**Universidad Nacional Autónoma de México**

**Facultad de derecho**

# “Derecho penal informático”

**TESIS**

Que para obtener el título de

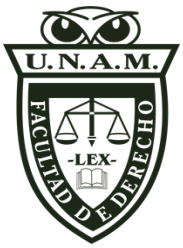
**Licenciado en Derecho**

**PRESENTA**

Juan Manuel Simbrón Castañeda

**ASESORA**

Lic. Esp. Martha Liliana Malanche Gómez



**CIUDAD DE MÉXICO** **2023**

Dedicatorias

A mi querido Hachiko-Chiwis:

El corto tiempo que estuviste conmigo

te lo agradezco todavía con lágrimas en mis ojos,

más que una mascota, eras un ser superior en amor y cariño,

sé que en el más allá nos volveremos a ver

y esta vez estaremos juntos por toda la eternidad.

A mi padre, madre, hermano y mascota Malawi:

Quien con sus acciones me convirtieron en un guerrero y ante sus omisiones a ser un rebelde con causa justa.

Agradecimientos

A la Universidad Nacional Autónoma de México, pero especialmente a mi amada Facultad de Derecho quien me dio la oportunidad de estudiar y conocer a personas espléndidas como profesores, profesoras y amigos, amigas.

A la Doctora Erika Bardales Lazcano, quien representa una segunda madre para mí por su apoyo moral y que me reconoció como un gran futuro abogado penalista, agradezco a la vida quien la puso en mi camino de estudiante. No le fallaré querida maestra.

Todo esfuerzo es inútil si no crees en ti mismo.

No dejes que nada te desvíe del camino que te has fijado y mantenlo hasta el final, sé fiel a él y enorgulléceme, sé todo lo que quieras ser.

*Might Guy.*

# DERECHO PENAL INFORMÁTICO

## ÍNDICE


INTRODUCCIÓN…… I

**CAPÍTULO I. MARCO TEÓRICO**

1.1 LA INFORMÁTICA, ORIGEN Y DESARROLLO…… 1

1.2 DERECHO PENAL. TEORÍAS Y SISTEMAS…… 7

1.2.1 SISTEMA CLÁSICO…… 8

1.2.2. SISTEMA NEOCLÁSICO…… 10

1.2.3 SISTEMA FINALISTA…… 11

1.2.4 SISTEMA FUNCIONALISTA…… 14

1.3 DERECHO PENAL INFORMÁTICO…… 17

1.4. DEFINICIÓN DE TÉRMINOS…… 18

**CAPÍTULO II. REDES SOCIALES Y CIBERSEGURIDAD**

2.1 LA IRRUPCIÓN DE LAS REDES SOCIALES -FACEBOOK, TWITTER, INSTAGRAM, TELEGRAM, TINDER-…… 24

2.2. EL ESQUEMA ICEBERG. SURFACE WEB, DEEP WEB, DARK WEB Y DARKNET…… 25

2.3. LA FUNCIÓN DE TOR, IP Y VPN…… 27

2.4. CIBERSEGURIDAD…… 29

2.4.1 USO DE KALI LINUX Y SOFTWARES UTILIZADOS PARA LOS DELITOS INFORMÁTICOS…… 29

**CAPÍTULO III. TEORÍA DE LA LEY PENAL Y DEL DELITO ENFOCADA AL ÁMBITO INFORMÁTICO**

3.1. ASPECTOS RELACIONADOS CON LA TEORÍA DE LA LEY PENAL…… 33

3.1.1 ÁMBITOS DE VALIDEZ……34

3.2. TEORÍA DEL DELITO –ELEMENTOS DEL DELITO DE LA TEORÍA TRIPTÓMICA-……37

3.2.1. TIPICIDAD……39

3.2.1.1 ELEMENTOS OBJETIVOS DEL TIPO PENAL……40

3.2.1.1.1 CONDUCTA……41

3.2.1.1.1.1 CONDUCTAS DELICTIVAS. GROOMING, SEXTING, CYBERBULLYING, PHISHING, PHARMING, CARDING, FAKE NEWS……43

3.2.1.1.2. SUJETO ACTIVO Y PASIVO…… 51

3.2.1.1.2.1 SUJETOS ACTIVOS. DELINCUENTES INFORMÁTICOS EXTERNOS E INTERNOS…… 51

3.2.1.1.3 BIEN JURÍDICO……55

3.2.1.1.4 MEDIOS COMISIVOS…… 56

3.2.1.1.5 CIRCUNSTANCIAS DE MODO, TIEMPO, LUGAR U OCASIÓN……56

3.2.1.1.6 OBJETO MATERIAL Y JURÍDICO…… 57
3.2.1.2 ELEMENTOS SUBJETIVOS DEL TIPO……57
3.2.1.3 ELEMENTOS NORMATIVOS DEL TIPO……59
3.2.2. ANTIJURIDICIDAD…….. 61
3.2.3. CULPABILIDAD…… 63

**CAPÍTULO IV. MARCO JURÍDICO**

4.1 CONVENCIONALIDAD…… 68
4.1.1 CONVENIO DE BUDAPEST ANALIZADO DESDE LA PROPUESTA DE DELITOS BÁSICOS Y DELITOS SUBORDINADOS……70
4.1.2 PROTOCOLO ADICIONAL AL CONVENIO SOBRE LA CIBERDELINCUENCIA RELATIVO A LA PENALIZACIÓN DE ACTOS DE ÍNDOLE RACISTA Y XENÓFOBA COMETIDOS POR MEDIO DE SISTEMAS INFORMÁTICOS……81
4.2 REGULACIÓN NACIONAL……83

**CAPÍTULO V. DERECHO PENAL COMPARADO. ALEMANIA Y CANADÁ**

5.1 FRAUDE INFORMÁTICO……87
5.2 DISTRIBUCIÓN DE CONTENIDO VIOLENTO O PORNOGRAFÍA DE ANIMALES……..89
5.3 DELITOS QUE TIENDEN A CORROMPER LA MORAL -MATERIALES OBSCENOS-……92

**CAPÍTULO VI. RESPONSABILIDAD PENAL DE LA EMPRESA EN LOS DELITOS INFORMÁTICOS**

6.1 LA FUNCIÓN DEL COMPLIANCE PENAL EN LOS DELITOS INFORMÁTICOS……..96
6.2 ARTÍCULO 12. CONVENCIÓN DE BUDAPEST……..99
6.3 BIENES JURÍDICOS INFORMÁTICOS DURANTE LA REALIZACIÓN DEL COMPLIANCE……102

**CAPÍTULO VII. PROBLEMÁTICAS DE LA REGULACIÓN JURÍDICA EN EL MUNDO INFORMÁTICO**

7.1 EL PROBLEMA DE LA AUTORÍA EN EL CIBERESPACIO……105
7.2 A MAYOR SEGURIDAD Y REGULACIÓN JURÍDICA EN EL MUNDO INFORMÁTICO MÁS VULNERACIÓN A LOS DERECHOS HUMANOS……109
7.2.1 CUARTA GENERACIÓN DE LOS DERECHOS HUMANOS……..110
7.2.2 El ESCUDO DORADO. INTERNET NACIONAL, CENSURA O SOLUCIÓN CONTRA LA INMUNIDAD DE LAS GRANDES EMPRESAS TECNOLÓGICAS……114
7.3. EL DELITO INFORMÁTICO……..116
7.3.1 DELITOS INFORMÁTICOS COMO SUBORDINADOS DEL DELITO TRADICIONAL……..117
7.3.2 DELITOS INFORMÁTICOS BÁSICOS……120
CONCLUSIONES……..128
PROPUESTA……130
BIBLIOGRAFÍA……135
OTRAS FUENTES……..139

# INTRODUCCIÓN

El mundo informático es muy vasto tanto como el mundo físico, por ende, al momento de querer intervenir penalmente en lo que se denomina ciberespacio se encuentran problemas que pueden ir desde la aplicación de validez espacial hasta comprender y dimensionar todo lo que acarrea tratar de definir lo que es el delito informático, pues la tecnología avanza demasiado rápido y nuestro Derecho Penal Mexicano se queda atrás ante la constante evolución de la tecnología.

Hoy en día, ya no sólo las computadoras y celulares tienen interconexiones, sino también nuestros refrigeradores, aspiradoras, e incluso nuestros autos y casas, esto es el *IoT* (*Internet of Things*), a lo cual vuelve más complicado definir lo qué es el delito informático, por ejemplo un homicidio a través de los medios informáticos (delito subordinado), en este caso puede ser en los carros autónomos, y todavía ir mucho más allá al hablar de una futura responsabilidad de los robots, así cambiando totalmente la concepción de una conducta ya no solo humana, sino también robótica autónoma. Hoy en día hablarle a un jurista de términos como *phishing*, *pharming*, *doxxing*, *cp*, *VPN*, *Kali Linux*, entre otros, es complicado porque son conductas y términos especiales que requieren una especialización en ciberseguridad, algo de lo que hoy en día se tiene muy poca concientización a pesar de que la mayor parte de nuestra vida es por el uso de redes sociales.

La responsabilidad penal informática vino a cambiar al Derecho Penal, como lo está haciendo actualmente la responsabilidad penal para las personas jurídicas a través del *compliance* penal; y para entender a la primera hay que abordar su historia, así como la irrupción de las redes sociales, los tipos de delincuentes informáticos, la utilización de *Kali Linux* y sus herramientas forenses para fines ilícitos; y sobre todo entender qué conductas delictivas informáticas son las más comunes en el ciberespacio.

Una vez entendidos estos elementos claves y básicos de la ciberseguridad podremos tener una idea de cómo podría ser definido el delito informático y tal vez

ir mucho más allá comprendiéndolo a través de la dogmática penal y análisis de ciertos tipos penales de carácter básico o subordinado que se encuentran en el código penal de la CDMX, el de Yucatán, en leyes especiales y extranjeras, pero lo más importante, como lo acabo de escribir en párrafos anteriores, es proponer una definición del delito informático, misma que aún es carente dada la complejidad que caracteriza la rápida evolución tecnológica, así como establecer las características esenciales que diferencian al delito básico y subordinado informático al momento de su estudio dentro de la dogmática penal para así poder tipificar conductas que aún no se encuentran en el Código Penal de la Ciudad de México las cuales son el contenido extremo y contenido violento y pornográfico en contra de los animales.

# CAPÍTULO I MARCO TEÓRICO

## 1.1 LA INFORMÁTICA, ORIGEN Y DESARROLLO

La informática tiene una historia tan apasionante y extensa que se podría escribir todo un libro sobre ella puesto que no solamente hoy en día se habla de una sociedad materializada sino también digitalizada, pasamos de roles físicos a roles metafísicos enfocados a las redes sociales, juegos, etc.

La informática no debe entenderse como sinónimo de computadora sino como la combinación de las palabras información y automática[1] como veremos en las definiciones pues hay un código penal en particular en nuestro país que establece los delitos informáticos y cibernéticos.

La informática y computadora son estrictamente necesarias para la evolución de nuestros dispositivos, en el caso de la informática es el *software* (entendido como el conjunto de tareas o programas que contiene el elemento físico) y la computadora es el propio *hardware* (entendido como el elemento físico que compone al sistema informático que en nuestro caso es la computadora o el celular); derivado de lo anterior no podría concebirse solamente hablar de informática sin mencionar la historia de la computadora, puesto que al hablar de información automática se refiere a que un equipo (en este caso una computadora o celular) hará el trabajo por el humano, donde *hardware* y *software* trabajaran en conjunto para realizar la labor que se le pide.

Por ejemplo: 1. Si queremos crear una página web sencilla se necesita que alguien haga esa labor por nosotros y en este caso utilizaremos *sublime text 3* y mediante lenguaje *html* se darán instrucciones al ordenador para que haga la labor que se le indique;  2. Si se quiere crear un párrafo en la página no se puede sólo escribir el párrafo bajo nuestro lenguaje natural, se debe escribir un lenguaje que

[1] Dr. Villazán Olivarez, Francisco José, *Manual de informática I*, https://www.upg.mx/wp-content/uploads/2015/10/LIBRO-31-Manual-de Informatica.pdf de 15 junio de 2021, 14:30 hrs, p. 8.

entienda el ordenador (por eso el *html*) así poniendo en el lenguaje antes mencionado  texto que queremos poner  para que la computadora haga el trabajo de manera automática.

Entonces si uno se basa en dichas ideas expuestas se puede entender por qué es inherente el desarrollo de las computadoras para el manejo, la digitalización y automatización de los datos que es propio de la informática.

La historia de la informática data de mediados del siglo XIX bajo las ideas de *Charles Babbage* y *Ada Byron*, con la creación parcial de la *Analytical Engine*.

La *Analytical Engine* fue un invento que nunca llegó a concretarse y fue el antecesor de lo que hoy conocemos como computadora moderna, dicho invento propiedad de Charles Babbage podía efectuar las 4 operaciones matemáticas más básicas y logaritmos[2]. Se dice que es el instrumento pionero de la informática, así como de las computadoras, esto porque logró automatizar operaciones matemáticas, además, por lo que se refiere a su *hardware*, dicha máquina tiene características que sirvieron de base a las computadoras posteriores.

La *Analytical Engine* se componía de una memoria para almacenar los números, una unidad de procesamiento y control y dispositivos de entrada y salida[3]. En cuanto a *Ada Byron* se le considera la primera programadora, ya que ella fue la que creó los primeros programas (entendidos como algoritmos o instrucciones que ejecutan los ordenadores) aplicables a la *Analytical Engine*, entre ellos se encuentra uno que permitía calcular la secuencia de los números de *Bernoulli*. Gracias a *Ada Byron* se vio el potencial y los posibles usos de la máquina analítica más allá de los números, incluso existe un lenguaje de programación que lleva su nombre[4].

A pesar de que la *Analytical Engine* fue sin duda el antecedente más significativo del ordenador y de la informática, no tiene mucho reconocimiento, todo fue debido a la influencia de la segunda guerra mundial (1939–1945) en donde se

[2] Véase. *System & Software Engineering, La Máquina Analítica de Babbage*, https://www.gtd.es/es/blog/la-maquina-analitica-de-babbage de 12 noviembre de 2022, 17: 10 hrs.
[3] Ídem.
[4] Véase. Facultad de biblioteconomía y documentación, *Ada Byron 1815 – 1852*, https://www.ugr.es/~anamaria/mujeres-doc/biogabyron.htm de 12 noviembre de 2022, 17: 20 hrs.

empieza a gestar la creación de las primeras computadoras y que tendría como consecuencia directa la evolución de la informática, por ejemplo, la máquina *Colossus*[5].

Inglaterra invirtió grandes cantidades de capital para la construcción de máquinas que lograran interceptar y descifrar los mensajes de la marina alemana, creando la máquina *Colossus*. También es destacable la labor de Alan Turing (uno de los mayores referentes del mundo de la informática) quien logro descifrar los códigos secretos de la máquina Enigma de la Alemania Nazi, acortando la segunda guerra mundial[6].

Otro gran paso en la evolución del ordenador y la informática fue la creación de la máquina *ENIAC* (*Electronic Numerical Integrator and Computer*) por parte de los Estados Unidos de América; la *ENIAC* fue una máquina diseñada para calcular trayectorias balísticas[7] y se establecieron las bases de lo que hoy en día entendemos como ordenador.

Para la construcción de la *ENIAC* hubo una clara división entre hombres y mujeres, pues el diseño del *hardware* (elementos físicos) fue parte del género masculino, mientras que la programación (*Software*) fue tarea del género femenino, y es aquí donde podemos decir que lo que hoy llamamos computadora deviene de la *ENIAC* (*Electronic Numerical Integrator and Computer*), pues el nombre de la máquina contiene la palabra *computer* y que viene del verbo calcular, por ende la palabra computadora es calcular o computar y se les llamaba *computer* a las personas que eran muy buenas para el cálculo matemático, es por esto, por lo que a las mujeres se les consideró mejores que los hombres al hacer cálculos

[5] Véase. Pérez, Christian, "Colossus, el primer ordenador a gran escala que ayudó a ganar la segunda guerra mundial", *Muy interesante*, 2020, https://www.muyinteresante.es/tecnologia/articulo/colossus-el-primer-ordenador-a-gran-escala-que-ayudo-a-ganar-la-segunda-guerra-mundial-251600107042 de 12 de noviembre de 2022, 18:00 hrs.
[6] Ídem.
[7] Véase. Doménech Pujol, Álvaro et al., *Un viaje a la historia de la informática*, Editorial Universitat Politécnica de Valéncia, España, 2016, https://museo.inf.upv.es/wp-content/uploads/2021/04/Un-viaje-a-la-historia-de-la-informatica.pdf de 15 junio de 2021, 14:40 hrs.

matemáticos, dejándoles la tarea de la programación de la *ENIAC*, naciendo así *The ENIAC girls*[8].

Con ello, podemos ver cómo lo que hoy llamamos computadora deviene de grandes máquinas que al principio sólo calculaban para hacer operaciones matemáticas como la *Analytical Engine*, interceptar y descifrar mensajes de la máquina alemana Enigma con la máquina *Colossus* de Alan Turing, o el cálculo de trayectorias balísticas como la *ENIAC*; actualmente, los ordenadores han sobrepasado dichos cálculos, pues las computadoras con las que se cuentan en los hogares ya no son básicas, pues no sólo calculan, sino que también se puede hablar de una digitalización del mundo físico.

En cuanto al primer ordenador personal o mejor llamado *PC* (*Personal computer*) fue creación de un grupo de ingenieros italianos en el año de 1964, que trataban de competir con la hegemonía que tenían los Estados Unidos de América con *IBM* (*International Business Machines Corporation*) en el mundo de la electrónica e informática. La primer *PC* fue construido por la empresa italiana *Olivetti*, cuyo presidente fue *Roberto Olivetti* quien dio instrucciones al ingeniero *Pier Giorgio Perotto* para la creación de una PC, siendo que él junto con Pier Giorgio Perotto junto a Gastone Garziera, Giancarlo Toppi, Giovanni de Sandre y Giuliano Gaiti crearon la *Programma 101* en el año de 1964, considerada la primera *PC* del mundo[9].

La *Programma 101* fue presentada un año después, como la primera *PC* del mundo dirigida a usuarios no especializados en el mundo de la informática, en la exposición universal de *Nueva York BEMA*. Durante su presentación, se hizo la prueba de dicha PC donde se calculaba la órbita de un satélite alrededor de la tierra[10].

La creación de la *Programma 101* dio nacimiento a la era de las PC, así creando en 1971 la *Kenbak-1* creada por el ingeniero informático John Blankerbaker

[8] Ídem.
[9] Véase. Estrella Contreras, Antonio, *La calculadora programable Programma 101*, https://museo.inf.upv.es/programma-101-4/ de 12 de noviembre de 2022, 18:35 hrs.
[10] Ídem.

y que incluso el *Computer History Museum* y la *American Computer Museum* la consideraban como el primer *PC* comercialmente disponible[11].

