviembre de 2020]

DELGADO GRANADOS, María de Lourdes, "Delitos informáticos, delitos electrónicos", Orden Jurídico, información visible en:

http://www.ordenjuridico.gob.mx/Congreso/pdf/120.pdf [Fecha de consulta: 02 de octubre de 2020]

MAGLIONA MARKOVICTH, Claudio Paul, *et al.*, *Delincuencia y Fraude Informático, Jurídica de Chile*, 1999, *op. cit.* ACURIO DEL PINO, Santiago,"Delitos informáticos: generalidades", 2016, Información visible en: https://www.oas.org/juridico/spanish/cyb_ecu_delitos_inform.pdf [Fecha de consulta: 18 de octubre de 2020]

MEZA LOPEHANDIA, Matias, "Los delitos cibernéticos en la legislación estadounidense", Biblioteca del Congreso Nacional de Chile, 2014, Chile, visible en: https://obtienearchivo.bcn.cl/obtienearchivo?id=repositorio/10221/20864/5/FINAL%20_%20Informe%20_%20Cibercrimen%20en%20EEUU_v5.pdf [Fecha de consulta: 09 de noviembre de 2020]

-LIBROS

ALVARADO, Rolando y MORALES, Ronald, *Cibercrimen*, s.f., España, Ius ediciones, 2012.

TÉLLEZ VALDÉS, Julio *Los Delitos informáticos. Situación en México, Informática y Derecho* Nº 9, UNED, Centro Regional de Extremadura, Mérida, 1996.

TÉLLEZ VALDÉS, Julio, *Derecho Informático*, 4ª ed., México, Mc Graw-Hill, 2008. -

REVISTAS Y PUBLICACIONES PERIÓDICAS CALLEGARI, Nidia "Delitos Informáticos y Legislación" 2015, visible en:

https://egov.ufsc.br/portal/sites/default/files/6054-12231-1-sm.pdf

COLEOTE,Cinthya, "Rompen silencio víctimas poblanas de Brad Hunter" Excelsior agosto 2020, información visible en: https://www.excelsior.com.mx/nacional/rompenel-silencio-victimas-poblanas-de-brad-hunter/1401076
[Fecha de consulta: 24 de noviembre de 2020]

DELGADO, Ángel, "Ley olimpia de 3 a 6 años de prisión a quien difunda packs", El universal, 2018, información visible en: https://www.eluniversal.com.mx/estados/leyolimpia-de-3-6-anos-de-prision-quien-difunda-packs [Fecha de consulta: 24 de noviembre de 2020]

"Desarticulada en Granada una red de cibercriminal liderada p2or dos menores tras 47 estafas" en Periódico El País, 2020, información visible en: https://elpais.com/espana/2020-08-19/desarticulada-en-granada-un-red-decibercrimen-liderada-por-dos-menores-tras-47-estafas.html [Fecha de consulta: 20 de octubre de 2020]

ESPEJO, Joskua, "Policía Cibernética de Puebla, sin atribución en 6 de cada 10 denuncias", Datamos, Noviembre 2020, información visible en:

https://datamos.com.mx/2019/12/18/policia-cibernetica-de-puebla-sin-atribucion-en6-de-cada-10-denuncias/

FORBES, Staff, "Senado aprueba ley olimpia: 6 años de cárcel por acoso sexual digital", Forbes México, Noviembre 2020, información visible en:

https://www.forbes.com.mx/politica-senado-ley-olimpia-hasta-6-anos-carcel-acososexual-digital/
[Fecha de consulta: 24 de noviembre de 2020]

GARCÍA, Elvia, "Aumentan 28% delitos cibernéticos en Puebla; al dia hay 15 reportes", Milenio, 2020, Puebla, información visible en:

https://www.milenio.com/policia/aumentan-28-los-delitos-ciberneticos-en-puebla

GÓMEZ, Paulina, "Cada semana 12 poblanos son víctimas de ciberdelitos", El sol de Puebla, 2019, Puebla, información visible en: https://www.elsoldepuebla.com.mx/policiaca/cada-semana-12-poblanos-sonvictimas-de-ciberdelitos-puebla-3261724.html [Fecha de consulta: 23 de noviembre de 2020]