Por su parte, *Apple* con sus fundadores Steve Wozniak y Steve Jobs trajeron al mundo la *PC Apple I* en 1976 y *Apple II* en 1977, dichas *PC* comparten mucho parecido en su *hardware* con la *Programma 101* y la *Kenbak-1*, pero con la llegada de *Apple III* de 1980 y Lisa de 1983 se hace un cambio total a su *hardware;* así compartiendo estas dos últimas computadoras características propias de los ordenadores de escritorio que solían ser populares no muchos años atrás. En ese sentido, dentro de las laptops su antecedente más remoto es la *Apple Powerbook* de 1991[12].

En paralelo, la historia del *Software* corre con la misma suerte que la del *Hardware* o los componentes físicos que en este caso fue la computadora. El *Software* como componente lógico tiene un antecedente tan remoto como el ábaco chino antiguo, ya que tanto los componentes lógicos como físicos en sus inicios tenían como únicas tareas las operaciones más básicas de las matemáticas.

El *Software* se divide en 1. *Software* de sistema y 2. *Software* de aplicación; el primero es la gestión y la plataforma para que pueda operar el segundo, donde éste es el que realiza las tareas específicas en la propia computadora, claro ejemplo el *Software* de sistema es el sistema operativo y el *Software* de aplicación son los programas que se ejecutan cuando quieren ser utilizados[13].

Ada Byron o Lovelace, conocida por sus aportes a la máquina analítica desde el punto de vista lógico, o sea, desde el *Software* (he ahí de ser considerada la primera programadora de la historia), escribió sus famosas notas que van desde la A hasta la G, esta última es la más importante considerada como el primer programa

[11] Véase. Wilson, Bill, *John Blankerbaker, El hombre que creó la primera computadora personal de la historia*, BBC News, 2015,https://www.bbc.com/mundo/noticias/2015/11/151109_tecnologia_john_blankenbaker_hombre_creo_primera_computadora_personal_lv, de 17 junio de 2021, 19:30 hrs.

[12]Véase. Universidad Libre Colombia, *La evolución del computador*, 2015, https://www.unilibre.edu.co/bogota/ul/noticias/noticias-universitarias/256-la-evolucion-del-computador, de 20 junio de 2021. 13:25 hrs.

[13] Véase. M., José Manuel, *Diferencias entre software de sistema y software de aplicación*, 2018, https://pc-solucion.es/2018/04/16/diferencias-entre-software-de-sistema-y-software-de-aplicacion/ de 31 enero de 2022, 12:24 hrs.

de ordenador, intitulada de la misma manera. La nota G, es un escrito sobre la descripción de cómo la máquina analítica podría calcular los números de *Bernoulli*, pero sobre todo deja como predicción lo siguiente, parte del escrito de su nota G:

"La Máquina Analítica no tiene ninguna pretensión de producir nada. Puede hacer cualquier cosa que sepamos cómo ordenarle que haga"[14].

Alan Turing, fue otro gran precursor de lo que hoy conocemos como *Software*, en su artículo sobre números computables estableció lo que era computable, es decir, todo número que puede resolverse con un algoritmo, entendido éste como un conjunto de instrucciones, en tanto que el resto eran tareas no computables.

Las propiedades de numerabilidad son las siguientes:

1. Todo número racional es computable;
2. Todo número algebraico es computable;
3. Toda aritmética de punto flotante está contenida en NUMCOMP;
4. Sólo hay una cantidad de números computables;
5. La gran mayoría de los números irracionales no son computables[15].

Sin duda, Ada Byron y Alan Turing, fueron los precursores del *Software* y aunque nunca hicieron mención propiamente de dicha palabra fueron quienes formaron las primeras ideas de lo que más adelante por primera vez el matemático John Wilder Tukey haría uso de dicha palabra en su artículo *"The teaching of concrete mathematics"*[16] del año de 1958.

En 1968 nace la crisis del *Software* debido a las excesivas horas de elaboración y costos, por lo cual la OTAN en su primera conferencia sobre desarrollo de *Software*, dio nacimiento a la ingeniería de *Software* entendida como una

[14] Ada Byron, Augusta, *Nota G del bosquejo de la Máquina Analítica (El primer programa de ordenador)*, trad. de Rodríguez Alberich, Gabriel, https://notage.org/ de 31 enero de 2022, 13:05 hrs.

[15] Véase. Morales-Luna, Guillermo, *Números computables y números reales,* https://miscelaneamatematica.org/download/tbl_articulos.pdf2.8895cee46b870f64.353630322e706466.pdf, 2 de febrero de 2022, 09:37 hrs.

[16] Véase. Wilder Tukey, John, "The teaching of concrete mathematics", *The American mathematical monthly*, 1958, Vol. 65, No. 1, https://www.maa.org/sites/default/files/pdf/CUPM/first_40years/1958-65Tukey.pdf, de 2 de febrero de 2022, 12:12 hrs.

"disciplina que intenta racionalizar el proceso de desarrollo de software y establecer unas pautas a seguir para el desarrollo, por las cuales se minimice tiempo, esfuerzo, y coste de desarrollo, así como se maximice la calidad del software"[17]. Desde este punto se le empieza a dar una mayor importancia, pero sobre todo a ver como un producto empezando a dejar de lado el *Software* cooperativo.

Lo anterior daría nacimiento a las grandes empresas de *Software* privado como *Microsoft*, surgiendo *Windows 1.0* en el año de 1985. Por contraparte tenemos el *Software libre* que es la distribución, estudio, modificación y mejora de los códigos fuente, mientras que éstos son archivos que contienen instrucciones en lenguaje de programación, siendo *Unix*, es el más grande representante de los sistemas operativos libres[18].

Actualmente el *Software* es tan avanzado que no se discute sobre su gran utilidad en todos los ámbitos de la vida humana y que junto con el *Hardware* forman el binomio perfecto de la evolución humana mucho más allá del arma de doble filo que representa en la vida cotidiana.

## 1.2 DERECHO PENAL: TEORÍAS Y SISTEMAS

"El derecho penal se compone de la suma de todos los preceptos que regulan los presupuestos o consecuencias de una conducta conminada con una pena o con una medida de seguridad y corrección"[19]. De esta definición otorgada por Claus Roxin, se pueden desprender los preceptos que ordenan las consecuencias de la conducta.

Tales preceptos pueden ser entendidos como los elementos integradores del delito que son el presupuesto (propiamente la conducta), la tipicidad, la

[17] Historia de la informática, *La crisis del Software,* 2011, https://histinf.blogs.upv.es/2011/01/04/la-crisis-del-software/, de 2 febrero de 2022, 13:03 hrs.
[18] Véase. Marker, Graciela, *Software libre vs Software propietario*, https://www.tecnologia-informatica.com/software-libre-propietario/ de 12 noviembre de 2022, 19:30 hrs.
[19] Roxin, Claus, *Derecho penal. Parte general, Tomo I. Fundamentos. La estructura de la teoría del delito*, segunda edición, trad. Luzón Peña, Diego-Manuel et al, Editorial Civitas, Tomo I, Madrid, 1997, p. 41.

antijuridicidad y la culpabilidad, además de la consecuencia que es la pena o medida de seguridad.

Partiendo del presupuesto, elementos y consecuencias del delito se puede hacer un análisis de lo que constituye el derecho penal a través de su historia (no evolución) con el estudio de los sistemas penales para comprender las ideas que se han aportado desde el sistema clásico hasta el funcionalismo.

### 1.2.1 SISTEMA CLÁSICO

El sistema clásico fue el primer momento en que el que se dio un verdadero estudio a los elementos constitutivos del delito, a pesar de que se tienen antecedentes como la escuela clásica, la escuela positiva, la escuela ecléctica y la dirección técnica jurídica de donde destaca esta última debido a la desviación que estaban tomando la escuela clásica, positiva y ecléctica, cuestión que criticaba la dirección técnica jurídica, por ende, ésta, era una crítica hacia las escuelas anteriores por desviar el estudio del derecho penal, es así que Arturo Rocco, apoyado de las teorías de Von Liszt, Binding y Beling, trata de dar un cauce verdadero a la dogmática penal italiana.

Alemania, durante la mitad del siglo XIX, no perdió el camino (como había pasado en Italia) sobre el objeto de estudio de la dogmática que era el derecho penal (*Strafrecht*) creando las verdaderas bases de una dogmática penal y que, hasta hoy en nuestros días, Alemania, es el eje del derecho penal (He ahí que Italia recurriera a los sistemas e ideas penales de Alemania para encauzar el camino que habían perdido hace mucho tiempo).

Otra característica esencial que dio paso al nacimiento del sistema clásico fue el positivismo en Alemania que durante el siglo XIX se tuvo al derecho positivo como objeto de estudio, mas, sin embargo, el positivismo no tenía un único cauce, por ende, había dos corrientes: 1. Positivismo normativista y; 2. Positivismo naturalista.

El derecho penal enfocado en el positivismo normativista está centrado en el estudio de la ley, omitiendo los juicios de valor o todo lo relacionado a la realidad metajurídica de la dogmática penal, mientras que el positivismo naturalista nace de las constantes críticas al derecho penal y a la dogmática por su insensibilidad y alejamiento de los problemas sociales. El positivismo naturalista no niega al positivismo positivo, sino que lo complementa a través del análisis metajurídico donde el delito no solo es formal sino también un fenómeno social[20].

Derivado de lo anterior el positivismo naturalista, ya no solo se apoyaba de la ley penal, ahora también se auxiliaba de las ciencias naturales. Ante tal situación, es como nace con Maximilian Von Buri, la teoría de la conditio sine qua non que marca como teoría de la imputación (*Zurechnung*) al sistema clásico.

Es así como el sistema clásico como primer rasgo característico es que en la conducta en relación con el nexo causal predomina la teoría de la conditio sine qua non, la cual se puede resumir en el que es causa de la causa, es causa del daño causado[21].

En cuanto a la tipicidad, destacan los elementos objetivos como aquellos que se perciben con los sentidos y que son demostrables científicamente, así como elementos externos no debían ser concebidos en el tipo (positivismo normativo y naturalista).

La antijuridicidad era la valoración del objeto que constituía al tipo y la culpabilidad era de carácter psicológico teniendo como especies a la conducta y al dolo[22].

---

[20] Véase. Universidad de Cádiz, *Introducción al derecho penal,* España, https://ocw.uca.es/mod/book/view.php?id=1237&chapterid=14 de 13 de noviembre de 2022, 12:34 hrs.

[21] Véase. Valverde Esquinas, Patricia, "Conditio sine qua non y concreción del riesgo en el resultado: cómo eliminar un paso repetitivo en el análisis de la imputación objetiva al tipo", *Revista Penal México*, Vol. 8, núm. 14-15, marzo 2018 – febrero 2019, México, https://revistaciencias.inacipe.gob.mx/index.php/01/article/view/295/253 de 13 de noviembre de 2022, 13:50 hrs, pp. 120, 121.

[22] Véase. Plascencia Villanueva, Raúl, *Teoría del delito*, UNAM Instituto de Investigaciones Jurídicas, México, 2004, https://archivos.juridicas.unam.mx/www/bjv/libros/1/44/5.pdf de 13 de noviembre de 2022, 14: 05 hrs, p. 37.

## 1.2.2. SISTEMA NEOCLÁSICO

El sistema neoclásico es la "denominación dada al concepto de delito siguiente al clásico construido por la ciencia penal en los años 20 y 30 del siglo XX, influida por la filosofía de los valores y su consideración de que el análisis de los fenómenos sociales como el delito requiere tener en cuenta valores y normas"[23].

Este sistema, como bien se explica en la anterior definición sobresalen los valores y las normas que deben ser considerados al momento de estudio del delito, de esto derivan sus principales aportaciones que son los elementos normativos y anímicos del tipo.

La conducta ya no solo cuenta con la teoría de la *conditio sine qua non*, sino ahora también la teoría de la causalidad adecuada[24], mediante el juicio de probabilidad, por ejemplo: X1, dispara contra X2, dejándolo gravemente herido, así X2 siendo trasladado al hospital, pero durante la noche el nosocomio sufre un incendio así muriendo X2 derivado de tan lamentable suceso.

Para la *conditio sine qua non*, X1 debe responder por el delito de homicidio, pues su conducta fue condición esencial para que X2 muriera en el incendio, pero para la causalidad adecuada no puede ser imputable al delito de homicidio X1, puesto que no hay una previsibilidad objetiva derivada de que X1 hubiera sabido que no iba a matar de un disparo a X2, pero sí de un incendio que se iba a producir en el hospital, algo ilógico y carente de probabilidades.

El tipo penal como se escribió con anterioridad ya no solo se constituye de elementos objetivos, sino también anímicos y culturales. Los elementos anímicos se relacionan con el ánimo del sujeto, por ejemplo: el patrón que le dice un piropo a

[23] Diccionario panhispánico del español jurídico, *Concepto neoclásico de delito*, https://dpej.rae.es/lema/concepto-neoclásico-de-delito de 1 octubre de 2022, 09:30 hrs.

[24] Véase. Rojas – Quiñones, Sergio y Mojica – Restrepo, Juan Diego, "De la causalidad adecuada a la imputación objetiva en la responsabilidad civil colombiana", 2014, núm. 129, junio – diciembre 2014, Colombia, https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwjpydS4_av7AhXSKEQIHTZRCEMQFnoECCYQAQ&url=https%3A%2F%2Frevistas.javeriana.edu.co%2Findex.php%2Fvnijuri%2Farticle%2Fview%2F11949%2F9784&usg=AOvVaw3E-PnaQmKd81Df5-NCHBzc de 13 de noviembre de 2022, 15:00 hrs, pp. 208 – 216.

su secretaria, ¿Hasta qué punto se puede considerar acoso?, ¿Cuál fue la intención del sujeto?

El elemento normativo, destaca de la valoración jurídico o cultural sobre ciertos aspectos contenidos en el tipo. En el tipo de robo, no solo basta el *animus apropiandi,* sino por igual la valoración del elemento normativo de lo que envuelve el robo, términos como bien mueble y ajenidad que deber ser valorados desde un aspecto jurídico[25].

La antijuridicidad, por otro lado, empezó a tener características de contradicción entre el hecho y la ley, que desembocaría a una culpabilidad ya no estrictamente subjetiva pues ahora se debía requerir la valoración de las circunstancias materiales que rodean al hecho y así reprochar al sujeto al sujeto por ir contrariamente a derecho, naciendo ya no solo una culpabilidad psicológica sino también normativa[26].

### 1.2.3 SISTEMA FINALISTA

El sistema finalista parte de ideas de Alexander Graf Zu Dohna y Hans Welzel, en cuanto al primer autor, dio una idea tan esencial para este sistema al considerar que el dolo y la culpa como elementos psicológicos deberían ser parte del tipo penal (*Tatbestand*).

"La crítica a esta mezcla de elementos, tanto normativos como psicológicos, ha sido resuelta colocando los elementos psicológicos en la tipicidad; por lo tanto, el dolo ha quedado sin el elemento normativo, con lo cual se puede estructurar un concepto normativo de culpabilidad… Aceptado que el dolo y la culpa pertenecen al tipo, la culpabilidad aparece como normativa"[27].

---

[25] Véase. Universidad de Navarra, *Elementos subjetivos del injusto*, España, http://www.unav.es/penal/crimina/topicos/elementossubjetivosdelinjusto.html de 13 de noviembre de 2022, 15:49 hrs.

[26] Esta última parte -culpabilidad- es muy interesante, debido a que Reinhard Frank, es considerado el máximo exponente de la culpabilidad psicológica, algo que desde mi punto de vista no es así, y he ahí el error de querer clasificar a los autores por sistemas. Reinhard Frank, fue quien expuso la culpabilidad como reproche y las circunstancias concomitantes del hecho. Esto se abordará más adelante en el presente trabajo.

[27] Donna, Edgardo Alberto, *Teoría del delito y de la pena tomo 2 Imputación objetiva*, Editorial Astrea, tomo 2, Buenos Aires, 1995, p. 185.

Las aportaciones de Welzel son esencialmente en la conducta, derivado de esto, se da paso a la teoría de la adecuación social, lo adecuadamente social es atípico. Por ejemplo: A1 en *Halloween*, decide asustar a A2, pero de tal susto, A2, muere de un infarto. A1 no puede ser imputable por el delito de homicidio, derivado de la adecuación social, puesto que lo que es socialmente adecuado no es jurídicamente típico.

Otra característica esencial es que la causalidad deja de ser ciega, para ser una finalidad vidente o como bien lo establece Welzel de la siguiente forma:

"La acción humana es el ejercicio de la actividad finalista. La acción es, por lo tanto, un acontecimiento finalista, y no solamente causal… Por eso, gráficamente hablando, la finalidad es vidente, la causalidad es ciega"[28].

Además, Welzel, en un principio, invierte el centro del derecho penal dándole una finalidad ético social, o sea, centrado en los valores ético-sociales, dando paso a lo que denominó Wilhelm Gallas como *Gesinnungsausdruck* (expresión del sentimiento) y Jürgen Baumann como derecho penal del sentimiento. Tal aspecto, derivo en considerar que el derecho penal tiene una función ético social, por ende, protege valores de sentimiento[29].

Así, considerando que el delito en primer lugar quebranta deberes jurídicos y en segundo lugar lesiona bienes jurídicos y que de igual manera destaca el disvalor de la acción antes que el disvalor del resultado.

Ante esto, Wilhelm Gallas, estableció lo siguiente:

"En oposición crítica a la dirección teleológica, dirige la atención al aspecto personal y ético-social del injusto: El delito es injusto no sólo como lesión de bienes o intereses jurídicos, sino también, y, en primer lugar, como lesión del deber y expresión del carácter (*Gesinnungsausdruck*)"[30].

---

[28] Welzel, Hans, *Teoría de la acción finalista*, Editorial DEPALMA, Buenos Aires, 1951, pp. 19,20.

[29] Está característica del derecho penal como algo ético-social parece derivar del momento que estaba pasando Alemania, bajo el régimen nacionalsocialista.

[30] Gallas, Wilhelm, *Teoría del delito en su momento actual*, trad. de Córdoba Roda, Juan, Editorial HEBO, Ciudad de México, 2022, p. 16.

Para Jürgen Baumann, darle un sentido ético-social al derecho penal es confundirlo con las normas morales. El derecho penal debe ser en primer lugar lesión de bienes jurídicos y consecuentemente una lesión del deber, por igual debe ser primero el disvalor del resultado (*Erfolgsunwert*) y después el disvalor de la acción (*Handlungsunwert*).

> En contra de este punto de vista algunos autores sustentan la tesis de que el derecho penal tiene una función ético-social y que protege, antes que nada, valores ético-sociales de sentimiento (y de esta manera, indirectamente, también bienes jurídicos); también afirman que el delito' es en primer término lesión del deber y que hay que destacar el disvalor de la acción = disvalor del acto (y no el disvalor del resultado). Estas opiniones son inaceptables. Aíslan el derecho penal, en su función, del derecho en su totalidad, confunden norma moral y norma jurídica, corren el peligro de encontrar los componentes de lo injusto en forma preponderante en la persona del autor (y no en su acción) (el llamado concepto personal de lo injusto) y se encuentran siempre a poca distancia del precipicio del derecho penal del sentimiento[31].