GÓMEZ, Paulina, “Dispara confinamiento a los ciberdelitos en Puebla; piden no caer en falsas ofertas”, El sol de Puebla julio 2020, información visible en:https://www.elsoldepuebla.com.mx/policiaca/dispara-confinamiento-losciberdelitos-en-puebla-piden-no-caer-en-falsas-ofertas-seguridad-policia-ciberneticainternet-pandemia-covid19-ciberfraude-ciberextorsion-ciberamenaza-5491110.html [Fecha de consulta: 25 de noviembre de 2020]

“Hackers chinos robaron información en España sobre vacuna contra Covid-19. 2020”. El Economista, 2020, información visible en:https://www.eleconomista.com.mx/internacionales/Hackers-chinos-robaroninformacion-en-Espana-sobre-vacuna-contra-Covid-19-20200918-0041.html [Fecha de consulta: 20 de octubre de 2020]

JIMÉNEZ ROJAS, Jesús Ramón, “Delitos informáticos en México”, *Seguridad*, México, UNAM, 2018, núm. 26, información visible en: https://revista.seguridad.unam.mx/numero26/delitos-inform-ticos-en-m-xico [Fecha de consulta: 09 de noviembre de 2020]

INTERPOL, Secretaría General de INTERPOL 200, quai Charles de Gaulle 69006 Lyon Francia “CIBERDELINCUENCIA: EFECTOS DE LA COVID-19”, 2020 p.5, información visible en: https://www.interpol.int/es/Noticias-yacontecimientos/Noticias/2020/Un-informe-de-INTERPOL-muestra-un-aumentoalarmante-de-los-ciberataques-durante-la-epidemia-de-COVID-19 [Fecha de consulta: 27 de octubre de 2020]

MAYER LUX, Laura y OLIVER CALDERÓN, Guillermo, “El delito de fraude informático: concepto y delimitación”, Revista chilena derecho tecnológico, 2020, vol.9, n.1, información visible en: https://scielo.conicyt.cl/scielo.php?pid=S071925842020000100151&script=sci_arttext [Fecha de consulta: 20 de octubre 2020]

OCHOA, Maricela, “Delitos Informáticos en México, ¿Que dice la ley?”,IT Masters MAG, 2020, información visible en: https://itmastersmag.com/noticiasanalisis/delitos-informaticos-en-mexico-que-dice-la-ley/ [Fecha de

RODRIGUEZ DAVARA, Miguel Angel. Manual de Derecho Informático. *Revista Chilena de Derecho Informático*, 2002.

TÉLLEZ VALDÉS, Julio, “Delitos Informáticos: Situación en México”, Informática y derecho: Revista iberoamericana de derecho informático,Nº 9-11, 1996,vol. I, visible en: https://dialnet.unirioja.es/servlet/articulo?codigo=248768 [Fecha de consulta: 10 de noviembre de 2020]

-DOCUMENTOS

"Estudio exhaustivo sobre el delito cibernético", *United Nations Office on Drugs and Crime,* 2013, visible en: https://www.unodc.org/documents/organizedcrime/cybercrime/Cybercrime_Study_Spanish.pdf

LOREDO GONZALEZ, Jesús Alberto, "Delitos informáticos: su clasificación y una visión general de las medidas de acción para combatirlo", Universidad Autónoma de Nuevo León, 2013, información visible en: http://eprints.uanl.mx/3536/1/Delitos_informaticos.pdf [Fecha de consulta: 20 de octubre de 2020]

IBARRA SÁNCHEZ, Ernesto, "Protección de niños en la red: sexting, ciberbullying y pornografía infantil", México, UNAM,Instituto de Investigaciones Jurídicas, informacion visible en: https://archivos.juridicas.unam.mx/www/bjv/libros/8/3646/5.pdf [Fecha de consulta: 17 de octubre de 2020]

INTERPOL, Secretaría General de INTERPOL 200, quai Charles de Gaulle 69006 Lyon Francia "Ciberdelincuencia: efectos de la covid-19", 2020, información visible en: https://www.interpol.int/es/Noticias-y-acontecimientos/Noticias/2020/Un-informe-deINTERPOL-muestra-un-aumento-alarmante-de-los-ciberataques-durante-laepidemia-de-COVID-19 [Fecha de consulta: 27 de octubre de 2020]