Ahora bien, en cuanto a los opuestos del delito sobresale el error de tipo (*Tatbestandsirrtum*) y el error de prohibición (*Verbotsirrtum*), derivados de todas las ideas anteriores. El error de tipo es parte de un dolo que no ha sido valorado (neutro) y el error de prohibición es cuando propiamente el dolo (*Vorsatz*) ha sido valorado, así pudiendo distinguirse de manera tajante dichos errores.

Por último, la antijuridicidad pasa a ser un juicio de valor objetivo, pero en la culpabilidad, quedan removidos sus elementos psicológicos (dolo y culpa) para ser considerada predominantemente de carácter normativa.

Como se puede apreciar, el sistema finalista fue quien dio mayores cambios a la teoría del delito aportando las siguientes características:

1. Causalidad vidente y no ciega, a través de la finalidad;
2. Teoría de la adecuación social;
3. El derecho penal debe estar enfocado en lo ético-social;
4. El dolo y la culpa pasan a ser elementos del tipo subjetivo;

[31] Baumann, Jürgen, *Derecho penal conceptos fundamentales y sistema, introducción a la sistemática sobre la base de casos*, cuarta edición, trad. de A. Finzi, Conrado, Editorial DEPALMA, Buenos Aires, 1972, p. 10 .

5. El error de tipo opera en el tipo y el error de prohibición en la culpabilidad y; la culpabilidad es predominantemente normativa.

## 1.2.4 SISTEMA FUNCIONALISTA

El sistema funcionalista, destaca por la aportación de una teoría de la causalidad denominada teoría de la imputación objetiva (*Die Lehre der Objektiven Zurechnung*) y por la autoría mediata por aparatos de poder (*Mittelbare Täterschaft Kraft organisatorischer Machtapparate*), entre otras características importantes para este sistema[32].

La imputación objetiva (*Objektiven Zurechnung*) es una teoría del tipo o más propiamente de la causalidad como elemento objetivo del tipo (*Objektiver Tatbestand*), por ende, está asociada con el tema de las teorías de la causalidad ya analizadas con anterioridad.

1. Clásico: Teoría de la *conditio sine qua non*;
2. Neoclásico: Teoría de la causalidad adecuada;
3. Finalismo: Teoría de la adecuación social y;
4. Funcionalismo: Teoría de la imputación objetiva.

La imputación objetiva cuenta con varios elementos y que desde el punto de vista del Dr. Claus Roxin, la palabra clave es riesgo.

> Sin embargo, en la doctrina científica cada vez se impone más la concepción de que la imputación al tipo objetivo se produce conforme a dos principios sucesivamente estructurados:
>
> a) Un resultado causado por el agente sólo se puede imputar al tipo objetivo si la conducta del autor ha creado un peligro para el bien jurídico no cubierto por un riesgo permitido y ese peligro también se ha realizado en el resultado concreto…

[32] En lo que respecta a esta tesis, solo se trabajará con las dos primeras teorías antes escritas, puesto que este sistema cuenta con varios elementos ya sean político criminales o normativos desde el punto de vista de que autor se estudie y seria ampliar en demasía un trabajo digno de un análisis propio.

b) Si el resultado se presenta como realización de un peligro creado por el autor, por regla general es imputable, de modo que se cumple el tipo objetivo. Pero, no obstante, excepcionalmente puede desaparecer la imputación si el alcance del tipo no abarca la evitación de tales peligros y sus repercusiones…[33]

De estos fundamentos ubicados en su tratado y páginas posteriores, así como en su artículo *Gedanken zur Problematik der Zurechnung im Strafrecht* (Reflexiones sobre la problemática de la imputación en el derecho penal) y en su ensayo *Pflichwidrigkeit und Erfolg bei fahrlässigen Delikten* (Infracción del deber y resultado en los delitos imprudentes) es como da bases a la teoría de la imputación a través del riesgo[34].

Por otro lado, tenemos al Dr. Gunthër Jakobs, aportando elementos como el rol neutral[35] parte del principio de confianza, así como otro elemento característico que es la imputación a la víctima.

"El principio de confianza significa que, a pesar de la experiencia de que otras personas cometen errores, se autoriza a confiar -en una medida aún por determinar- en su comportamiento correcto (entendiéndolo no como suceso psíquico, sino como estar permitido confiar). El principio de confianza no es sólo un supuesto particular del riesgo permitido, sino también de la prohibición del regreso"[36].

"El manejo inconscientemente descuidado de los propios bienes puede llevar al obrar al propio riesgo, que exime de responsabilidad al <<dañador>>"[37].

De tales antecedentes se puede desprender la imputación objetiva con sus elementos de la siguiente manera:

1. Creación de riesgo no permitido e;
2. Incremento de riesgo permitido.

---

[33] Roxin, Claus, *Derecho penal. Parte general, Tomo I. Fundamentos. La estructura de la teoría del delito*, op. cit, pp. 363, 364.
[34] Ídem.
[35] Almanza Altamirano, Frank, *Clase gratuita sobre Imputación objetiva*, https://www.youtube.com/watch?v=66zdlgXt0J8 de 4 octubre de 2022, 12:23 hrs.
[36] Jakobs, Gunthër, *Derecho penal parte general. Fundamentos y teoría de la imputación*, segunda edición corregida, trad. de Cuello Contreras, Joaquín y Serrano González de Murillo, José Luis, Editorial Marcial Pons, Madrid, 1997, p. 253
[37] Ibidem, p. 306.

En su opuesto se tiene:

1. Disminución del riesgo;
2. Riesgo socialmente adecuado[38];
3. Riesgo mínimo o insignificante;
4. Ámbito de protección de la norma -en el caso de los delitos culposos-;
5. Rol neutral e;
6. Imputación a la víctima.

Pasando al otro tema de interés para este trabajo que es la autoría mediata por aparatos organizados de poder.

> En este lugar se va a tratar en primer lugar otra manifestación del dominio mediato del hecho que hasta ahora no ha sido ni siquiera mencionada por la doctrina ni por la jurisprudencia: el dominio de la voluntad en virtud de maquinarias o estructuras de poder organizadas. Se alude así a los supuestos que en la posguerra han ocupado en creciente medida a la jurisprudencia y que se caracterizan porque el sujeto de detrás tiene a su disposición una maquinaría personal (casi siempre organizada estatalmente) con cuya ayuda puede cometer sus crímenes sin tener que delegar su realización a la decisión autónoma del ejecutor[39].

Es así como la autoría mediata por aparatos organizados de poder, opera como parte de la autoría mediata quedando de la siguiente manera:

1. Error;
2. Coacción;
3. Inimputabilidad y;
4. Aparatos organizados de poder[40].

[38] Es muy curioso este elemento porque es como si se estuviera abordando la adecuación social, como lo que es adecuado para la sociedad es un riesgo socialmente permitido.
[39] ROXIN, Claus, *Autoría y dominio del hecho en derecho penal*, séptima edición alemana, trad. de Cuello Contreras, Joaquín y Serrano González de Murillo, José Luis, Editorial Marcial Pons, Madrid, 2000, p. 270 .
[40] Más adelante en el presente trabajo se abordará más profundamente a tema tan interesante.

## 1.3 DERECHO PENAL INFORMÁTICO

Teniendo ya, como bases propiamente la informática y el derecho penal, podemos definir al derecho penal informático como el sistema de delitos básicos y subordinados inherentes al uso de las TIC[41].

Es así que el presente trabajo partirá desde el conocimiento de la ciberseguridad que es factor esencial para conocer las herramientas que usan los cibercriminales para delinquir y una vez entendida la importancia de la ciberseguridad se pasará al estudio analítico de lo que constituye el delito informático tomando como base un poco de cada uno de los sistemas penales explicados con anterioridad, así conjuntando el delito con sus opuestos y el uso de las TIC (específicamente la informática), por ejemplo la importancia del tipo en sus clases (en nuestro caso, los tipos básicos y subordinados), así como la relación que guarda con la antijuridicidad, etc.

De igual manera, en el ámbito internacional se estudiará el Convenio de Budapest, considerado la máxima ley para el estudio integral de los delitos informáticos, para dar paso a un siguiente capítulo donde será abordado el derecho comparado y la relación de algunos tipos penales del orden informático contenidos en códigos penales como el de Alemania y Canadá.

Del análisis derivado del Convenio de Budapest, se desprenderá otro tema que es que propiamente la responsabilidad penal de las empresas en la comisión de delitos, a lo cual abordaremos ésta y como complemento se explicará lo que significa el *compliance* penal para una empresa y la importancia de éste para el momento de la prevención y defensa de la empresa para la prevención de delitos del orden informático.

Por último, se abordarán las problemáticas con las que cuenta todavía el derecho penal informático como una clara definición de lo que representa el delito

[41] "Las TIC son el conjunto de tecnologías que permiten el acceso, producción, tratamiento y comunicación de información presentada en diferentes códigos (texto, imagen, sonido, ...)". Véase. Belloch Ortí, Consuelo, *Las Tecnologías de la Información y Comunicación*, https://www.uv.es/~bellochc/pdf/pwtic1.pdf de 3 octubre de 2022, 13:42 hrs.

informático, la censura como medio de control, y la propuesta de estudio de los delitos informáticos en básicos y subordinados, donde los primeros constituyen el fundamento y atentan contra la CID, mientras que los segundos son el uso de las nuevas tecnologías para cometer delitos tradicionales.

## 1.4. DEFINICIÓN DE TÉRMINOS

1. *Phishing: "El phishing* es una técnica que consiste en el envío de un correo electrónico por parte de un ciberdelincuente a un usuario simulando ser una entidad legítima (red social, banco, institución pública, etc.) con el objetivo de robarle información privada, realizarle un cargo económico o infectar el dispositivo. Para ello, adjuntan archivos infectados o enlaces a páginas fraudulentas en el correo electrónico"[42].

2. *Pharming*: "*Pharming* es la explotación de una vulnerabilidad en el software de los servidores *DNS (Domain Name System)* o en el de los equipos de los propios usuarios, que permite a un atacante redirigir un nombre de dominio *(Domain Name)* a otro ordenador diferente"[43].

3. DNS: "*El DNS*, o sistema de nombres de dominio, traduce los nombres de dominios aptos para lectura humana (por ejemplo, www.amazon.com) a direcciones IP aptas para lectura por parte de máquinas (ejemplo, 192.0.2.44)"[44].

4. IP: "Una dirección IP es una representación numérica del punto de Internet donde está conectado un dispositivo. Se usa para identificar dónde hay algo

[42] Instituto Nacional de Ciberseguridad, *Phishing*, España, https://www.incibe.es/aprendeciberseguridad/phishing de 2 octubre de 2022, 15:56 hrs.
[43] Rodríguez Magariños, Faustino Gudin, *Nuevos delitos informáticos: Phishing, Pharming, Hacking y Cracking*, https://web.icam.es/bucket/Faustino%20Gud%C3%ADn%20-%20Nuevos%20delitos%20inform%C3%A1ticos.pdf de 2 octubre de 2022, 16:05 hrs.
[44] Amazon Web Services, *¿Qué es DNS?*, https://aws.amazon.com/es/route53/what-is-dns/ de 2 octubre de 2022, 16:14 hrs.

y, en cierto modo, qué es. Comprender los fundamentos de las direcciones IP es esencial para desenvolverse por Internet"[45].

5. *Doxing*: "El *doxing* (a veces escrito como doxxing) consiste en revelar información identificadora de una persona en línea, como su nombre real, dirección particular, lugar de trabajo, teléfono, datos financieros y otra información personal. Luego, esta información se divulga al público sin el permiso de la víctima"[46].

6. *Exploit*: "Un *exploit* es un programa informático, una parte de un software o una secuencia de comandos que se aprovecha de un error o vulnerabilidad para provocar un comportamiento no intencionado o imprevisto en un software, hardware o en cualquier dispositivo electrónico"[47].

7. *Payload*: "En *Metasploit* tenemos los exploits y los *payloads*. Un exploit es una vulnerabilidad, y el *payload* es la carga que se ejecuta en esa vulnerabilidad, es decir, la carga que activamos a la hora de aprovechar dicha vulnerabilidad"[48].

8. *Hardware y software*: "*Hardware* es el conjunto de componentes físicos de los que está hecho el equipo y *software* es el conjunto de programas o aplicaciones, instrucciones y reglas informáticas que hacen posible el funcionamiento del equipo"[49].

9. *Meatspace y cyberspace*: "La palabra "espacio de la carne" se refiere al mundo físico de la vida real en el que vivimos. El término se inventó en contraste con la aparición del "ciberespacio", que es el mundo virtual

[45] Patrizio, Andy, *¿Qué es una dirección IP?*, 2022, https://www.avast.com/es-es/c-what-is-an-ip-address de 2 octubre de 2022, 16:30 hrs.
[46] Kaspersky, *Doxing: definición y explicación*, https://latam.kaspersky.com/resource-center/definitions/what-is-doxing de 2 octubre de 2022, 16:40 hrs.
[47] Pandasecurity, *¿Qué es un exploit?,* https://www.pandasecurity.com/es/security-info/exploit/ de 3 octubre de 2022, 10:03 hrs.
[48] Rizaldos, Héctor, *Qué es un payload*, https://openwebinars.net/blog/que-es-payload/ de 3 octubre de 2022, 10:15 hrs.
[49] GCFGlobal, *¿Qué es Hardware y software?*, https://edu.gcfglobal.org/es/informatica-basica/que-es-hardware-y-software/1/ de 3 octubre de 2022, 10:30 hrs.

interconectado de computadoras en el que interactuamos. En un contexto moderno, el ciberespacio estaría completamente en línea, mientras que el espacio físico estaría completamente fuera de línea"[50].

10. VPN: "La sigla VPN viene del inglés *Virtual Private Network*, que en español sería red privada virtual, que, en comparación con otras palabras informáticas, como HTTP, sí nos dan unas pistas precisas sobre hacia qué va el concepto… Lo que permite una conexión VPN es crear una red local sin que los integrantes estén físicamente en un mismo espacio, sino a través de internet. De ahí que su nombre sea red privada virtual"[51].

11. TOR: "Tor *Browser* aísla cada sitio web que visitas para que los rastreadores y anuncios de terceros no puedan seguirte. Cualquier cookie se borra automáticamente cuando terminas de navegar. También lo hará su historial de navegación, evita que alguien que esté viendo tu conexión sepa qué sitios web visitas. Todo lo que cualquier persona que controle tus hábitos de navegación puede ver es que estás usando Tor"[52].

12. *Router*: "Los *routers* guían y dirigen los datos de red mediante paquetes que contienen varios tipos de datos, como archivos, comunicaciones y transmisiones simples como interacciones web"[53].

13. *Hidden Wiki*: "Es uno de los directorios de enlaces más antiguos de la *dark web*. Famoso por listar todos los enlaces *onion* importantes. Desde los mercados de medicamentos hasta los servicios financieros"[54].

14. HTTPS: Protocolo de transferencia de hipertexto seguro (HTTPS) es una versión segura del protocolo HTTP. El protocolo HTTPS hace posible que los usuarios del

[50] Diario informe, *¿Qué significa "Meatspace" ?*, https://diarioinforme.com/que-significa-meatspace/ de 3 octubre de 2022, 10:50 hrs.
[51] Bautista García, Iván Jahel, *VPN: ¿Qué es y para qué sirve?,* https://www.servnet.mx/blog/vpn-que-es-y-para-que-sirve de 3 octubre de 2022, 11:08 hrs.
[52] The Tor Project, Inc., *Navegar en privado. Explora libremente*, https://www.torproject.org/ de 3 octubre de 2022, 11:17 hrs.
[53] CISCO, *¿Qué es un Router?*, https://www.cisco.com/c/es_mx/solutions/small-business/resource-center/networking/what-is-a-router.html de 3 octubre de 2022, 11:34 hrs.
[54] Hidden wiki, *Hidden wiki*, https://thehiddenwiki.org de 3 octubre de 2022, 11:43 hrs.

sitio web transmitan datos confidenciales como números de tarjetas de crédito, información bancaria y credenciales de inicio de sesión de forma segura a través de Internet. Por esta razón, HTTPS es especialmente importante para asegurar actividades en línea como compras, banca y trabajo remoto. Sin embargo, HTTPS se está convirtiendo rápidamente en el protocolo estándar para todos los sitios web, ya sea que intercambien o no datos confidenciales con los usuarios[55].

15. Binero: "Los bineros son los "*carders*" más comunes, no roban tarjetas, solo se aprovechan del método de pago. Un bin (*Bank Identification Number*) son los 6 primeros números de una tarjeta de crédito…"[56]

16. *Script Kiddie*: "*Script Kiddie* (en español, niño de guion, y también conocido como *Script Bunny, Skiddie o Script Kitty*) es un término para designar a un hacker no cualificado que depende en gran medida del software y los scripts de terceros para llevar a cabo ciberataques en redes informáticas, sistemas y sitios web"[57].

17. *Surface web*: "En internet, estos espacios públicos se conocen como *surface web* (internet visible). Son las páginas web, las aplicaciones web y otros elementos en línea que los *bots* de búsqueda —los equivalentes digitales de las cámaras cartográficas— pueden indexar. Pueden albergar documentos, archivos multimedia y más. Cualquier persona puede usar un motor de búsqueda y verlos sin pagar, registrarse o instalar un *software* especial"[58].

18. *Deep web*: "*Deep web* también se refiere al contenido para el cual no existen enlaces provenientes de la web superficial o visible. Un *bot* de búsqueda simplemente no sabe que dicho contenido existe; encuentra nuevas páginas seguidas de enlaces a partir de página que ya existen. Del mismo modo en

[55] Equipo de soporte de SSL, *¿Qué es HTTPS?*, https://www.ssl.com/es/preguntas-frecuentes/que-es-https/ de 3 octubre de 2022, 12:00 hrs.
[56] Malumbres Cervera, Eduardo Pérez, *Carding, ¿Cómo nos la lían?*, https://derechodelared.com/carding/ de 4 octubre de 2022, 18:08 hrs.
[57] ESGEEKS, *¿Qué es un Script Kiddie? Características y peligros*, https://esgeeks.com/script-kiddie-que-es/ de 4 octubre de 2022, 18:15 hrs.
[58] Grustniy, Leonid, *Darknet, Darkweb, Deep web y Surface web: las diferencias*, https://latam.kaspersky.com/blog/deep-web-dark-web-darknet-surface-web-difference/20962/ de 4 octubre de 2022, 18:30 hrs.

que el coche de *Google Street View* no puede entrar a un patio, los *bots* de búsqueda no pueden encontrar contenido sin enlaces"[59].

19. *Darkweb*: "La "*Dark Web*" utiliza complejos sistemas que anonimizan la verdadera dirección IP de un usuario, lo que hace muy difícil averiguar qué sitios web ha visitado un dispositivo. Generalmente se accede a ella mediante un software específico, el más conocido es el llamado Tor (*The Onion Router*)"[60].

20. *Darknet*: "A diferencia de la *Dark Web* – que son las páginas de contenido existente en la web que ha sido deliberadamente ocultado – la *darknet* son redes específicas, como TOR o I2P, que alojan esas páginas"[61].