PIÑA LIBIEN, Hiram Raúl, "Delitos informáticos previstos y sancionados en el ordenamiento jurídico mexicano", información visible en:

http://www.ordenjuridico.gob.mx/Congreso/2doCongresoNac/pdf/PinaLibien.pdf [Fecha de consulta: 09 de noviembre de 2020]

TEMPERINI MARCELO, Gabriel Ignacio, "Delitos informáticos en Latinoamérica: Un estudio de derecho comparado. 1ra. Parte", información visible en: http://conaiisi.unsl.edu.ar/2013/82-553-1-DR.pdf [Fecha de consulta: 10 de noviembre de 2020]

TORRES RUIZ, Pedro,"Aspectos generales de los delitos informáticos y el combate a los mismos", información visible en: http://ordenjuridico.gob.mx/Congreso/2doCongresoNac/pdf/TorresRuiz.pdf [Fecha de consulta: 19 de octubre de 2020]

-FUENTES ELECTRÓNICAS

ARGUELLES ARELLANO, María del Consuelo, “Retos de la legislación informática en México”, vol.20, n.4, Computación y sistemas, 2016, visible en: http://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S1405554620160004008 27 [Fecha de consulta: 10 de noviembre de 2020]

CORONA, Pablo, *¿Qué es el ciberbullying?*, Gobierno de México, 2016, información visible en: https://www.gob.mx/ciberbullying/articulos/que-es-el-ciberbullying [fecha de consulta: 05 Octubre 2020]

CiberPolicía Pue | Facebook, (1) CiberPolicía Pue (@CiberPoliciaPue) / Twitter, Número de habitantes. Puebla (inegi.org.mx), [Fecha de consulta: 25 de noviembre de 2020]

https://centrosconacyt.mx/objeto/delitosinform/ [Fecha de consulta: 04 de Octubre 2020]

http://ssp.puebla.gob.mx/index.php/delitos-ciberneticos [Fecha de consulta: 25 de octubre de 2020]

Tabla es de elaboración propia con información tomada de las siguientes fuentes: https://biblioteca.cejamericas.org/bitstream/handle/2015/1723/cl-bcn-delitosinformaticos.pdf?sequence=1&isAllowed=y; https://www.poderjudicialmichoacan.gob.mx/tribunalm/biblioteca/almadelia/Cap4.htm https://obtienearchivo.bcn.cl/obtienearchivo?id=repositorio/10221/20864/5/FINAL%20_%20Informe%20_%20Cibercrimen%20en%20EEUU_v5.pdf [Fecha de consulta: 09 de noviembre de 2020]

LEGISLACIÓN NACIONAL

Código Penal Del Estado Libre y Soberano De Puebla

Código Penal Federal

Código Penal para el Estado de Guerrero

Código Penal para el Estado de Hidalgo

Código Penal para el Estado de Morelos

Código Penal para el Estado de México

Código Penal para el Estado de Nuevo León

Código Penal para el Estado de Sinaloa

Código Penal para el Estado Libre y Soberano de Jalisco

Código Penal para el Estado Libre y Soberano de Quintana Roo

Código Penal para el Estado Libre y Soberano de Tlaxcala

Código Penal Para El Estado Libre y Soberano De Veracruz De Ignacio De La Llave

-JURISPRUDENCIA

Tesis 1a. CXCII/2011 (9a.) Semanario Judicial de la Federación y su Gaceta, Décima Época, Octubre de 2011, Página: 1094.

ANEXOS

ANEXO 1: Protocolo de investigación

PROTOCOLO DE INVESTIGACIÓN

“DELITOS CIBERNÉTICOS”

ELBA JAHANA THANAYRI ROMERO APONTE IVANA VÁSQUEZ CONTRERAS
MARIFER ORTIZ BALLHAUS

EL PROTOCOLO DE INVESTIGACIÓN

TEMA

"DELITOS CIBERNÉTICOS"

OBJETIVOS

-DEFINIR LOS DELITOS CIBERNÉTICOS Y SUS TIPOS

-REVISAR LAS LEYES QUE EXISTEN PARA COMBATIR LOS DELITOS CIBERNÉTICOS EN EL MUNDO

-ANALIZAR LA LEGISLACIÓN DEL ESTADO DE PUEBLA EN MATERIA DE DELITOS CIBERNÉTICOS

HIPÓTESIS

¿SÍ LOS DELITOS CIBERNÉTICOS SE DETERMINARÁN DE FORMA MÁS PRECISA EN EL CÓDIGO PENAL DEL ESTADO DE PUEBLA SE LOGRARÍA UNA MAYOR CERTEZA JURÍDICA?.