21. Ciberseguridad: "La ciberseguridad es la práctica de proteger sistemas, redes y programas de ataques digitales. Por lo general, estos ciberataques apuntan a acceder, modificar o destruir la información confidencial; Extorsionar a los usuarios o los usuarios o interrumpir la continuidad del negocio"[62].

22. Estructura crítica: "Las estructuras críticas incluyen las redes gubernamentales, los equipos físicos de suma importancia, los sistemas de almacenamiento que estén centralizados con todos los datos de los ciudadanos y los servicios fundamentales para la vida, como la electricidad o el gas"[63].

---

[59] Ídem

[60] Universidad Autónoma de Madrid, *¿Tienes clara la diferencia entre Darkweb, Deepweb y Darknet?*, https://www.uam.es/uam/vida-uam/bibliotecas/biblioteca-politecnica/noticias/diferencias-darkweb-deepweb-darknet de 4 octubre de 2022, 18:43 hrs.

[61] Ídem.

[62] CISCO, *¿Qué es la ciberseguridad?*, https://www.cisco.com/c/es_mx/products/security/what-is-cybersecurity.html de 4 octubre de 2022, 19:34 hrs.

[63] Universidad Internacional de Valencia, *¿Qué se considera una infraestructura crítica?*, https://www.universidadviu.com/es/actualidad/nuestros-expertos/que-se-considera-una-infraestructura-critica#:~:text=Las%20estructuras%20cr%C3%ADticas%20incluyen%20las,la%20electricidad%20o%20el%20gas de 4 octubre de 2022, 19:42 hrs.

23. *Hacker*: Aquella persona que programa de manera entusiasta y aprende a detalle los sistemas de cómputo. En efecto, un hacker es una persona que tiene profundos conocimientos en informática, es decir, incursiona a detalle los sistemas operativos, la programación, arquitectura de computadoras, sistemas de comunicación de datos, entre otros. Su objetivo principal es conocer y demostrar que conoce… Muchos *hackers* penetran sistemas informáticos sin que sus propietarios o administradores tengan conocimiento de ello, eso justamente los hace caer en la ilegalidad y, además, una vez realizada su fechoría, la información obtenida puede ser empleada para cometer actos criminales[64].

[64] Instituto de Ingeniería UNAM, *Hackers*, http://www.ii.unam.mx/es-mx/AlmacenDigital/CapsulasTI/Paginas/hackers.aspx de 4 octubre de 2022, 19:54 hrs.

# CAPÍTULO II. REDES SOCIALES Y CIBERSEGURIDAD

## 2.1 LA IRRUPCIÓN DE LAS REDES SOCIALES FACEBOOK, TWITTER, INSTAGRAM, TELEGRAM, TINDER

Para la RAE una red social es una "Plataforma digital de comunicación global que pone en contacto a gran número de usuarios"[65]. Mientras que para *Oxford Languages* es una "Página web en la que los internautas intercambian información personal y contenidos multimedia de modo que crean una comunidad de amigos virtual e interactiva"[66].

Si bien se coincide con ambas definiciones, se estima que la definición que aporta la RAE es más amplia al hablar de plataforma digital pues dentro de ésta se encuentra la página web de la que se refiere la definición de *Oxford Languages*.

Para los efectos de este trabajo la segunda definición es mucho más acorde a este presente trabajo puesto que las redes que hoy en día se conocen no son más que páginas *web*, o sea, un sistema de información digitalizada que puede contener desde escritos hasta contenido multimedia como imágenes, videos, *gifs*, etc.

Así para ingresar a dichas páginas se necesita su dirección web, lo que se llama *World Wide Web* (www), que junto con el *HTTPS* (*HyperText Transfer Protocol Secure*) son los enlaces de la página web. Por ejemplo, para ingresar a cualquier red social que se desee desde un buscador web basta con poner en la barra de búsqueda la red deseada, e inmediatamente desplegará la página web de la red social que se buscó, por ejemplo: *https://www.facebook.com* que es la página oficial de *Facebook*, es fácil de encontrar porque está indexada.

Ahora bien, qué pasa cuando se ingresa a una página denominada *http://www.facebok.com*. Es de suma importancia observar que no cuenta en primer

[65] Real Academia Española, https://dle.rae.es/red de 25 junio de 2021, 17:56 hrs.
[66] Oxford Languages, https://www.lexico.com/es/definicion/red_social de 25 junio de 2021, 18:06 hrs.

lugar con la “s” en el *http*, como se aprecia en el primer enlace, por demás le falta una “o” a éste, lo que implica la posibilidad de que se trate de un probable delito informático, el cual se abordará más adelante, bajo el rubro *phishing* y *pharming*.

En ese sentido, la irrupción nació desde el surgimiento de las grandes redes sociales como *Facebook, Twitter, Instagram, YouTube*, etc., cuya continuación se advierte en las “modas” que surgen constantemente, impulsadas aún más por la diversa de *Tik tok* y la cuarentena que digitalizó en su totalidad las relaciones en el orden mundial.

A pesar de que redes sociales como *Myspace*, *Hi5* o el tan aclamado *Metroflog* que fue popular en Latinoamérica se hayan desempeñado desde mucho antes que las redes antes mencionadas no causaron un gran revuelo como lo fue la salida de *Facebook* y un año después en 2005 con la salida de *YouTube* que redes sociales como *Myspace*, *Hi5*, *Metroflog*, *Ares*, poco a poco sus usuarios fueron emigrando a lo que hoy en día es el imperio de *Facebook* y *YouTube*; llegando después *Twitter* en 2006, *WhatsApp* entre 2009 y 2010, *Instagram* entre 2010 y 2012, y actualmente, como se mencionó, la muy famosa aplicación *Tik tok* que desde el 2017 se lanzó internacionalmente[67].

## 2.2. EL ESQUEMA ICEBERG. SURFACE WEB, DEEP WEB, DARK WEB Y DARKNET

El esquema *iceberg* es el más utilizado para entender cómo se dividen los contenidos que podemos encontrar en el ciberespacio y esto es muy importante para la aproximación conceptual del delito informático.

Para tales efectos, primero deben definirse los conceptos de *Surface web*, *Deep web*, *Dark web* y *Darknet,* ya que dependiendo del nivel en el que se encuentre se pueden configurar diversidad de delitos.

[67] De la Hera, Cristina, *Historia de las redes sociales: cómo nacieron y cuál fue su evolución*, 2022, https://marketing4ecommerce.net/historia-de-las-redes-sociales-evolucion/ de 25 junio de 2021, 19:00 hrs.

1. *Surface web*: conocida como web superficial, es aquella en la que todo internauta tiene acceso a través de cualquier motor de búsqueda. Se compone de toda página indexada, por ende, contiene todas las redes populares que conocemos, como *Facebook*, *Twitter*, *Tik tok*, *Instagram*, *WhatsApp*, etc.

2. *Deep web*: es aquella que genera mucha desinformación en cuanto al contenido que se puede encontrar, ya que los medios de comunicación dividen el contenido que se puede encontrar en el ciberespacio solamente en *Surface* y *Deep web*, omitiendo la *Dark web* y *Darknet*. Esta red profunda es considerada un lugar sin ética en la que se encontrar toda clase de delitos, aunque tal percepción que se tiene sobre esta *web* es totalmente errónea. La *Deep web,* fue definida por *BrightPlanet*[68] de la siguiente manera: "La web profunda es cualquier cosa que un buscador no puede encontrar"[69].

   En dicha definición se puede entender que es todo aquello que se encuentra privado o a lo cual no se puede acceder mediante un navegador común.

   Definida la *Deep web* se pueden citar como ejemplos: los *paywalls*, cuentas de *Gmail*, *Mega*, o todo aquello que no se encuentre indexado para no ser encontrados por un buscador común.

3. *Dark web*: ésta es similar a la *Deep web* -de ahí que exista confusión- ya que también contiene contenido oculto, con la diferencia de que aquí el contenido es en su mayoría ilegal, por ende, no se encuentran indexados en los buscadores comunes. Además, para entrar a esta web se necesitan de buscadores especiales como *Tor* ya que tiene dominios propios.

---

[68] Empresa encargada sobre el proceso de recopilación web.

[69] *"The Deep web is anything that a search engine can´t find",* Véase. BrightPlanet, *Clearing up confusion – Deep web vs Dark web,* 2014, https://brightplanet.com/2014/03/27/clearing-confusion-deep-web-vs-dark-web/ de 1 julio de 2021, 13:45 hrs .

4. *Darknet*: no es más que una parte de la *Dark web* y su contenido son páginas privadas a las que sólo es posible acceder mediante links directos.

Otra manera de ejemplificar este tipo de *webs* es con el cielo y la ciudad. El cielo sería la *Surface web* porque es aquello que está a la vista de todos y todas; la ciudad es la *Deep web* y dentro de aquélla se encuentran los barrios peligrosos que propiamente sería la *Dark web*, dentro de los barrios peligrosos se encuentran las casas, a las cuales, para poder entrar a ellas se necesitan programas, buscadores especiales, *links*, etc, dichas casas corresponden con la *Darknet*.

El problema en la actualidad no es adentrarse en la *Darkweb* y *Darknet* propiamente, sino que la web superficial se está plagando de conductas ilegales. Grupos privados de *Facebook*, *WhatsApp*, *Telegram*, e inclusive de manera pública en *Twitter*, alojan contenido totalmente ilegal que va desde sicariato para cometer homicidios, feminicidios, hasta tráfico de personas -disfrazado de sitios para citas- y pornografía infantil -en especial este último punto-.

Es de común acuerdo saber que los delitos informáticos más graves pasaron de encontrarse en lugares tan inaccesibles como la *Darkweb* y *Darknet* para encontrarse hoy en día en redes tan comunes como las de la *Surface web.*

## 2.3. LA FUNCIÓN DE TOR, IP Y VPN

Este tema es fundamental para entender que en el ciberespacio es fácil ocultarse si se tienen conocimientos básicos de informática y eso hace más complicada la labor de la policía informática.

Tanto en el *meatspace*[70], así como en el *cyberspace*[71] si se pretende delinquir el primer paso es ocultar la identidad; esto debido a que la vida en internet

[70] El *meatspace* es el mundo físico en contraposición con el *cyberspace*.
[71] El *Cyberspace* es el mundo virtual donde se desenvuelven las personas dentro de las redes sociales, metaverso o cualquier otra aplicación.

no es privada, sino que en su mayoría es pública. Desde el momento en que se realiza una búsqueda en internet ya se puede localizar a quién la realizó y saber lo que se solicita en las búsquedas.

Los dispositivos se identifican a través de una *IP* (*Internet Protocol*), para *Kaspersky* la *IP* significa "una dirección única que identifica a un dispositivo en internet o en una red local. En esencia las direcciones *IP* son el identificador que permite el envío de información entre dispositivos en una red"[72].

La *IP* autoriza el contacto entre dos o más sistemas electrónicos, para identificar un dispositivo en una red, saber qué información está solicitando y desde dónde lo está haciendo. También cabe mencionar que hay dos clases de *IP*:

1. Privada: refiere aquella con la que cada uno de los dispositivos cuenta y con la que se conecta a nuestro *Router,* y;
2. Pública: relativa a la que cuenta nuestro módem y la cual logra la conexión a internet, es la *IP* que da la cara al exterior en nuestras búsquedas por internet.

Por lo anterior, quien desee delinquir en el ciberespacio tendrá antes que todo configurar sus dispositivos electrónicos para que su *IP* no sea descubierta, con el fin de que no sea localizable, a través de una *VPN* (*Virtual Private Network)*. En este caso, interesan las *VPN* de túneles de datos por ser una "conexión encriptada entre su equipo o dispositivo móvil y la internet en general"[73]. De dicha definición se puede desprender que su navegación es totalmente segura, así evitando la intromisión de nuestros proveedores de servicios de internet, e inclusive del propio gobierno, por demás oculta la *IP* a través del servidor al cual nos conectamos.

[72] Kaspersky, *Qué es una dirección IP: definición y explicación*, 2021, https://www.kaspersky.es/resource-center/definitions/what-is-an-ip-address de 3 julio de 2021, 09:02 hrs.

[73] ExpressVPN, *¿Qué es un túnel VPN?*, 2021, https://www.expressvpn.com/es/what-is-vpn/vpn-tunnel 4 de julio de 2021, 14:34 hrs.

Para mayor precisión, el ejemplo de una conexión a internet básica donde participa 1. El dispositivo, 2. El módem con el *ISP* (*Internet Service Provider*)[74] y 3. Servidores de internet.

Así el dispositivo (*IP* privada) al pretender entrar a *Google* envía una solicitud al módem y de éste al *ISP* (*IP* pública) donde el servidor de internet envía la solicitud al internet propiamente, quedando de manera pública la *IP*, así sabiendo desde dónde se conectó una persona y lo solicitado en su búsqueda, la información queda a disposición de quienes tienen los conocimientos técnicos suficientes; sin embargo, con una *VPN* túnel, se incorpora un cuarto elemento que es el servidor de internet que se elige al conectar con la *VPN*, quedando de la siguiente forma: 1. Dispositivo con *VPN*, 2. Módem e *ISP*, 3. Servidor *VPN* del país que se haya elegido y 4. Internet; siendo que la información es encriptada y estableciendo la *IP* del servidor al que se conecta.

## 2.4. CIBERSEGURIDAD

### 2.4.1 USO DE KALI LINUX Y SOFTWARES UTILIZADOS PARA LOS DELITOS INFORMÁTICOS

*Kali Linux* es un *software distro*[75] diseñado principalmente para cuestiones de seguridad informática, como por ejemplo las auditorías; si bien es cierto que ello no implica que los usuarios sean todos delincuentes informáticos, sí puede ser empleado por éstos; dicho software, es descrito en el libro oficial "*Kali Linux revealed*" de la siguiente manera: "El término *linux* es a menudo usado para referirse a todo el sistema operativo, pero en realidad, *linux* es el núcleo del sistema

[74] El *Internet Service Provider* o proveedor de servicios de internet es una empresa que brinda servicios de internet a sus clientes.

[75] "Una distribución o distro de Linux no es más que una versión personalizada del sistema operativo original, el kernel o núcleo de Linux", Pascual Estapé, Juan Antonio, *Qué es una distribución Linux, en qué se diferencian y cómo elegir una*, 2017, https://computerhoy.com/noticias/software/que-es-distribucion-linux-que-diferencian-como-elegir-54784 de 20 febrero de 2022, 15:23 hrs.

operativo…"[76], por ende, *Kali linux* no es un sistema operativo como *Windows* o *MAC*, sino más bien una distribución de *software* del sistema operativo *GNU/Linux* basada en el núcleo *Linux*.

Así, *Kali Linux* posee una gran variedad de programas entre los que destacan:

1. *Armitage*: "Es una herramienta y colaboración en equipo que permite el uso de scripts para *Metasploit* que permite visualizar objetivos, recomendar *exploits…*"[77].
2. *Metasploit*: "Es un proyecto de código abierto que nos ayuda a investigar las vulnerabilidades de seguridad… es una herramienta muy completa que tiene muchísimos *exploits*"[78].
3. *BeEF*: "Es la abreviatura de *The Browser Exploitation Framework*. Es una herramienta de pruebas de penetración que se encuentra en el navegador web"[79]
4. *Wireshark*: "Es el analizador de protocolos de red más importante y utilizado del mundo"[80].
5. *John the Ripper*: "Es una utilidad *open source* para auditar y recuperar contraseñas, fue creada por *Solar designer* y podría decirles que es una de las herramientas para romper contraseñas de más alto desempeño y flexibles que existe en la actualidad"[81].

[76] "*The term linux is often used to refer to the entire operating system, but in reality, linux is the operating system kernel…*" Hertzog, Raphaël et al., *Kali Linux Revealed. Mastering the Penetration Testing Distribution*, 2021, https://kali.training/downloads/Kali-Linux-Revealed-2021-edition.pdf de 7 julio de 2021, 16:40 hrs.

[77] Parra, Edgar, *Manual de Armitage en español*, 2014, https://www.dragonjar.org/manual-de-armitage-en-espanol.xhtml de 8 julio de 2021, 13:23 hrs.

[78] Rizaldos, Héctor, *Qué es metasploit framework*, 2018, https://openwebinars.net/blog/que-es-metasploit/ de 8 julio de 2021, 13:45 hrs.

[79]Martínez, Raúl, *Ataques al navegador del usuario usando BEEF*, 2016, https://noticiasseguridad.com/hacking-incidentes/ataques-al-navegador-del-usuario-usando-beef/ de 8 julio de 2021, 14:25 hrs .

[80] Wireshark, *About Wireshark*, 2021, https://www.wireshark.org/ de 8 julio de 2021, 14:37 hrs.

[81] Daza, Santiago, *¿Qué es John the Ripper?*, 2021, https://behacker.pro/que-es-john-the-ripper/ de 8 julio de 2021, 14:45 hrs.

En el caso de *Armitage* y *Metasploit*, son herramientas necesarias para tener el control de un dispositivo a través de *exploits* y *payloads,* el primero por ser una vulnerabilidad, en tanto que el segundo es la carga que ejecuta.

Una manera de ejemplificar lo anterior es lo que sucede cuando se intenta el hackeo a un dispositivo de nuestra red, buscando un *exploit* dependiendo del dispositivo, por ejemplo, un *reverse_tcp*, crea un archivo infectado que atrae la atención de la víctima en este caso dinerogratis.exe para ser enviado al dispositivo del cual se quiere tener el control, justo en este paso se hará uso de la ingeniería social[82] para lograr que la falsa aplicación sea descargada y abierta por el usuario que se pretende afectar. Una vez infectado el dispositivo del usuario se puede tener acceso a todos los comandos que brinda *Metasploit* que van desde un simple registro de llamadas hasta capturar imágenes de la cámara del dispositivo -he ahí la decisión de tapar las cámaras de los dispositivos-.

Otro caso que se suscita es el propio uso de las famosas redes sociales, videojuegos y toda aplicación que pida acceso al dispositivo. Por esto, es importante revisar de dónde provienen las aplicaciones, quién las crea y sobre todo ver sus reseñas, porque incluso en los lugares que parecieran más seguros, como en la tienda de aplicaciones del teléfono móvil, abundan aplicaciones maliciosas con el único fin de obtener todo aquello con lo que se pueden lucrar y que se publicitan como verdaderas a través de la ingeniera social. Casos como el de aquellas aplicaciones que prometen préstamos, créditos ilimitados y que al final sólo sirven para obtener datos de las personas que las descargan y utilizan para poder extorsionarlas[83].

[82] La ingeniería social es un conjunto de técnicas para la obtención de datos confidenciales mediante el engaño.

[83] Ante estas situaciones es estrictamente necesario revisar cuidadosamente toda aplicación que se descargue ya que los delincuentes informáticos cada vez incursionan más en supuestas aplicaciones que parecieran legitimas, pero no lo son, inclusive la Policía Cibernética de la Secretaría de Seguridad Ciudadana de la Ciudad de México en su comunicado 2452 identificó al menos 80 aplicaciones fraudulentas. El *modus operandi* se da a través del acceso que se da a las aplicaciones para tener datos relevantes de la víctima y después enviar amenazas para el cobro de préstamos que nunca existieron. Véase. Secretaría de Seguridad Ciudadana, *2452: La Policía Cibernética de la SSC informa sobre los riesgos de descargar y utilizar aplicaciones de préstamos a través de la red pública de internet*, 2021, https://www.ssc.cdmx.gob.mx/comunicacion/nota/2452-la-policia-cibernetica-de-la-ssc-informa-sobre-los-riesgos-de-descargar-y-utilizar-aplicaciones-de-prestamos-traves-de-la-red-publica-de-internet de 22 febrero de 2022, 19:03 hrs.