JUSTIFICACIÓN DE LA INVESTIGACIÓN

La evolución de la sociedad a partir de la globalización y las nuevas tecnologías han dado lugar a un panorama extenso en el uso del internet. Si bien sabemos el uso de éste como una herramienta nos proporciona grandes ventajas para el desarrollo social y para el desempeño de las actividades diarias; entre ellas se encuentra la facilidad para adquirir bienes y servicios nacionales e internacionales, tener a disposición de forma instantánea información de toda índole, facilita el acceso a programas que fomentan la educación, el conocimiento, la cultura, promueve la libertad de expresión sobre temas polémicos y de interés público. No obstante, el uso de esta herramienta se ha ido tergiversando para el uso de fines nocivos y para la comisión de delitos.

Hoy en día se ven nuevos actos ilícitos y conductas antisociales que se cometen por medio de las tecnologías de la información, el desarrollo del internet ha quebrantado las barreras de su fin primordial y para el que fue creado, llegando a un punto en el que no hay un límite a su uso y al tipo de contenidos que se suben a la red; se han abierto nuevas oportunidades para infringir la ley, ya que cualquier persona desde el

anonimato o con datos falsos puede cometer delitos, causando daños patrimoniales, a la personalidad, fiscales, financieros, inclusive los que perturben al orden público.

Nos enfrentamos ante una situación de riesgo, donde no se encuentra plenamente establecido la naturaleza jurídica de cada uno de los actos delictivos que se pueden cometer en el internet; es por ello que es necesario que se regulen las consecuencias del uso indebido de los medios informáticos, que hoy en día son cada vez más frecuentes.

Ahora bien, nuestras legislaciones actuales tanto federal y de las entidades federativas sobre delitos informáticos se han visto superadas por la rápida evolución de los medios electrónicos. Uno de los principales problemas es la incorporación de las nuevas figuras delictivas que han surgido a la largo de los últimos años y de la adecuación de los distintos tipos penales ya existentes, por lo que resulta de vital importancia reformar los distintos ordenamientos vigentes para crear nuevos tipos penales que logren sancionar a estas figuras por la ley. (Medina, D, 2020)

Unas de las razones por las que es de suma importancia regular de forma precisa y más clara los delitos cibernéticos en el Código Penal del Estado de Puebla es por la afectación de los derechos fundamentales, tales como la dignidad humana, seguridad física y psicológica, así como, un menoscabo al patrimonio, vulnera la libertad sexual, el desarrollo de la personalidad y la vida misma.

Como podemos ver, en el estado de Puebla el desarrollo del uso de redes, medios tecnológicos y sistemas informáticos ha demostrado un incremento en la comisión de delitos cibernéticos, puesto que en lo que va de los últimos años se reciben una gran cantidad de denuncias por se han perfilado varios campos de posible conflicto debido a la ausencia de reglas suficientemente claras. Hay quienes consideran que basta con legislar, aunque el problema es de mayor complejidad debido a las características únicas de Internet.

La legislación actual sobre delitos cibernéticos en Puebla se encuentra tipificado en el Código Penal del Estado de Puebla en el apartado de “Delitos Informáticos” Cap. 25o, del Art. 475 al 478; y de forma secundaria en los delitos de “Extorsión” en el Art. 292 Bis, en el de “Amenazas” en su Art. 290 Frac I y II, el de “Fraude” en el Art. 402, y en la “Pornografía Infantil” en el Art 217, Frac. I) y, por último en el Reglamento Interno de la Secretaría de Seguridad Pública del Estado de Puebla. No obstante,

dichos supuestos se encuentran generalizados, por lo que al ser mencionados a grosso modo, carecen del énfasis que requieren para su correcta interpretación y por ende obstaculiza que sean sancionados.