En el caso de *BeEF* que como se leyó con anterioridad es una herramienta centrada en el navegador web, donde de nuevo se hará uso de la ingeniería social, programa que se encuentra anclado al tema de *phishing* y *pharming*, donde el primero es el anzuelo para hacer que la víctima caiga en el fraude, y el segundo es la recolección de los datos que introdujo ésta.

Entre las funciones principales de la herramienta -*BeEF*- está solicitar credenciales para que sean copias casi idénticas a la web que se desea, por lo general sesiones de *Facebook*, *Gmail*, *Twitter*, etc; otra función es la creación de links modificados y falsos, es por eso por lo que es importante verificar cuando un *enlace* es totalmente seguro o inseguro porque de esto también depende la seguridad del dispositivo.

En síntesis, no siempre el uso de *Kali linux* y los programas que contiene son los adecuados, pues si bien *Kali linux* fue creado para tareas éticas y con fines de ciberseguridad y auditoría, teniendo como consecuencia los *hackers* conocidos como “de sombrero blanco” quienes pueden ser los propios empleados de una empresa, para salvaguardar los dispositivos de ésta, así como los diversos *“*de sombrero negro o gris” quienes harán uso de dichas herramientas para obtener beneficios.

# CAPÍTULO III TEORÍA DE LA LEY PENAL Y DEL DELITO ENFOCADA AL ÁMBITO INFORMÁTICO

Una vez analizado el capítulo 1 y 2 de este trabajo donde se partió de las bases de la electrónica e informática entendiendo de manera sucinta cómo el *meatspace* dejo de ser el centro de esta vida para partir al ciberespacio lo cual da como resultado una necesaria intervención del derecho penal a nuestras relaciones ya no solo físicas sino también informáticas, o sea, digitalizadas. En nuestra actualidad el derecho penal ha evolucionado al hablar de *compliance penal* y responsabilidad penal informática.

## 3.1. ASPECTOS RELACIONADOS CON LA TEORÍA DE LA LEY PENAL

La globalización ha hecho que la sociedad pase a una dualidad -física y cibernética- creando desafíos para el derecho penal de cualquier nación no solo la nuestra. Físicamente nos podemos encontrar en México, pero dentro del ciberespacio nuestra conducta se verá reflejada en cualquier otra parte del mundo.

Por ejemplo: El hombre que desde un país europeo tiene contacto por vía chat con un menor de edad el cual vive en el continente americano, mediante el engaño el hombre europeo logra que el chico le envié fotos y videos de carácter sexual. Una vez obtenido el material decide subirlo a una página pederasta cuyos miembros son alrededor de mil personas.

Esto trae grandes problemas de investigación al derecho penal al haber muchos países envueltos, ¿cuál país debe investigar?, mucho peor, el resultado que ocasiona la descarga y difusión masiva de los contenidos que difunden por todo el internet[84].

[84] El tema de la distribución de contenidos que constituyen delitos es relevante ya que el derecho al olvido como derecho humano por el momento es solo una utopía debido a las descargas, distribuciones y subidas que se dan por el ciberespacio que hacen que la tarea de eliminar en su totalidad contenidos sea imposible con nuestra tecnología por el momento así afectando el derecho al olvido de la víctima y la dignidad de sus familiares.

Este ejemplo es una muestra de la teoría de la ley penal en su vertiente de validez -en especial espacial-, así como el lugar y el tiempo de comisión del delito, pues en el mundo informático no existen barreras y si es que existen la *VPN* en su mayoría de veces pueden derribarlas.

Este último punto es otro tema muy interesante con respecto a las ya crecientes barreras del internet que se vienen promoviendo desde China y su gran Escudo Dorado, que de manera indirecta puede beneficiar o perjudicar al derecho penal para delimitar responsabilidades penales en el ámbito de validez como lugar y comisión del delito[85].

### 3.1.1 ÁMBITOS DE VALIDEZ

En México operan tres ámbitos de validez de la ley penal que son:

1. Validez espacial;
2. Validez temporal y;
3. Validez personal.

La validez espacial es la más importante a estudiar dentro del derecho penal informático ya que es dónde -hablando desde un aspecto de demarcación- debe aplicarse la ley penal en un aspecto amplio, o sea, desde un código penal que contiene a ésta y a la parte de la teoría del delito.

El Dr. Francisco Pavón Vasconcelos establece tres escuelas modernas que estudian al ámbito de validez desde:

a) Territorialidad;
b) Personalidad del derecho y;

[85] La nueva Gran Muralla, del siglo XXI, sirve a otro propósito: 'proteger' a la población china de las influencias negativas de internet y evitar que ciertos tipos de contenido de la red global desconcierten a los usuarios del país asiático…

Como resultado, hoy en día en China existe un sistema desarrollado de censura que se amplía a cada año. Lukyanov, Denis, *El gran hermano te vigila: el impenetrable escudo dorado de china que "protege" su internet de EEUU,* Sputnik, 2019, https://mundo.sputniknews.com/20190523/escudo-dorado-de-china-protege-su-internet-de-eeuu-1087364992.html de 26 febrero de 2022, 12:40 hrs.

c) Objeto social[86].

La escuela de la territorialidad es la aplicación de la ley penal a cada individuo y objeto que se encuentren dentro del territorio de cada país, o "… que las leyes de los países son territoriales y por tanto se aplican, dentro del territorio a todas las personas y las cosas. Aun reconociendo la posibilidad del funcionamiento, en casos excepcionales, de la ley extranjera…"[87].

A manera de ejemplo podemos considerar un caso hipotético: El de Víctor, quien tiene 30 años, con domicilio en Veracruz, es detenido por almacenaje, distribución y venta de pornografía infantil, en la Ciudad de México. Dicho contenido era distribuido por un grupo de *WhatsApp,* del cual ya se tenía una denuncia. El problema radica en que solo se detuvo a un miembro de quienes conforman el grupo. Si los demás integrantes pertenecen al mismo país -que en este caso es México- una solución podría ser que se lleven a cabo acuerdos entre las diferentes entidades federativas para llevar una investigación y una posible extradición inter regional; en este caso hipotético, el mismo joven puede ser juzgado en la CDMX ya que el almacenaje y distribución de material pornográfico infantil es un delito continuo ya que éste se consuma inmediatamente al enviar dicho contenido constitutivo de un delito, pero el resultado y afectación siguen prolongándose a través del internet y con el mismo almacenaje del contenido.

Teniendo como fundamento el artículo 8 -principio de aplicación extraterritorial de la ley penal- en su fracción II del CPCDMX[88]. Ya que el delito que está cometiendo sigue produciendo efectos dentro de la CDMX, caso contrario sería si por ejemplo Víctor, hubiera cometido un homicidio en su entidad de origen, entonces la CDMX, no puede juzgar a Víctor, si no le correspondería al estado de Veracruz porque el homicidio es instantáneo (principio de territorialidad), es así que por acuerdo entre la Ciudad de México y el estado de Veracruz se daría una

[86] Pavón Vasconcelos, Francisco, *Manual de derecho penal mexicano. Parte general*, Ciudad de México, Porrúa, 2016,p. 130.

[87] Ídem.

[88] ARTÍCULO 8 (Principio de aplicación extraterritorial de la ley penal). Este Código se aplicará, asimismo, por los delitos cometidos en alguna entidad federativa, cuando:

I. Produzcan efectos dentro del territorio del Distrito Federal; o

II. Sean permanentes o continuados y se sigan cometiendo en el territorio del Distrito Federal.

extradición inter regional con fundamento en el artículo 119 fracción II constitucional[89].

Un Estado puede apoyarse del principio territorial y extraterritorial cuando los delitos informáticos se cometen en su territorio. Lo complicado es cuando son redes internacionales.

La solución a casos donde la comisión de delitos informáticos es a nivel internacional se dará a través de la cooperación internacional[90]. Estas figuras se encuentran contenidas en el convenio de Budapest, el problema es que nuestro país no se encuentra como Estado parte de dicho convenio.

A pesar de que nuestro país no sea Estado parte del Convenio de Budapest, eso no impide que pueda realizar investigaciones sobre delitos pertenecientes a redes de pederastia, drogas, tráfico de personas, armas, entre otras a nivel internacional, solo se tendrá que solicitar cooperación a instancias de países donde residen los servidores o tengan una mayor capacidad de investigación cibercriminal como en el caso del *FBI* (*Federal Bureau of Investigation*), *CIA* (*Central Intelligence Agency*), *DoS* (*Department of State*), *NSA* (*National Security Agency*), pertenecientes a Estados Unidos de América, mientras que en Australia tenemos a la *ACSC* (*Australian Cyber Security Centre*), en China el *MSS* (*Ministry of State Security*) y obviamente la policía internacional, la misma *Interpol* (*International Criminal Police Organization*) de la cual nuestro país es parte[91].

Entonces se puede identificar que en el ámbito local de un país, los problemas de validez espacial del delito se pueden resolver por principio de territorialidad o extraterritorialidad mediante la aplicación de acuerdos entre entidades federativas y dependiendo de la duración de su delito y sus efectos

[89] Artículo 119… Las entidades federativas están obligadas a entregar sin demora a los imputados o sentenciados, así como a practicar el aseguramiento y entrega de objetos, instrumentos o productos del delito, atendiendo a la autoridad de cualquier otra que los requiera. Estas diligencias se practicarán, con intervención de los respectivos órganos de procuración de justicia, en los términos de los convenios de colaboración que, al efecto, celebren las entidades federativas. Para los mismos fines, las autoridades locales podrán celebrar convenios de colaboración con la fiscalía general de la República…

[90] La cooperación internacional es un elemento esencial del convenio de Budapest, figura contenida del artículo 23 al 35. La cooperación internacional consta de: 1. Extradición; 2. Asistencia mutua; 3. Medidas provisionales; 4. Poderes de investigación y; 5. Red 24/7.

[91] Dichas instituciones son las más importantes para la investigación criminal no solo en el campo físico sino también cibernético.

producidos podamos hablar de una extradición inter regional; mientras que en casos internacionales es mediante cooperación internacional -tema relacionado con el Convenio de Budapest, que se analizará en el siguiente capítulo- y a través del principio extraterritorial dónde se realice la conducta o el hecho o se produzca el resultado, así encuadrando los delitos de resultado formal y material.

En cuanto al ámbito de validez temporal y personal, no hay mayor problema al ser analizados, pues el ámbito temporal no es más que referencia a la abrogación, derogación, ley más benigna e irretroactividad de la ley. En el ámbito personal son cuestiones de inmunidad diplomática y fuero que no tendrían nada de relevancia analizarlos de manera profunda ya que esto aplica a las personas, no se puede hablar de inmunidad diplomática o fuero sobre los dispositivos electrónicos, sino sobre los sujetos activos.

## 3.2. TEORÍA DEL DELITO: ELEMENTOS DEL DELITO DE LA TEORÍA TRIPTÓMICA

Establecido el ámbito de validez en su calidad espacial con el principio de territorialidad, así como el lugar y tiempo de comisión del delito, debemos ahora analizar los elementos constitutivos de delito informático desde un punto de vista de tres elementos positivos que integran al delito[92].

De manera general todo delito es un elemento típico, antijurídico y culpable, o sea, desde un homicidio, hasta un delito informático que para poder configurarse necesitan satisfacer dichos elementos antes mencionados, pero desde un punto particular cada delito tiene su propia definición, pues por simple lógica no es lo mismo un secuestro a un allanamiento de morada y eso es porque cada delito tiene

[92] Es importante dejar en claro que se manejará tanto teoría finalista y funcionalista para el análisis de los tipos informáticos. En cuanto a la teoría finalista se analizará la teoría tripartita del delito y la teoría funcionalista en la autoría mediata por aparatos organizados de poder, aunque no omito en señalar que utilizaré ideas de otros sistemas, debido a que encuadrar a ciertos autores dentro de sistemas penales la mayoría de las veces no es correcto.

sus propias características contenidas dentro de un tipo penal que está relacionado con la tipicidad, es por eso que ésta será el primer elemento a analizar.

El delito informático también tiene su propia definición y sus propias características, el principal problema es que dichos delitos son parte de una responsabilidad penal informática apenas naciente en nuestro país -si es que se puede considerar así pues desde los años 90 ya se empieza a hablar sobre responsabilidad penal informática- al igual que la responsabilidad penal empresarial a través del *compliance* penal, es por eso que definir el delito por parte de la empresa, así como el delito informático pueden presentar aun bastantes deficiencias en sus definiciones y características, en especial el segundo, pues los juristas muy poco saben de informática y los expertos en ésta, muy poco saben de derecho penal, aun así me atreveré a dar una definición de delito informático derivada del entendimiento de los tipos básicos y subordinados.

El Doctor Julio Téllez Valdés, citado por el Dr. Santiago Acurio del Pino; define al delito informático en 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",[93] Nótese como se establece a los dispositivos electrónicos como medio o fin. Así desde 1996 ya se empieza establecer lo que vendría a ser un delito informático y es sorprendente que desde finales de los 90´s se pueda entender que los delitos informáticos en su mayoría de veces son medios comisivos para otro delito, por ejemplo, una extorsión[94].

Jesús Alberto Loredo González, considera como delito informático: "toda acción dolosa que provoca un perjuicio a personas o entidades, sin que necesariamente conlleve un beneficio material para su autor aun cuando no perjudique de forma directa o inmediata a la víctima y en cuya comisión intervienen necesariamente de forma activa dispositivos habitualmente utilizados en las

[93] Acurio del Pino, Santiago, *Delitos informáticos generalidades*, 2016, https://www.oas.org/juridico/spanish/cyb_ecu_delitos_inform.pdf de 5 septiembre de 2021, 12:08 hrs.
[94] Aunque de manera más técnica deben ser entendidos como delitos básicos y subordinados.

actividades informáticas"[95]. Esta definición aporta otra característica que da como resultado los delitos informáticos de mero orgullo -aquellos que no persiguen una finalidad económica, sino solo demostrar sus conocimientos en *hacking*-.

### 3.2.1. TIPICIDAD

La tipicidad es la columna vertebral de la dogmática penal, pues sin ésta no existe el delito, mientras que la antijuridicidad en sus causas de justificación, así como la culpabilidad con su inculpabilidad no son capaces de desaparecer el delito, sino que más bien lo justifican o lo inculpan que no son más que facultades excepcionales que brinda el derecho penal. Así de importante es el primer elemento del delito que además marca un principio de legalidad establecido bajo la siguiente fórmula "*Nullum crimen, nulla poena sine lege*" del gran jurista y filosofo Paul Johann Anselm Von Feuerbach, que después Ernst Von Beling, establece por primera vez en la definición de delito el elemento tipicidad, describiendo al delito de la siguiente manera:

"acto punible es una acción (*Handlung*) conforme a un tipo de acto punible descrito en la ley (*Tatbestandmässige Handlung*), antijuridica (*Rechtswidrige*), culpable (*Schuldhafte)* sujeta a la apropiada sanción penal (*eine einer passeden Strafdrohung unterstellbare Handlung*), que comprende todas las condiciones de la sanción penal (*eine des passeden Strafdrohung unterstellbare Handlung*)".[96]

Además de establecer al tipo por primera vez como elemento del delito, también estableció una teoría del tipo (tipo no es lo mismo que tipicidad), naciendo así el *Tatbestand* o *Leitbild*, *Deliktstypus*, *Tatbestandmässigkeit, Unrechtstypus* y el

[95] Loredo González, Jesús Alberto y Ramírez Granados, Aurelio, *Delitos informáticos: Su clasificación y una visión general de las medidas de acción para combatirlo*, 2013, http://eprints.uanl.mx/3536/1/Delitos_informaticos.pdf de 6 septiembre de 2021, 10:23 hrs.

[96] Franco Guzmán, Ricardo, *Delito e injusto. Formación del concepto de antijuridicidad*, segunda edición, Porrúa, México, 2012, p. 17.

tipo de culpabilidad. Es así como Johann Feuerbach y Ernst Beling, son los máximos exponentes al querer hablar de tipicidad y tipo.

La tipicidad "es la adecuación de la conducta realizada por un sujeto al tipo penal, o sea, el encuadramiento de un comportamiento real a la hipótesis legal"[97]. De manera más corta, sencillamente la tipicidad es el encuadramiento de la conducta al tipo, mientras que el tipo es la descripción que hace el legislador de una conducta constituida bajo un verbo o varios rectores que se plasman en un código penal o leyes especiales.

### 3.2.1.1 ELEMENTOS OBJETIVOS DEL TIPO PENAL

Los elementos objetivos del tipo varían para cada autor, hay quienes consideran más, menos elementos. La Dra. Erika Bardales Lazcano contempla diez elementos objetivos del tipo los cuales son:

a) Sujetos. Que se clasifica en activo y pasivo.
b) Calidad de sujetos. Tanto del activo como del pasivo.
c) Conducta. Que puede ser de acción, omisión o comisión por omisión.
d) Bien jurídico tutelado. Resultando si es personal o supra-personal.
e) Objeto material.
f) Circunstancias. De tiempo, lugar o situación.
g) Medios comisivos. Que puede ser violencia física o violencia moral.
h) Nexo causal.
i) Resultado. Que puede ser formal o material.
j) Imputación objetiva del resultado (atribuibilidad del resultado a la conducta). Mediante la creación de un riesgo no permitido; la concreción del riesgo no permitido en un resultado y que el mismo pertenezca al ámbito protector de la norma[98].

Desde mi perspectiva solo hay seis elementos objetivos del tipo, los cuales son:

[97] Amuchategui Requena, Irma Griselda, *Derecho penal*, cuarta edición, Oxford, México, 2012, p. 63.
[98] Bardales Lazcano, Erika, *Guía para el estudio del sistema penal acusatorio. Nuevo sistema de justicia penal*. Primera reimpresión a la sexta edición, Editorial Flores, México, 2018, pp. 266, 267.

1. Conducta;
2. Sujeto activo y pasivo;
3. Bien jurídico;
4. Medios comisivos;
5. Circunstancias de modo, tiempo, lugar u ocasión y;
6. Objeto material y jurídico.

Al considerar seis elementos es porque propiamente el nexo causal como el resultado y la imputación objetiva del resultado forman parte de la conducta, considerando incorrecto tenerlos como elementos independientes. De igual modo pasa con la calidad en los sujetos, ya que de manera amplia se debe hacer su estudio correspondiente dentro del sujeto activo y pasivo.

### 3.2.1.1.1 CONDUCTA

La conducta es toda acción o inacción humana exteriorizada que puede o no llevar una finalidad.

Derivada de dicha definición se desprende que la conducta es una acción, pero sobre todo una inacción de donde derivan sus divisiones en 1. Omisión simple; y 2. Comisión por omisión.

Desde la informática, no se puede hablar de una conducta por parte del dispositivo propiamente, pues éste solo es el medio comisivo, es como el arma del homicida, acaso, ¿el arma -simboliza violencia- comete una conducta?, por ende, no se puede dar una responsabilidad a un dispositivo electrónico por el resultado que se desarrolló, entonces de manera sencilla la conducta y responsabilidad penal recaen en quienes -sujetos físicos- hacen uso de los dispositivos de manera no correcta, pero tal vez en un futuro esto cambie de manera rotunda al verdaderamente dar una responsabilidad a los dispositivos autónomos o mejor dicho robots que cuenten con una mentalidad y conducta autónoma, porque si no cuentan con estas características tal vez se haga referencia al hombre de atrás de

la autoría mediata, añadiendo a lo mejor un nuevo elemento como el uso de máquinas programables.

Derivado de lo anterior, entonces un delito informático también cabe en las formas derivadas de la conducta, o sea, la omisión simple y la comisión por omisión, por ejemplo en la omisión impropia se puede dar el caso del encargado de la ciberseguridad de una empresa que es omisivo a dar mantenimiento a los dispositivos informáticos que son parte del patrimonio de la empresa, así aprovechando que delincuentes externos puedan aprovechar las vulnerabilidades de los equipos y cometer sabotaje informático, provocando como resultado daño a la propiedad.

Otros elementos objetivos que se incluyen dentro la conducta es propiamente la duración del delito -instantáneo, continuo y continuado-, resultado y nexo causal a través de varias teorías entre las que destaca *Die Lehre der Objektiven Zurechnung* -La teoría de la atribución objetiva-. En el ciberespacio también somos una sociedad de riesgos, así como en el *meatspace* vivimos bajo riesgos y los aceptamos, por igual pasa en el *cyberspace* aceptando y viviendo bajo peligros.

Lo que puede sobresalir en estos últimos elementos es la duración de los delitos informáticos.

La duración instantánea es cuando convergen todos los elementos típicos y en ese momento se da la consumación como la obtención de datos informáticos, ejemplo el *Phishing*, en el instante en que el *phisher* se hace de los datos de la víctima se ha consumado la conducta.

El delito continuo se da de forma instantánea, pero el resultado se prolonga a través del tiempo, ejemplo; la distribución de pornografía infantil, el delito se consuma inmediatamente al enviar dicho contenido constitutivo de delito, pero el resultado y afectación siguen prolongándose a través del internet. Este tipo de duración es un problema desde el ámbito práctico, pues, las autoridades correspondientes qué podrían hacer para que dichos contenidos sean removidos del internet de manera definitiva, además cómo localizar cada dispositivo que tenga almacenado dicho contenido.

Lo anterior suele pasar mucho en las plataformas de contenido pornográfico donde se suele subir demasiado contenido sin consentimiento de las víctimas, lo cual no asegura que muchas personas ya lo hayan descargado y mucho más, ya esté posteado en otros sitios de contenidos similares, así cruzando las fronteras ilimitadas del ciberespacio y haciendo una labor prácticamente imposible de que los delitos informáticos continuos puedan dejar de prolongarse.

El delito continuado por otra parte debe cumplir con ciertos requisitos los cuales son: a) Unidad de propósito delictivo; b) Pluralidad de conductas; c) Identidad de víctima y d) Vulneración de un solo tipo penal[99].

### 3.2.1.1.1.1 CONDUCTAS DELICTIVAS: GROOMING, SEXTING, CYBERBULLYING, PHISHING, PHARMING, CARDING, FAKE NEWS

El *sexting* es un chat de contenido sexual ya sea en texto, vídeos, imágenes o cualquier contenido multimedia de índole sexual que se tiene con otra/s personas, deviene del inglés *sex* que significa sexo y *texting* de textear, o sea, escribir mensajes.

El *sexting* es dual -sí y no es un medio comisivo-. No es un medio comisivo desde el punto de vista jurídico por el hecho de que sólo es un medio, así como quien desea comprar un carro tendrá que ahorrar para poder adquirirlo. El ahorro simplemente es el medio, pero no comisivo porque no representa algún interés para el derecho penal.

El derecho penal no tiene intromisión mediante los medios comisivos en que se pueda sextear con otras personas pues el humano debe disfrutar de su libre desarrollo sexual, el problema deviene cuando el contenido compartido es difundido sin el debido consentimiento de quienes deban otorgarlo, no se haga bajo el consentimiento de las partes o haya desproporcionalidad de edad -persona menor de edad y mayor de edad-.

[99] Jiménez Holguín, Noel Orlando, *Delito instantáneo, permanente y continuado*, 2018, https://www.youtube.com/watch?v=xQp5xi2Q5sE de 3 marzo de 2022, 15:21 hrs.

En el caso de que el contenido sea difundido sin el consentimiento de quien pueda otorgarlo sí representa un medio comisivo y es justo aquí cuando el derecho penal entra en su papel como vigilante de la sana convivencia social, el medio comisivo más común que puede representar al *sexting* es el engaño y por lo general las víctimas suelen ser los menores de edad y adolescentes[100].

El *sexting* no representa un medio comisivo del delito siempre y cuando:

1. Las personas participantes sean mayores de edad;
2. Sea bajo el consentimiento de las partes y;
3. El contenido compartido sea exclusivo para las partes participantes.

Ahora bien, brindando estos tres puntos en contrario *sensu* se pueden actualizar los siguientes delitos; si en el primer punto actúa un mayor de edad con una persona menor de edad o adolescente encuadra su conducta al delito contra intimidad conforme al artículo 179 bis del CPCDMX. Además, el delito de pornografía conforme al artículo 187 párrafo IV del CPCMDX; el punto dos y tres (no haya consentimiento de las partes y no sea exclusivo el contenido) por igual encuadran en los artículos anteriores, así como en el artículo 181 fracción II, 183, 184, 209 y 236 del ya citado código. Así pudiendo comprender que, si no se cumplen los tres puntos brindados con anterioridad, el *sexting* pasa de ser una actividad lícita a una totalmente ilícita pues actualiza los distintos tipos penales como se explicó anteriormente.

En ese mismo sentido, el ciberacoso "es un término que se utiliza para describir cuando un niño o adolescente es molestado, amenazado, acosado,

[100] La Secretaría de Seguridad ciudadana de la CDMX en su comunicado 1894, "invita a sensibilizar a los jóvenes sobre los riesgos de compartir fotos de su cuerpo en redes sociales", Secretaría de Seguridad Ciudadana, *1894: Para evitar que los menores de edad caigan en engaños de sexting, la SSC alerta a la ciudadanía y padres de familia, sobre cuentas apócrifas de personas públicas*, 2020, https://www.ssc.cdmx.gob.mx/comunicacion/nota/1894-para-evitar-que-los-menores-de-edad-caigan-en-enganos-de-sexting-la-ssc-alerta-la-ciudadania-y-padres-de-familia-sobre-cuentas-apocrifas-de-personas-publicas de 23 febrero de 2022, 17:56 hrs.

humillado, avergonzado o abusado por otro niño o adolescente, a través de Internet o cualquier medio de comunicación como teléfonos móviles o *tablets*"[101].

El ciberacoso es de común acuerdo que es algo de índole física y que se ha trasladado al mundo de las redes sociales. El acoso puede verterse en contra de la religión, el físico de las personas, color, sexo, orientación sexual y especialmente el acoso sexual contra las mujeres de manera digital.

Interesante es la investigación de la Licenciada Fernanda Gómez en colaboración con Luchadoras MX sobre su trabajo intitulado "Violencia sexual digital. Un balance de la Ley Olimpia en CDMX", donde se abordan aspectos sobre el tipo de acoso sexual bajo la modalidad digital (artículo 179 BIS) y contra la intimidad sexual (artículo 181 QUINTUS), así como las órdenes de protección en materia penal consistentes en el retiro y bloqueo de contenido sexual privado.

En el primer punto (acoso sexual digital) especifica que constituye un nuevo delito, algo que desde mi perspectiva es clara muestra de un delito subordinado puesto que constituye una agravante y adición de medios digitales al tipo básico de acoso -conocido también como delito medio-. En cuanto al delito contra la intimidad sexual es el claro ejemplo de un delito informático básico pues atenta contra la confidencialidad digital en su división de intimidad sexual, o sea, contenido sexual privado[102].

Las órdenes de protección sobre el bloqueo y retiro de contenido privado de la víctima es un punto tan vital y relevante en el creciente derecho penal informático desde una vista procesal. La misma autora hace conocer los grandes retos que enfrentan las autoridades al momento de retirar contenido privado de una plataforma fundamentando su idea a través de la sección 230 de la *Communications Decency Act* que libera de responsabilidad a los proveedores de servicios tecnológicos[103].

---

[101] Cyberbullying, *¿Qué es el cyberbullying?,* 2016, https://www.gob.mx/ciberbullying/articulos/que-es-el-ciberbullying de 24 febrero de 2022, 09:38 hrs.

[102] Se profundizarán más adelante estos tipos pues son esenciales para el derecho penal informático .

[103] Véase. Gómez, Fernanda y Luchadoras MX, *Violencia sexual digital. Un balance de la Ley Olimpia en CDMX*, 2019, https://luchadoras.mx/un-balance-de-la-ley-olimpia-en-cdmx/ de 14 noviembre de 2022, 18:36 hrs.

De lo anterior, la sección 230, no solo es el fundamento legal bajo el que se protegen grandes empresas de la tecnología, sino también algo que está muy relacionado con las personas en especial referencia a la autoría y participación en cuanto los resultados que se producen por la difusión de contenido multimedia. Hasta el momento es prácticamente imposible eliminar contenidos multimedia privados que hayan sido subidos al internet de manera total. De mucho o muy poco sirve que cierto contenido sea removido de la web si las mismas personas son las que motivan conductas como la descarga y distribución de contenido que en esencia es constitutivo de un delito. Es tarea de todos y todas el erradicar todo contenido multimedia que se haya filtrado en internet para poner un alto a la infinita distribución de materiales privados que afectan a las víctimas de delitos como el ciberacoso y la extorsión.

El ciberacoso no solo se encuentra fundamentado en el tipo 179 BIS y 181 QUINTUS, sino también bajo el tipo de discriminación (artículo 206 CPCMDX), mientras que en el estado de Yucatán se denomina ciberacoso en su artículo 243 bis 12 del código penal, que establece:

"Comete el delito de ciberacoso quien intimide y asedie a cualquier persona, a pesar de su oposición, por medio de las Tecnologías de la Información y Comunicación, tales como redes sociales, mensajería instantánea, correo electrónico o cualquier otro medio digital; mediante el envío de mensajes de texto, videos, impresiones gráficas, sonoras o fotografías…"[104].

Nótese cómo los medios comisivos son los medios digitales y las tecnologías de la información. Es importante recalcar la idea anterior de la que se puede diferenciar con toda claridad del delito de discriminación, ya que éste no exige medios comisivos, es mucho más amplio que el tipo de ciberacoso, pero eso no implica que se pueda en el caso de la Ciudad de México que el ciberacoso -que no se encuentra tipificado como delito subordinado- pueda adecuarse al tipo de discriminación por la simple razón de que el ciberacoso atenta contra el color de piel, nacionalidad, posición económica, características físicas, entre otras razones,

[104] Con amplitud, véase el artículo 243 bis 12 del Código penal de Yucatán.

el cual sólo incitan al odio o la violencia partes fundamentales de la discriminación y que por igual son inherentes al ciberacoso.

En cuanto al *grooming*, puede ser denominarlo engaño pederasta que implica que "un adulto que se pone en contacto con un niño, niña o adolescente con el fin de ganarse poco a poco su confianza para luego involucrarle en una actividad sexual"[105]. Por su parte la página oficial del gobierno de Argentina describe al *grooming* de la siguiente manera:

"El *grooming* es la acción deliberada de un adulto, varón o mujer, de acosar sexualmente a una niña, niño o adolescente a través de un medio digital que permita la interacción entre dos o más personas, como por ejemplo redes sociales, correo electrónico, mensajes de texto, sitios de chat o juegos en línea"[106].

La *Children Porn* o mejor conocida por sus siglas *CP* deriva de varias conductas delictivas como el *grooming*. La pornografía infantil es uno de los comportamientos más perniciosos para los niños y niñas de todo el mundo. Este delito por lo general abundaba en zonas tan recónditas de la *darkweb* y *darknet*, pero que ahora se encuentra en la misma *surface web*, demostrando los mínimos avances en la erradicación de tales conductas.

La pornografía infantil desde el punto de vista jurídico para el caso de la Ciudad de México encuadra en el tipo de pornografía -artículo 187 CPCDMX- que tiene como sujetos pasivos a los menores de 18 años y quienes no puedan comprender el hecho para realizar actos lascivos o sexuales con la finalidad crear contenido multimedia.

Para el Código Penal Federal es curiosa cierta figura contenida en los artículos 209 BIS y TER, pues es el tipo denominado "Pederastia" y que es de carácter físico, puesto que mientras la pornografía es dual -índole informática y

---

[105] Save the Children, *Grooming qué es, cómo detectarlo y prevenirlo,* 2019, https://www.savethechildren.es/actualidad/grooming-que-es-como-detectarlo-y-prevenirlo de 10 agosto de 2021, 11:03 hrs.

[106] Gobierno de Argentina, *Grooming Qué es y cómo prevenirlo*, 2021, https://www.argentina.gob.ar/grooming de 10 agosto de 2021, 11:30 hrs.

física-, la pederastia es solo del orden físico pues se ejecutan actos sexuales contra el menor sin el uso de medios tecnológicos para crear contenido multimedia. La pederastia en la CDMX se actualiza bajo los tipos de violación, abuso y acoso sexuales, cometido a menores de doce años -artículo 181 BIS a 182- y que de cometerse una violación contra un menor y que a la vez sea videograbada se estaría ante un concurso de delitos -violación contra menores y pornografía-.

Respecto al *phishing* y *pharming,* son dos conductas que guardan cierto grado de relación pues ambas tienen la esencia de sustraer datos de la víctima que hace uso de la informática. El *phishing* para Iván Belic "es una de las estafas más antiguas y mejor conocidas de Internet. Podemos definirlo como un tipo de fraude en las telecomunicaciones que emplea trucos de ingeniería social para obtener datos privados de sus víctimas"[107].

El *pharming* por su cuenta es "una combinación de los términos *phishing* y *farming*, es un tipo de cibercrimen muy semejante al *phishing*, en el que el tráfico de un sitio web es manipulado para permitir el robo de información confidencial"[108]. Si el *phishing* puede ser entendido como anzuelo, el *pharming* como recolección. Éste se encarga de atacar los principios de básicos de internet a través del *DNS* (*Domain Name System*)[109], pues sin un dominio no se podría buscar de forma indexada, por ejemplo *Google.com*, sino sólo se podría mediante su dirección *IP*.

Claro ejemplo es cuando se realiza la búsqueda de *Facebook* en donde en vez de que aparezca la *IP* verdadera de éste, se dirige a la *IP* del delincuente informático así llevando a la víctima a una web fraudulenta donde el sujeto pasivo

---

[107] Belcic, Iván, *Guía esencial del phishing: cómo funciona y cómo defenderse,* Avast, 2021, https://www.avast.com/es-es/c-phishing de 13 agosto de 2021, 16:12 hrs.

[108] Kaspersky, *¿Qué es el pharming y cómo evitarlo?*, 2021, https://latam.kaspersky.com/resource-center/definitions/pharming de 13 agosto de 2021, 16:20 hrs.

[109] "El **DNS** *(Domain Name System, Sistema de Nombres de Dominio)* es un conjunto de protocolos y servicios que permite a los usuarios utilizar nombres en vez de tener que recordar direcciones IP numéricas. Ésta es ciertamente la función más conocida de los protocolos DNS: la asignación de nombres a direcciones IP. Por ejemplo, si la dirección IP de www.uja.es es **150.214.170.139**, la mayoría de la gente llega a este equipo especificando www.uja.es y no la dirección IP. Además de ser más fácil de recordar, el nombre es más fiable. La dirección numérica podría cambiar por muchas razones, sin que tenga que cambiar el nombre." Véase. Universidad de Jaén, *Nombres de dominio (DNS),* https://www.ujaen.es/servicios/sinformatica/catalogo-de-servicios-tic/nombres-de-dominio-dns de 25 febrero de 2022, 18:43 hrs.

pensará que es el sitio web verdadero de *Facebook*, introduciendo sus datos, los cuales son recolectados por el delincuente para su beneficio, todo esto se logra instalando un virus, cambiando o infectando los *DNS*.

El phishing y el pharming, constituyen conductas que encuadran dentro del tipo de Fraude -artículo 230 CPCDMX-[110], pues se aprovechan del error en que la víctima se haya, por ejemplo, el caso hipotético anterior del *pharming* y en el *phishing* puede ejemplificarse con enviar un correo electrónico falso aparentando ser un ejecutivo del banco para obtener datos de la víctima.

El *carding* consiste en ser el medio por el cual se detectan los cargos no reconocidos en sus tarjetas de crédito y débito. Ésta es una forma de estafas online, misma que consiste en acceder ilegalmente a todos los datos de una tarjeta bancaria"[111]. Esta conducta se ejecuta mediante el uso de *softwares* que a través de combinaciones generan los datos bancarios de las tarjetas para ser utilizadas para el pago de planes de *Netflix, Spotify* o cualquier otro servicio que requiera suscripción hasta para comprar cosas muy valiosas como joyas.

El *carding* puede hacerse mediante *phishing*, *pharming*, o los tan conocidos *bins* que son los seis primeros números de una tarjeta de ahí su nombre como *Bank Identification Number*, o sea, número de identificación bancaria, los cuáles definen el banco y tipo de tarjeta. Los *bins* sirven para generar tarjetas de banco falsas con las cuales se pueden hacer compras en línea, existan o no tales tarjetas. El uso más común es engañar a una página y hacerle creer que en verdad se introdujo una tarjeta para comprar o hacer el pago de algo todo esto porque los bancos tienen *bins* no asignados a algún cliente, es aquí donde el binero mediante el uso de programas genera *bins* a través de un método de ensayo y error, o bien, comprar los datos a terceros.

También se debe de contar con una fecha de expiración y un CVV, o sea, un número de seguridad que se le asigna a la tarjeta que consta por lo general de tres

[110] También pueden encuadrar en el artículo 432 de la Ley General de Títulos y Operaciones de Crédito, que será analizado a continuación con la conducta del *carding.*

[111] Ahorra seguros, *¿Cómo prevenir el carding al contratar un seguro de auto?,* 2020, https://ahorraseguros.mx/blog/que-es-carding/ de 25 febrero de 2022, 19:00 hrs.

números para que sus compras online sean más seguras, utilizando programas como *Namso ccgen v5*.

El *carding*, puede encuadrar a la perfección en el tipo penal contenido en el artículo 432 de la Ley General de Títulos y Operaciones de Crédito al hacer un uso no facultado y sin causa legítima de una tarjeta de crédito o en general cualquier instrumento de pago para la adquisición de bienes y servicios.

Para cerrar con el tema de conductas ciber delictivas se abordará un tema bastante en debate que es la libertad de prensa contra la censura. Las *fake news* (falsas noticias) traen como consecuencia la desinformación, pero sobre todo la alarma social.