En palabras de Gutiérrez (2003), algunos delitos como los fraudes cibernéticos, el phishing, el pharming, la trata de personas y la pornografía, se encuentran tipificados en México a nivel Federal, Estatal y Municipal; sin embargo, la formación de ciberpolicias es insuficiente en este ámbito, ya que su labor es preventiva y no tiene las atribuciones para llevar a cabo una investigacion, debido al requerimiento de contar con previa autorizacion de una autoridad jurisdiccional.

Por otro lado, existe un desconocimiento por parte de la sociedad que constantemente sufre de estos actos ilícitos, ya que los ciudadanos navegan por el internet sin preocupación alguna y sobre todo sin saber que pueden ser víctimas de estos mismos, es por ello que han aumentando de forma exponencial.

Si bien es cierto,el poder legislar los delitos cibernéticos cuenta con cierta dificultad ya que el Internet no puede ser restringido ni limitado como tal, no es fácil definir las fuentes de donde proviene la información y quién está realizando esos actos, toda vez que los sujetos activos muchas veces actúan de forma anónima; Sin embargo, debido al alcance y trascendencia que han tenido en los últimos años se ha visto la necesidad de que los Estados delimiten los distintos tipos de delitos cibernéticos existentes así como un mecanismo de seguimiento de estos.

Es así que, a nivel internacional existen ciertos convenios y reglamentaciones que regulan de forma amplia los delitos cibernéticos, tales como el Convenio sobre la Ciberdelincuencia de Budapest, el Cybercrime Legislation Toolkit de la Unión Internacional de Telecomunicaciones, la Ley Modelo de la Commonwealth sobre Delitos Informáticos entre otras, que buscan dar un marco de referencia para los Estados con el fin de que estos creen una legislación eficaz que permita combatir estos delitos.

De acuerdo con el autor, Loredo (2013):

> “Una de las principales limitaciones que presentan estos acuerdos es la reducida cantidad de países miembros con los que cuenta, a abril de 2010 la Convención sobre el Delito Cibernético del Consejo de Europa tenía el más amplio alcance: ha sido firmada por 46 Estados y ratificada por 26 , son los

países desarrollados quienes cuentan con la experiencia y los recursos que demanda la implementación de este tipo de acuerdos".

Por consiguiente, estos convenios y reglamentaciones quedan como un instrumento de referencia doctrinal. La actual legislación Penal de Puebla tiene precedentes en medios internacionales para crear y reformar dicha legislación que amplíe su marco regulatorio en materia de delitos informáticos, con el fin de que no siga existiendo una impunidad de estos mismos.

> "La doctrina del Derecho de la Informática, ha identificado tres alternativas de solución para hacer frente al problema jurídico que representa la sociedad informatizada, mismas que consisten en: 1) la actualización de la legislación, 2) la evolución jurisprudencial; y, 3) la redacción de leyes de carácter particular." (Piña, H, 2005)

Como se ha logrado vislumbrar, el estado de derecho en México se ve rebasado por estas nuevas conductas delictivas, las autoridades legislativas no han propuesto nuevas iniciativas para colmar las lagunas existentes en materia de delitos cibernéticos, es por ello que a nivel local, el estado de Puebla no ha logrado dar el primer paso para la implementación de un marco regulatorio amplio y detallado, que permita frenar el crecimiento exponencial de los delitos informáticos en Puebla.

METODOLOGÍA:

Para la realización de este trabajo se utilizarán los siguientes métodos y técnicas:

MÉTODO ANALÍTICO: Consiste en la disolución, es decir la descomposición en partes del todo, por lo que se formula de manera separada cada uno de sus elementos. (Baena, 2011)

MÉTODO SINTÉTICO: Es el que se compone o forma un todo con elementos diversos, es decir se parte de elementos diversos, donde la razón descubre sus relaciones y se termina con la integración de los elementos en un solo conjunto o sistema conceptual. (ibidem)

MÉTODO DEDUCTIVO: Es el que parte de las ideas generales y pasa a los casos particulares, es decir va de lo general a lo particular y, por tanto no plantea un problema. (ibidem)

*TÉCNICA DE INVESTIGACIÓN DOCUMENTAL***:** Es una serie de métodos y técnicas de búsqueda, procesamiento y almacenamiento de la información contenida en los documentos, en primera instancia, y la presentación sistemática, coherente y suficientemente argumentada de nueva información en un documento científico, en segunda instancia. (Tancara, 1993).