El Estado de Veracruz de Ignacio de la Llave, respecto a su código penal tiene a las noticias falsas como un delito en el siguiente artículo:

CAPÍTULO III

Perturbación del Orden Público.

> Artículo 373. Al que, con la intención de perturbar el orden público, dé a conocer falsamente, a sabiendas de ello y por cualquier medio, la existencia de aparatos explosivos u otros que puedan causar el mismo efecto; de ataques con armas de fuego; o de sustancias químicas, biológicas o tóxicas que puedan causar daño a la salud, se le impondrá prisión de uno a cuatro años y multa de quinientos a mil días de salario, atendiendo a la alarma o perturbación del orden efectivamente producido[112].

El tipo penal propiamente es perturbación del orden público, y se relaciona con las fake news pues cuenta con el elemento subjetivo especifico "A sabiendas" para que no se vuelva a repetir el caso de cierta mujer que por twittear información falsa llevo un proceso por el delito de terrorismo… al final se reformo dicho artículo que se limita a delitos dolosos.

[112] Artículo 373, Código Penal para el Estado de Veracruz de Ignacio de la Llave, México, 2021, https://www.legisver.gob.mx/leyes/LeyesPDF/CPENAL15112021.pdf de 20 agosto de 2021, 15:06 hrs.

### 3.2.1.1.2. SUJETO ACTIVO Y PASIVO

El sujeto activo "es la persona individual con capacidad penal que realiza la conducta típica"[113] mientras que el sujeto pasivo "es el titular del interés jurídico lesionado o puesto en peligro"[114]. De manera sencilla el primero es quien comete la conducta delictiva considerada como delito y el segundo es quien resiente dicha conducta.

En el ámbito informático cualquiera puede ser sujeto activo de un delito informático, no se necesita tener una calidad específica, hasta un *script kiddie* puede delinquir. En el caso de los sujetos pasivos por igual cualquiera puede ser víctima de estos delitos -regla general, aunque hay sus excepciones en ciertos tipos penales-.

#### 3.2.1.1.2.1 SUJETOS ACTIVOS. DELINCUENTES INFORMÁTICOS EXTERNOS E INTERNOS

Quien comete el delito de homicidio se le denomina homicida, al que comete feminicidio se le llama feminicida, entre otros; en el mundo informático se le denomina al delincuente de manera general como ciberdelincuente o delincuente informático.

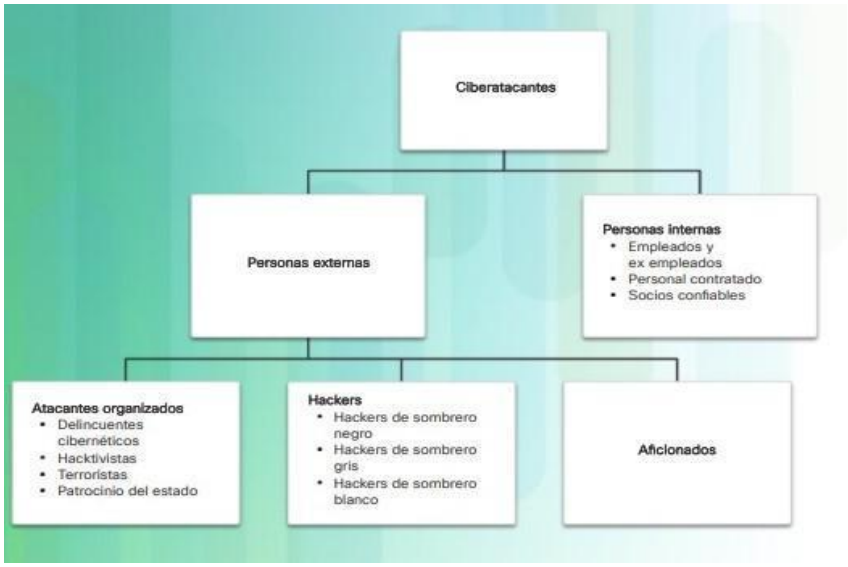
Un delincuente informático la mayoría de veces tendrá grandes conocimientos de la informática y programación, por ende, no cualquiera puede ser sujeto activo de estos delitos, con esto no se está tratando de explicar que se tratan de delitos de sujeto activo exclusivo, ya que por lo general la mayoría de delitos informáticos son de sujeto común[115], sino que simplemente para crear una página

[113] Peña Gonzáles, Oscar y Almanza Altamirano, Frank, *Teoría del delito: Manual práctico para su aplicación en la teoría del caso,* Perú, Asociación Peruana de Ciencias Jurídicas y Conciliación, 2010, p.71.
[114] Ibidem, p. 74.
[115] Dentro del estudio de la tipicidad se encuentra como elemento objetivo del tipo el sujeto pasivo y activo del delito, en el caso del sujeto activo hay que saber que en su análisis se encuentra la calidad ya sea común o exclusiva, en el primer supuesto cualquiera puede cometer el delito y en el segundo solo quien detenta una calidad específica.

fraudulenta, virus, *exploits* y demás métodos para aprovecharse de la víctima es vital tener un poco de conocimiento en el área de la informática, programación.

Cisco[116], divide a los ciber atacantes en dos ramas principales: 1. Personas externas y 2. Personas internas, dentro de la primera rama se subdividen los 1.1. Atacantes organizados -delincuentes cibernéticos, hacktivistas, terroristas y patrocinados por el Estado-; 1.2. Hackers -sombrero negro, sombrero gris y blanco- y 1.3. Aficionados -script kiddies-. En la segunda rama encontramos, 2.1. Personas internas -empleados, exempleados, personal contratado y socios confiables-. Véase figura 1.

***Figura 1.*** *Tipos de ciber atacantes[117].*




De tal suerte, las personas externas son todas aquellas ajenas a la empresa, mientras que las personas internas son una clara referencia a la empresa -trabajadores, trabajadoras, proveedores, extrabajadores, extrabajadoras, socios- y

[116] CISCO es empresa dedicada a la venta y producción de equipos de telecomunicaciones con sede en San Francisco, Estados Unidos de América. Además, cuenta con programas educativos para la formación y certificación de profesionales.

[117] Nota. Se puede observar los tipos de delincuentes informáticos que antes fueron escritos y cómo de manera general se les denomina Ciber atacantes y de ahí nacen sus divisiones. Fuente: CISCO, disponible en: https://contenthub.netacad.com/legacy/I2CS/2.1/es/index.html#1.3.1.2 . Fecha de consulta: 30 de Julio de 2021, hora: 13:56 hrs.

que por cuestiones de su trabajo manejan datos confidenciales, sistemas informáticos y todo lo relacionado a la ciberseguridad de la empresa. Otra característica que ofrece Cisco es la división de las personas externas en cuanto al cuadro de los atacantes organizados y que da lugar a la delincuencia organizada.

> El *hacktivismo* es la combinación única de las palabras «piratería» y «activismo», y ha surgido a medida que las personas usan Internet para manifestarse por causas políticas o sociales. Esas personas a veces se llaman guerreros de la justicia social.
>
> Es el acto de hacer mal uso de un sistema informático o red por una razón motivada social o políticamente. Las personas que realizan *hacktivismo* se conocen como hacktivistas[118].

Los terroristas y patrocinados por el Estado, de algún modo pueden ir conjuntamente ya que todo Estado que patrocine a un grupo de ciber atacantes para sabotear a otro estado extranjero se le puede considerar un terrorista patrocinado por el Estado, naciendo así lo que se conoce como ciberguerra. En este punto podemos adentrarnos al virus *Stuxnet* que se puede resumir como el primer virus espía *SCADA*[119] que permite controlar, o sea, modificar, supervisar procesos a distancia; donde una de las principales víctimas del ataque era Irán con sus infraestructuras de alto valor como plantas nucleares y que tiene como posibles autores intelectuales a los Estados Unidos de América e Israel, para sabotear los programas nucleares de Irán, según fuentes *de Kaspersky*[120].

El segundo cuadro contiene los tipos de hackers que existen dentro del estudio de la ciberseguridad. El primer tipo de *hacker* es el de sombrero negro, el *hacker* de sombrero negro puede ser definido como "delincuentes que se introducen en redes informáticas para llevar a cabo algún acto malicioso. Algunos también se dedican a robar contraseñas, números de tarjetas de crédito y otras clases de

[118] Ciberseguridad, *Hacktivismo*, https://ciberseguridad.com/amenzas/hacktivismo/ de 14 de noviembre de 2022, 19:46 hrs.
[119] "SCADA" es el acrónimo de *Supervisory Control and Data Acquisition* (supervisión, control y adquisición de datos), término que describe las funciones básicas de un sistema SCADA. Las empresas usan los sistemas SCADA para controlar los equipos de sus centros y recopilar y registrar datos de sus operaciones". Véase. COPADATA, *¿Qué es SCADA?,* https://www.copadata.com/es/productos/zenon-software-platform/visualizacion-control/que esscada/#:~:text=SCADA%20es%20el%20acr%C3%B3nimo%20de,registrar%20datos%20de%20sus%20operaciones. de 22 febrero de 2022, 17:38 hrs.
[120] Kaspersky, *Stuxnet: Los orígenes*, 2014, https://latam.kaspersky.com/blog/stuxnet-los-origenes/4553/ de 22 febrero 2022, 18:00 hrs.

información confidencial, a tener sistemas de rehén o a propagar malware diseñado para borrar información"[121]. Una explicación un tanto casuística y que de manera simple se puede definir a un *hacker* de sombrero negro como aquel ciber atacante que de manera ilegal se introduce en dispositivos informáticos sean o no críticos ajenos o sin la necesidad de acceder a éstos con el propósito de obtener un lucro en perjuicio del sujeto afectado.

El segundo tipo es el hacker de sombrero gris y son aquellos "que no utilizan sus habilidades para obtener beneficios, pero que no operan con total integridad"[122].

Esta definición es idónea para describir a esta clase de delincuentes por el simple hecho de que igual que el sombrero negro, el sombrero gris se introduce a los dispositivos informáticos para descubrir vulnerabilidades u obtener información de forma ilícita, para después distribuirla o bien secuestrar datos, alterarlos, etc.; con la diferencia de que no busca un beneficio propio, se denominan como "delitos de alarde"[123] y que puede configurar delitos como el acceso ilícito a los sistemas informáticos o hasta contra la intimidad sexual.

Por ejemplo, el sujeto que accede de manera ilícita a un dispositivo y obtiene imágenes privadas del dueño o de la dueña, para luego difundirlas por las redes sociales sin esperar nada a cambio, más que reconocimiento por haber sido tan hábil, es por eso por lo que se denominan delitos de alarde.

El tercer tipo son los *hackers* de sombrero blanco los cuales son definidos como "hackers éticos que trabajan para proteger los sistemas y a las personas"[124]. Mientras que desde otra perspectiva son aquellos que tratan de mejorar la seguridad de los sistemas, encontrando vulnerabilidades y dando aviso inmediato a los dueños

---

[121] Kaspersky, *Hackers de sombrero negro, blanco y gris: definición y explicación*, 2021, https://latam.kaspersky.com/resource-center/definitions/hacker-hat-types de 30 julio de 2021, 13:25 hrs.

[122] McAfee, *9 tipos de hackers y sus motivaciones*, 2019, https://www.mcafee.com/blogs/languages/espanol/9-tipos-de-hackers-y-sus-motivaciones/ de 30 julio de 2021, 13:40 hrs.

[123] Instituto Nacional de Ciencias Penales, *Delitos informáticos*, https://www.youtube.com/watch?v=ggg0v65j474 de 5 octubre de 2022, 09:54 hrs.

[124] Romero, Sarah, *¿Cuántos tipos de hackers existen?,* Muy interesante, 2019, https://www.muyinteresante.es/tecnologia/articulo/que-es-un-hacker-de-sombrero-gris-831473842564 de 22 febrero de 2022, 14:37 hrs.

correspondientes. No se considera propiamente a los *hackers* de sombrero blanco como ciber atacantes, porque pueden ser trabajadores del propio Estado o empresas privadas que de manera consensuada dan acceso a sus trabajadores encargados de la ciberseguridad para tener acceso a los sistemas para descubrir, errores, vulnerabilidades y dar aviso inmediato para subsanar dichas vulnerabilidades, a efecto de no ser víctimas de ataques exteriores e inclusive internos.

El último cuadro es donde se encuentran los denominados aficionados o mejor dicho *script kiddies*, o sea, las personas comunes con escaso conocimiento en el mundo de la informática. El *script kiddie* es definido como "un individuo no calificado que utiliza scripts o programas desarrollados por otros para atacar sistemas informáticos, redes y defectos de sitios web"[125].

### 3.2.1.1.3 BIEN JURÍDICO

El bien jurídico o bienes jurídicos "son circunstancias dadas o finalidades que son útiles para el individuo y su libre desarrollo en el marco de un sistema social global estructurado sobre la base de esa concepción de los fines o para el funcionamiento del propio sistema"[126].

El bien jurídico es el interés tutelado por el derecho penal, de tal suerte que en el ámbito informático hay diferentes bienes jurídicos tutelados entre los que destaca el patrimonio, y es apropiado saber que la mayoría de los delitos informáticos lo que buscan es obtener un lucro patrimonial a través del fraude y la extorsión, otro es la confidencialidad digital que conlleva la distribución de lo que se

[125] Valencia Santiago, Iván, *Hacker, Crackers, Lamers, Script Kiddies y Phreakers ¿Quiénes son?*, 2018, https://seguridad.cicese.mx/alerta/335/Hacker,-Crackers,-Lamers,-Script-Kiddies-y-Phreakers-Quienes-son de 5 agosto de 2021, 12:30 hrs.

[126] Roxin, Claus, trad. Luzón Peña, Diego-Manuel et al, op. cit., p.56.

denomina vulgarmente como *packs* o *nudes* y que dio como resultado la reforma Olimpia.

### 3.2.1.1.4 MEDIOS COMISIVOS

"Si el tipo señala que la conducta debe realizarse utilizando objetos o instrumentos, o bien mediante alguna actividad o inactividad, hablamos de la exigencia de medios de comisión"[127]. Resumiendo, los medios comisivos son aquellos elementos con los cuales se puede cometer el tipo y es aquí donde residen los medios informáticos para actualizar la conducta a los delitos tradicionales, ejemplo extorsión a través de apps de préstamos falsos. Los dispositivos informáticos, se añaden como elementos comisivos. En nuestra actualidad no solo opera la violencia física o moral como elementos más comunes del delito, sino ahora los dispositivos electrónicos como la *PC* o el propio celular.

### 3.2.1.1.5 CIRCUNSTANCIAS DE MODO, TIEMPO, LUGAR U OCASIÓN

Las circunstancias de modo, tiempo, lugar u ocasión delimitan el ámbito de protección de los tipos penales, o sea, restringe las conductas no dejándolas tan amplias como para llegar al extremo de ser consideradas como tipos penales abiertos[128]. Es debido a esto, que la mayoría de los tipos penales cuentan con tales circunstancias.

> Tiempo: Temporalidad que el tipo prevé para que se realice la conducta o se actualice el resultado;

[127] Cossío Zazueta, Luis et al, *Enciclopedia Jurídica de la Facultad de Derecho*, Porrúa, Tomo IX Derecho Penal, México, 2018, p. 48.

[128] El tipo penal abierto tiene como característica fundamental la no precisión de las conductas descritas en el tipo penal. Por ejemplo: Comete el delito de aborto a la mujer que estando embarazada decida abortar.
Como se puede notar, no se establece qué es el aborto, ni a las cuántas semanas de embarazo se empieza a gestar la vida, por lo tanto, se deja al criterio del juez decidir tales cuestiones. El tipo penal abierto es indicio de autoritarismo.

Lugar: Espacio físico que el tipo prevé para que se realice la conducta o se actualice el resultado;

Modo: Cualquier característica que deba resistir la conducta o la producción del resultado, prevista por el tipo y;

Ocasión: Riesgo al que está expuesto el bien jurídico y que el agente aprovecha para realizar la conducta o producir el resultado, igualmente previsto en el tipo[129].

### 3.2.1.1.6 OBJETO MATERIAL Y JURÍDICO

"El objeto material es la persona o cosa sobre la cual recae directamente el daño causado por el delito cometido o el peligro en que se colocó a dicha persona o cosa… El objeto jurídico es el interés jurídicamente tutelado por la ley"[130]. En el delito informático el objeto material puede ser tanto la persona como el dispositivo electrónico; en el primer supuesto puede ser la difusión de imágenes sexuales sin el consentimiento de la víctima, mientras que en el segundo es el *ransomware*[131] que da como resultado la inutilidad del dispositivo así afectando la disponibilidad de éste, o sea, el objeto material es el dispositivo electrónico que ha sido secuestrado.

### 3.2.1.2 ELEMENTOS SUBJETIVOS DEL TIPO

Los elementos subjetivos del tipo nacen con los sistemas valorativo o neoclásico (1920 a 1940) y el finalista (1940-1970) en contrasentido del sistema clásico o mal llamado causalista que impero a finales del siglo XIX y principios del XX. El sistema clásico es predominantemente objetivo dejando el lado subjetivo en la culpabilidad, ideas que fueron criticadas por el sistema neoclásico y más adelante

[129] Ibidem, p. 54
[130] Amuchategui Requena, Irma Griselda, op. cit., 41
[131] Secuestro de datos

por el finalista, puesto que no se podía concebir una voluntad sin contenido, una conducta sin voluntad -elemento esencial de la acción finalista-.

En el sistema neoclásico, "el tipo seguía siendo objetivo (aunque emparchado con elementos subjetivos cuando con los objetivos no alcanzaba para verificar la tipicidad)"[132]. Nótese como el tipo para el sistema valorativo seguía siendo en su mayoría objetivo, pero con la distinción de ciertos elementos subjetivos cuando los elementos objetivos no alcanzaban a verificar en su totalidad la tipicidad.

Estos elementos subjetivos son conocidos en nuestra dogmática penal como elementos anímicos o subjetivos específicos. El ejemplo más común se encuentra en el acoso sexual puesto que hasta qué punto por ejemplo un piropo puede representar un halago o una ofensa; esto dependerá del ánimo con el que sea dirigido hacia el sujeto.

En cuanto al dolo y la culpa "seguían siendo elementos de la culpabilidad, y ésta era entendida siempre normativamente, aunque al igual que en Frank el reproche contenía el objeto reprochado, que era precisamente la voluntad de producir el resultado o la negligencia (dolo o culpa)"[133].

El sistema neoclásico mantenía la postura de seguir conteniendo al dolo y la culpa dentro de la culpabilidad, pero con la característica de que ésta era normativa – o sea, el reproche por no haberse dirigido conforme a derecho- y no psicológica como la consideraba el sistema clásico.