Así mismo, esta técnica se basa en la consulta y recopilación de fuentes en libros, diccionarios, enciclopedias, revistas, leyes, jurisprudencia, entre otras.

MARCO TEÓRICO CONCEPTUAL:

Delitos cibernéticos: En un sentido amplio es cualquier conducta criminal que en su realización hace uso de la tecnología electrónica, ya sea como método, medio o fin y que, en un sentido estricto, el delito cibernético , es cualquier acto lícito penal en el que las computadoras, sus técnicas y funciones desempeñan un papel, ya sea como método, medio o fin.

Ciberbullying: 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.

Ciberfraude: Son todas aquellas conductas en las cuales las redes se convierten en instrumento esencial mediante el cual se logra un beneficio patrimonial ilícito derivado de un perjuicio patrimonial a una víctima.

Ciber Extorsión: Es aquella conducta por la que se obliga a una persona, mediante el uso de la violencia o intimidación, aplicada a través de los medios informáticos, de manera que se consiga que la víctima realice un acto en perjuicio propio o ajeno, normalmente de carácter económico, tramitado a través de la web.

Grooming: Es una conducta que se puede definir como una manera de engañar o atraer a menores por medio de Internet, en especial utilizan los chats o mensajería

instantánea para ganarse la confianza del menor de edad y poder acercarse a él fingiendo empatía, cariño, un vínculo emocional, etc., con fines de satisfacción sexual, para obtener imágenes eróticas o de actos sexuales.

Hacker: Es una persona que por sus avanzados conocimientos en el área de informática tiene un desempeño extraordinario en el tema y es capaz de realizar muchas actividades desafiantes e ilícitas desde un ordenador.

Hacking: Acceso ilegítimo de manera remota al ordenador de un usuario

Malware: Software o programas informáticos que, instalados en el ordenador o dispositivo móvil de la víctima sin su consentimiento, espían sus acciones permitiendo así obtener datos e informaciones como las antes citadas.

Manipulación de los datos: Este tipo de fraude informático conocido también como sustracción de datos, representa el delito informático más común, ya que es fácil de cometer y difícil de descubrir. Este delito no requiere de conocimientos técnicos de informática y puede realizarlo cualquier persona que tenga acceso a las funciones normales de procesamiento de datos en la fase de adquisición de los mismos.

Phishing: Se trata del envío de correos electrónicos fraudulentos aparentemente enviados por empresas y/o contactos de confianza, que intentan engañar a los destinatarios con el fin de que éstos les revelen sus datos personales, bancarios, credenciales de acceso a servicios, etcétera

Pharming: Por medio de un link redirige al usuario a una página falsa para proceder a la estafa

Spam: El famoso “correo basura” es un correo electrónico que es enviado a varias personas con el propósito de que descarguen un archivo, generalmente un virus, que roba la información del dispositivo en donde se descargó.

Virus: Es una serie de claves programáticas que pueden adherirse a los programas legítimos y propagarse a otros programas informáticos. Un virus puede ingresar en un sistema, por conducto de una pieza legítima de soporte lógico que ha quedado infectada.

CAPÍTULOS

INTRODUCCIÓN

I.¿ QUÉ SON LOS DELITOS CIBERNÉTICOS?

1.1 DEFINICIÓN

1.2 TIPOS DE DELITOS CIBERNÉTICOS

1.3 AFECTACIÓN DE LOS DELITOS CIBERNÉTICOS EN NUESTRO DESARROLLO

II. PRECEDENTES EN MATERIA DE DELITOS CIBERNÉTICOS

2.1 REVISAR LAS LEYES QUE EXISTEN PARA COMBATIR LOS DELITOS CIBERNÉTICOS EN EL MUNDO

2.2 COMPARAR LAS DIFERENTES LEYES QUE EXISTEN ACERCA DE LOS DELITOS CIBERNÉTICOS A NIVEL INTERNACIONAL

2.3 ANALIZAR LA LEGISLACIÓN EN MATERIA FEDERAL DE DELITOS CIBERNÉTICOS EN MÉXICO

III. DELITOS CIBERNÉTICOS EN EL ESTADO DE PUEBLA

3.1 ANALIZAR EL CÓDIGO PENAL DEL ESTADO DE PUEBLA EN MATERIA DE
DELITOS CIBERNÉTICOS

3.2 DEFICIENCIAS DE LA LEGISLACIÓN ACTUAL EN PUEBLA

3.3 DESARROLLAR POSIBLES SOLUCIONES

3.2 CONCLUSIONES

BIBLIOGRAFÍA:

-ALFOCEA J. (2018). Qué son y cuáles son los delitos cibernéticos. 2020, de DELITO PENAL Sitio web: https://delitopenal.com/cuales-los-delitosciberneticos/#:~:text=Algunos%20de%20los%20delitos%20cibern%C3%A9tico s,la%20identidad%20de%20las%20personas.

-Baena, G. (2011). Metodología de la Investigación. Grupo Editorial Patria

-Campos, P. (2016, julio 8). Delitos informáticos en México y sus formas de prevención. Tópicos Latinoamérica, Vol. 1, 29-47.

-Corona P. (2017). ¿Qué es el ciberbullying?. 2020, de gob.mx Sitio web: https://www.gob.mx/ciberbullying/articulos/que-es-el-ciberbullying

-Delgado María. (s/f). Delitos Informáticos, Delitos electrónicos . de Orden Jurídico Sitio web: http://www.ordenjuridico.gob.mx/Congreso/pdf/120.pdf

-Eliasson J. (2015). Delito cibernético. 2020, de NACIONES UNIDAS Sitio web: https://www.un.org/es/events/crimecongress2015/cibercrime.shtml

-Galarza K. (2019). Cibergrooming. 2020, de ABCUNIVERSIDADES Sitio web: https://www.abcuniversidades.com/Articulos/350/Cibergrooming__acoso_sexual_an_internet.html

-GARCÍA E.. (2020). Aumentan 28% delitos cibernéticos en Puebla; al día hay 15 reportes. 2020, de Milenio Sitio web: https://www.milenio.com/policia/aumentan-28-los-delitos-ciberneticos-enpuebla

-Medina D. (2020). Los delitos cibernéticos y los problemas a enfrentar. 2020, de UNAM Sitio web: https://revistas.juridicas.unam.mx/index.php/hechos-yderechos/article/view/14381/15543

-Tancara Q. (1993). LA INVESTIGACIÓN DOCUMENTAL. *Temas Sociales* , (17), 91-106. Recuperado en 14 de septiembre de 2020, de http://www.scielo.org.bo/scielo.php?script=sci_arttext&pid=S004029151993000100008&lng=es&tlng=es.

-Trejo, E. (2006). Regulación Jurídica de Internet. México, D.F: Dirección de Servicios de Investigación y Análisis. Disponible en: http://www.diputados.gob.mx/sedia/sia/spe/SPE-ISS-12-06.pdf

(Trujano, P; Dorantes, J, 2009) VIOLENCIA EN INTERNET: NUEVAS VÍCTIMAS, NUEVOS RETOS Liberabit. Revista de Psicología, vol. 15, núm. 1, pp. 7-19

-Piña,H. (2005). Los Delitos Informáticos previstos y sancionados en el Ordenamiento Jurídico Mexicano . 93949, de Orden Jurídico Sitio web: http://www.ordenjuridico.gob.mx/Congreso/2doCongresoNac/pdf/PinaLibien.pdf

CRONOGRAMA:

TAREAS A REALIZAR	FECHAS DE ENTREGA
ENTREGA DE PROTOCOLO DE INVESTIGACIÓN	MARTES 15 DE SEPTIEMBRE 2020
ENTREGA CAPÍTULO I Y AVANCES CAPÍTULO II	MARTES 13 DE OCTUBRE 2020
ENTREGA CAPÍTULO II Y AVANCES CAPÍTULO III	MARTES 10 DE NOVIEMBRE 2020
ENTREGA TESINA TOTALMENTE CONCLUÍDA	MARTES 1 DE DICIEMBRE 2020
ENVÍO DE PRESENTACIÓN FINAL DE LA INVESTIGACIÓN EN POWER POINT Y DE LA INFOGRAFÍA	MARTES 3 DE DICIEMBRE 2020

ANEXO 2: Infografia Delitos Cibernéticos

ANÁLISIS DE LOS DELITOS CIBERNÉTICOS EN EL ESTADO DE PUEBLA A LA LUZ DEL DERECHO NACIONAL E INTERNACIONAL

Los delitos cibernéticos son cualquier acción ilegal en que una computadora es la herramienta u objeto del delito. [1]

EL USO DESMEDIDO

Del Internet y las tecnologías de la información han quebrantado las barreras de su fin primordial, llegando a un punto en el que no hay un límite a su uso y ha dado la pauta a abrir nuevas oportunidades para infringir la ley causándole un perjuicio a la persona víctima del delito.

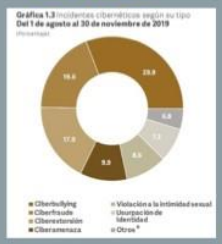
Nos encontramos ante una situación de riesgo, pues no se ha establecido la naturaleza jurídica de cada uno de los actos delictivos que se pueden cometer en el internet; es por ello que es necesario que se regulen las consecuencias del uso indebido de los medios informáticos, que hoy en día son cada vez más frecuentes.

ALGUNOS PAÍSES QUE REGULAN LOS CIBERDELITOS:
Alemania, Francia, Estados Unidos, Italia, Austria, Chile y España.

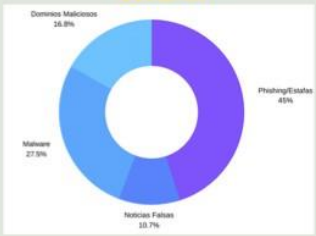
La pandemia actual causada por el virus COVID-19 ha tenido una repercusión importante en el aumento en la actividad delictiva mundial respecto de ciberamenazas y ciberdelitos a causa del confinamiento.

Las legislaciones actuales federales y estatales sobre delitos informáticos se han visto superadas por la rápida evolución de las TIC's.
La mayoría de los delitos cibernéticos NO son denunciados ni reportados a las autoridades ya que, las víctimas tienen una acepción negativa del sistema jurídico penal y no existe la debida difusión de las autoridades cibernéticas existentes ni cómo denunciar estos delitos.

LITOS CIBERNÉTICOS REGISTRADOS EN PUEBLA: [2]



CIBERAMENAZAS QUE AUMENTARON INTERNACIONALMENTE DURANTE EL COVID-19: [3]



REFERENCIAS

1. DELGADO GRANADOS, María de Lourdes, "Delitos informáticos, delitos electrónicos", Orden Jurídico, p.5, información visible en: http://www.ordenjuridico.gob.mx/Congreso/pdf/120.pdf
2. ESPEJO, Joskua, "Policía Cibernética de Puebla, sin atribución en 6 de cada 10 denuncias", Datamos, Noviembre 2020, información visible en: https://datamos.com.mx/2019/12/18/policia-cibernetica-de-puebla-sin-atribucion-en-6-de-cada-10-denuncias/
3. INTERPOL, Secretaría General de INTERPOL 200, quai Charles de Gaulle 69006 Lyon Francia "CIBERDELINCUENCIA: EFECTOS DE LA COVID-19", 2020, p.5, información visible en: https://www.interpol.int/es/Noticias-y-acontecimientos/Noticias/2020/Un-informe-de-INTERPOL-muestra-un-aumento-alarmante-de-los-ciberataques-durante-la-epidemia-de-COVID-19.

IBERO PUEBLA ®

Universidad Iberoamericana Puebla
Carrera: Derecho
Materia: Proyectos Jurídicos e Innovación (ASE III).
Integrantes: Marifer Ortiz Ballhaus
Elba Jahana Thanayri Romero Aponte
Ivana Vásquez Contreras

ANEXO 3: Tabla de Ranking de países con más sanción penal para los delitos informáticos.

N°	País	%
1	Puerto Rico	100%
2	República Dominicana	100%
3	Venezuela	100%
4	Argentina	88%
5	Costa Rica	88%
6	Panamá	88%
7	Paraguay	88%
8	Colombia	75%
9	México	75%
10	Brasil	63%
11	Chile	63%
12	Ecuador	63%
13	El Salvador	63%
14	Perú	63%
15	Uruguay	63%
16	Bolivia	50%
17	Guatemala	50%
18	Honduras	50%
19	Cuba	0%
20	Haití	0%
21	Nicaragua	0%

Tabla Nro 5. Ranking de países con más sanción penal para los delitos informáticos considerados.