Con el nacimiento del finalismo a mediados del siglo XIX se da un giro total a la teoría del delito pues nace el tipo subjetivo especifico moviendo al dolo y a la culpa a dicho tipo, pues "toda acción consciente es llevada por la decisión de acción, es decir, por la conciencia de lo que se quiere -el elemento intelectual-, y la decisión de querer realizarlo -el elemento volitivo-. Ambos elementos juntos, como factores creadores de una acción real, constituyen el dolo"[134]. El dolo es esencial para la acción finalista, pero por igual es importante para el tipo subjetivo pues el *Vorsatz* -

[132] Zaffaroni, Eugenio Raúl et al., *Manual de derecho penal parte general*, 2da edición, EDIAR, Buenos Aires, 2007, p. 301.
[133] Ídem.
[134] Welzel, Hans, *Derecho penal parte general,* trad. de Fontán Balestra, Carlos, Roque Depalma, Buenos Aires, 1956, p. 73.

Dolo- se integra de un elemento intelectual y volitivo -querer y voluntad-, así concibiendo al *Tatbestandsirrtum* -error de tipo- debido a que cuando no se integre uno de los elementos que constituyen al dolo se actualiza el error de tipo y dependiendo de la casuística penal se podrá hablar de un error vencible o invencible.

En la actualidad en nuestro derecho penal mexicano los elementos subjetivos son:

1. Dolo: Como la voluntad y conocimiento de concreción del tipo penal. Es así como de dicha definición se desprenden sus elementos como: a) Conocimiento y b) Voluntad.
2. Culpa: Como la violación a un deber objetivo de cuidado. La culpa se divide en dos clases: a) Culpa con representación y b) Culpa sin representación.

Los delitos informáticos se pueden cometer tanto de naturaleza dolosa como culposa, por ejemplo, en la culpa puede ser la distribución de *fake news* como dolosamente el *ransomware*.

### 3.2.1.3 ELEMENTOS NORMATIVOS DEL TIPO

Sobre los elementos normativos, “Max Ernst Mayer puso en evidencia que ciertos tipos penales no solo describen realidades (cosa, muerte o lesión, que están en una relación causal con la conducta y son perceptibles a través de los sentidos), sino que también se refieren a conceptos que requieren de una valoración jurídica o cultural previa a la antijuridicidad”[135].

Entonces los elementos normativos del tipo son aquellos que requieren de una valoración especial previos a la antijuridicidad y se dividen en culturales y jurídicos. Los primeros necesitan de una valoración cultural, social donde obviamente entran los especialistas en los temas -en el caso del derecho penal

[135] Díaz Aranda, Enrique y Roxin, Claus, *Teoría del delito funcionalista*, Flores Editor, México, 2017, p.127.

informático serán los especialistas en electrónica, informática, programación-, y los segundos por igual de una valoración, pero a través de otras normas jurídicas.

En los delitos informáticos la mayoría de elementos normativos de los cuales se integra este injusto -entendido como sinónimo de delito, no como antijuridicidad o elementos objetivos del delito- operan tanto elementos normativos culturales y jurídicos en este último se tienen algunas leyes que tratan de cuestiones electrónicas-informáticas, por ejemplo se tiene la Ley Federal de Telecomunicaciones y Radio fusión, Ley Federal del Derecho de Autor, la Ley de Acceso de las Mujeres a una Vida Libre de Violencia de la Ciudad de México, entre otras, por ejemplo esta última ley es donde establece lo que significa violencia digital, pues así, si un tipo penal llegase a relacionarse con la violencia digital o se haga mención expresa de ésta, pues como elemento normativo jurídico nos tendríamos que remitir a dicha ley.

Ahora bien, el elemento normativo cultural podría ser la palabra “medio tecnológico” establecido en la segunda fracción del artículo 181 Quintus del código penal de la CDMX, ya que solo da casuística de los dispositivos que integran a los medios tecnológicos, pero nunca el significado de lo qué es en sí un medio tecnológico, a lo cual se tendrá que acudir a lo cultural, social de lo que se entiende propiamente por dicha palabra.

### 3.2.2. ANTIJURIDICIDAD

La Antijuridicidad -*Rechtswidrigkeit*-, "es el desacuerdo de la acción con las exigencias que impone el derecho para las acciones que se realizan en la vida social. Es el disvalor jurídico, que corresponde a la acción a consecuencia de esa divergencia"[136]. De dicha definición se desprenden dos palabras fundamentales que son el desacuerdo y la exigencia esenciales para comprender un concepto más acorde a un punto de vista propio basado en la exigencia ligada a la sana convivencia social.

La antijuridicidad es un juicio de disvalor ex post que atenta contra la finalidad del derecho penal en cuanto ésta es la sana convivencia social, así cuando el sujeto delinque encuadra su conducta al tipo, no habiendo antijuridicidad en un primer plano, sino en segundo plano negando la sana convivencia social -se puede decir que la posibilidad en sentido positivo es la condición para que se dé paso a la antijuridicidad-.

Así viendo al tipo como presupuesto de la antijuridicidad, no como juicio, pues éste es una característica propia de la antijuridicidad, por eso se hace la alusión al primer plano y segundo plano. Ambos elementos -tipo y antijuridicidad- ligados, y que al momento de su estudio dentro del proceso penal como en la dogmática el tipo es *ratio essendi* de la antijuridicidad -*ex post*-, mientras que en la técnica legislativa al momento de tipificar los tipos penales se invierten los papeles donde la antijuricidad es *ratio essendi* del tipo -*ex ante*- quedando ahora como un juicio de disvalor ex ante…

Idea anterior que en parte está de acuerdo con lo escrito por el Dr. Ricardo Franco Guzmán al establecer que:

> Así que, es innegable que el nacimiento del tipo surge de una acotación de la conducta antijurídica que el legislador considera en un momento determinado como digna de una pena, constituyendo por tanto la antijuridicidad la *ratio essendi* de la tipicidad. Y por lo que respecta especialmente a los momentos del delito,

[136] Welzel, Hans, trad. de Fontán Balestra, Carlos, op, cit., p. 57

> consideramos que la tipicidad es un factor indiciario, es decir, *ratio cognoscendi* de la antijuridicidad de la conducta, pues si un determinado hecho es considerado típico estamos en presencia de un indicio de su calidad antijurídica… [137]

Interesante lo que escribió Wilhelm Gallas, al respecto sobre la evolución de la relación tipo-antijuridicidad al establecer lo siguiente:

"La acción es típica si se puede clasificar en un tipo, esto es, en una de las descripciones legales del aspecto externo de la conducta punible. Hasta aquí no se ha formulado aún, un juicio de valor. El pronunciamiento de este juicio ésta contenido por primera vez en la afirmación de la antijuricidad de la conducta… La subsunción en el tipo neutro valorativamente no permite fundar aún la antijuridicidad"[138].

Nótese, como en las primeras ideas sobre la relación tipo-antijuridicidad (*Tatbestand-Rechtswidrigkeit*) se concebía al tipo como un objeto neutro, algo que se podría pensar ir acorde a la definición de la antijuridicidad como disvalor *ex post*… pero no es así, puesto que el tipo en dicha definición es un presupuesto ya valorado desde una antijuridicidad *ex ante*, por eso se convierte en ratio *essendi* y no *cognoscendi*, pues como Gallas en siguientes páginas expresa:

"Tampoco fue ya posible mantener una separación entre el tipo y la función de protección propia del ordenamiento penal. De este modo ha perdido aquél su neutralidad valorativa, se ha convertido en la descripción legal de la lesión del bien jurídico, propia del delito respectivo, y ha pasado de ser un puro indicio de antijuridicidad (*ratio cognoscendi*) a transformarse en el elemento portador (*ratio essendi*) del injusto"[139].

Justamente tomó parte de las ideas de Gallas, al considerar al tipo como elemento portador, pero como un presupuesto valorado mediante la antijuridicidad

[137] Franco Guzmán, Ricardo, op cit, pp. 46, 47.
[138] Gallas, Wilhelm, trad. Córdoba Roda, Juan, op cit, p. 12.
[139] Ibidem, pp. 14, 15.

*ex ante* al momento de la tipificación de conductas. No se puede tipificar una conducta si no ha sido valorada con anterioridad.

Establecida la antijuridicidad, se puede entender que ésta es igual para todos los delitos ya que todos atentan contra la finalidad del derecho penal a menos que no exista el delito o lo faculte excepcionalmente, en todo caso la conducta es atípica, justificada o inculpada.

### 3.2.3. CULPABILIDAD

La culpabilidad como elemento del delito por igual no representa un mayor problema ya que no hay culpabilidades especiales, aquí se reprochará el delito al sujeto por haber contravenido la finalidad del derecho penal al elegir la posibilidad en sentido positivo, el reproche se hará de manera personalísima. El Dr. Enrique Díaz Aranda define a la culpabilidad como "el reproche que se hace a quien realizó o participó en el injusto, ya que pudiéndose comportar conforme a derecho decidió contravenirlo"[140].

De la definición del Dr. Enrique Díaz Aranda, se desprende el reproche el cual no es más que la desaprobación por haber delinquido, la segunda característica es el injusto y aquí es donde el injusto puede tener varios significados que van desde 1. Sinónimo de delito; 2. Elementos objetivos del delito; y 3. Sinónimo de antijuridicidad, justamente se refiere propiamente a sinónimo de delito, y no a los elementos objetivos del delito en cuanto que para llegar a la culpabilidad se tuvieron que haber concretado el elemento típico y antijurídico, por ejemplo: error de justificación -el sujeto cometió un injusto ya que su conducta es típica y antijuridica, pero no culpable-; por último establece en su definición el no haberse podido comportar conforme a derecho, por ende decidió contravenirlo; en este último punto claramente se puede apreciar con toda claridad que la posibilidad de delinquir fue

[140] Díaz Aranda, Enrique y Roxin, Claus, op. cit., p. 343.

en sentido positivo, así negando la sana convivencia social dando como resultado la antijuridicidad y después la exigencia, el reproche.

Es así como los elementos objetivos del tipo son el alma del reproche; donde el tipo en su verbo rector o verbos rectores reside la posibilidad de delinquir, si se da en sentido positivo entonces damos lugar a la antijuridicidad -nótese se está dando paso a un segundo plano, donde no se reprocha en sí el tipo penal, sino la antijuridicidad-.

Derivado de lo anterior se puede definir a la culpabilidad como el reproche personalísimo que se le hace al sujeto por haber elegido la posibilidad de delinquir en sentido positivo, así negando la sana convivencia social.

Otra característica de la culpabilidad es que es el elemento más humano que se puede encontrar como elemento del delito y el fundamento se encuentra en el artículo 405 con especial interés en su fracción III y el 410 en sus párrafos tercero, cuarto, quinto y último, dos artículos del Código Nacional de Procedimientos Penales -en adelante CNPP-.

> Artículo 405. Sentencia absolutoria
>
> En la sentencia absolutoria, el Tribunal de enjuiciamiento ordenará que se tome nota del levantamiento de las medidas cautelares, en todo índice o registro público y policial en el que figuren, y será ejecutable inmediatamente.
>
> En su sentencia absolutoria el Tribunal de enjuiciamiento determinará la causa de exclusión del delito, para lo cual podrá tomar como referencia, en su caso, las causas de atipicidad, de justificación o inculpabilidad, bajo los rubros siguientes:
>
> I. Son causas de atipicidad: la ausencia de voluntad o de conducta, la falta de alguno de los elementos del tipo penal, el consentimiento de la víctima que recaiga sobre algún bien jurídico disponible, el error de tipo vencible que recaiga sobre algún elemento del tipo penal que no admita, de acuerdo con el catálogo de delitos susceptibles de configurarse de forma culposa previsto en la legislación penal aplicable, así como el error de tipo invencible;
>
> II. Son causas de justificación: el consentimiento presunto, la legítima defensa, el estado de necesidad justificante, el ejercicio de un derecho y el cumplimiento de un deber, o

III. Son causas de inculpabilidad: el error de prohibición invencible, el estado de necesidad disculpante, la inimputabilidad, y la inexigibilidad de otra conducta.

De ser el caso, el Tribunal de enjuiciamiento también podrá tomar como referencia que el error de prohibición vencible solamente atenúa la culpabilidad y con ello atenúa también la pena, dejando subsistente la presencia del dolo, igual como ocurre en los casos de exceso de legítima defensa e imputabilidad disminuida[141].

Como se logra apreciar con toda claridad este artículo se basa en la sentencia absolutoria en su eje la aplicación de los elementos del delito, aquí es donde el delito no existe o simplemente el sujeto se encuentra facultado para delinquir.

La fracción III establece al 1. Error de prohibición invencible; 2. Estado de necesidad disculpante; 3. Inimputabilidad; y por último 4. Inexigibilidad de una conducta. Bajo estas cuatro facultades que otorga el derecho penal para delinquir bajo una inculpabilidad.

Claro ejemplo hipotético, el de Johann, un albañil; que a diario sale a las 5:00 a.m. de su casa ubicada en el molinito perteneciente al municipio de Naucalpan de Juárez, EDOMEX; a lo cual tiene que caminar alrededor de cinco minutos para tomar el primer transporte en el derrotero correspondiente. Un día miércoles sale de su casa para tomar rumbo a su trabajo ubicado en la CDMX, durante su caminata un sujeto lo intercepta con arma de fuego en mano y le exige sus pertenencias, a lo cual Johann no acepta y se abalanza contra el delincuente, al final el primero logra desarmarlo y el segundo cae al suelo sin el arma; así Johann ante la adrenalina decide darle dos disparos en el pecho al sujeto dando como resultado la muerte del delincuente. Si analizamos el delito hay un elemento típico, donde se encuentra la conducta -*Verhalten*- en su división de acción -*Handlung*-, donde conducta = acción y resultado -*Erfolg-;* donde estos dos últimos -acción y resultado- están unidos a una causalidad - *Kausalität* - = Homicidio, pero facultado excepcionalmente bajo el error de justificación o mal llamado error de prohibición –*Erlaubnisirrtum, Verbotsirrtum*- sobre la legítima defensa – *Notwehr*-, dando así como pregunta, ¿El

[141] Artículo 405, *Código Nacional de Procedimientos Penales*, México, 2021, http://www.diputados.gob.mx/LeyesBiblio/pdf/CNPP_190221.pdf de 25 septiembre de 2021, 14:24 hrs, pp. 114, 115.

Estado puede reprocharle a Johann el haber actuado de esa manera si su vida corría peligro?

Otro caso hipotético que puede ser más debatido puede ser el de una madre de una hija y un hijo, donde el padre es un alcohólico y golpeador, cada día los abusos tanto físicos como psicológicos no paran, a lo cual, ante tanto daño y trauma, la mujer no sabe qué hacer, tiene miedo de actuar e ir ante las autoridades, pero tampoco desea ver seguir sufriendo a sus descendientes.

A lo cual una noche durante la cena decide envenenar la comida del padre abusador, dándole muerte. Tan solo imaginar ponerse en el lugar de la madre, cuánta presión, miedo, tortura física como mental debió de haber vivido para haber actuado de tal manera, ¿El Estado puede reprocharle a la madre el haber actuado de esa manera?

El contexto especifico de cada caso deberá ser analizado minuciosamente para esta clase de delitos. El derecho penal no solo es ley, sino contexto y dependiendo de cada caso en concreto se deberá analizar minuciosamente si opera o no un error de prohibición, la inexigibilidad de una conducta u otra clase de inculpabilidad.

Las ideas de Reinhard Frank marcaron una gran evolución a la concepción de la culpabilidad a través de la graduación de la culpabilidad mediante las circunstancias concomitantes, así destacando elementos externos al dolo y la culpa.

“La doctrina dominante fija el concepto de culpabilidad de manera que ella solamente comprende los conceptos de dolo y de imprudencia. Po el contrario, es preciso, concebirlo de tal modo que tome en consideración las circunstancias concomitantes…”[142]

Explicada de manera resumida la culpabilidad, se puede entender que la culpabilidad es general para todos los delitos, al igual que la antijuridicidad, por eso no se puede escribir sobre una culpabilidad especial para los delitos informáticos.

[142] Von Frank, Reinhard*, Estructura del Concepto de Culpabilidad*, Editorial HEBO, Ciudad de México, 2022, p. 27.

Es así, que el único elemento del delito que verdaderamente presenta cambios en el orden informático es el elemento típico.

# CAPÍTULO IV MARCO JURÍDICO

## 4.1 CONVENCIONALIDAD

Si bien el punto de partida de los delitos informáticos se encuentra en el Convenio N.º 185 del Consejo de Europa, sobre la Ciberdelincuencia, también denominado Convenio de Budapest, se han desarrollado legislaciones especializadas como la *Surveillance Devices Act* -ley de dispositivos de vigilancia- de Australia, la cual se analizará a continuación.

La *Surveillance Devices Act* (Ley de dispositivos de vigilancia), que como su nombre lo indica es una ley para la utilización y regulación de dispositivos para vigilancia dentro del orden criminal. Sus objetivos son: 1. Proporcionar un marco jurídico para el uso de dispositivos de vigilancia en las investigaciones penales; 2. Permitir la recolección de pruebas de manera encubierta con fines para el proceso penal; y 3. Garantizar la privacidad de las personas.

En agosto de 2021, hubo un proyecto para reformar dicha ley sobre los dispositivos de vigilancia y las *Telecommunications (Interception and Access) Act*, entre otras leyes, el proyecto denominado *Identify and Disrupt* -identificar e interrumpir- tiene como ejes rectores que la *Australian Federal Police* (*AFP*) y la *Australian Criminal Intelligence Commission* (*ACIC)* cuenten con las siguientes facultades:

1. Interrupción de datos para modificar, agregar, copiar o eliminar datos para evitar la comisión de delitos graves en línea;
2. Solicitar órdenes de actividad de red para recopilación sobre actividades delictivas graves;
3. Solicitar órdenes de posesión sobre la cuenta en línea de una persona con el fin de reunir pruebas para promover una investigación criminal[143].

[143] Parliament of Australia, *Serveillance Legislation Amendment (Identify and Disrupt) Bill 2021*, Australia, 2021, https://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/Bills_Search_Results/Result?bId=r6623 de 3 noviembre de 2021, 14:56 hrs.

Estas acciones son las más destacables de las tantas que se proponen en dicho proyecto.

En el caso de México, se pretendió la creación del Padrón Nacional de Usuarios de Telefonía Móvil (PANAUT) que generó una acción de inconstitucionalidad 82/2021 mediante el control concentrado[144] cuyo fundamento es el artículo 105 fracción constitucional en lo que respecta a la acción de inconstitucionalidad. El asunto del PANAUT fue resuelto por la Suprema Corte de Justicia de la Nación (SCJN) así declarando inconstitucionales las disposiciones publicadas en el Diario Oficial de la Federación (DOF) publicadas el 16 de abril del 2021 que contenían reformas y adiciones a la Ley Federal de Telecomunicaciones y Radiodifusión que generaban afectaciones a los derechos a la privacidad, intimidad y protección de datos personales[145].

El PANAUT tenía como características principales obtener datos personales de los usuarios de telefonía móvil como:

1. Nombre;
2. Nacionalidad;
3. Número de identificación o CURP;
4. Datos sensibles (datos biométricos)[146].

El PANAUT trataba de tener la finalidad de colaborar con las autoridades encargadas de la seguridad y en asuntos relacionados con la comisión de delitos -en nuestro caso, delitos informáticos-.

---

[144] El control concentrado se da a través del Poder Judicial de la Federación y tiene como posible resultado la inconstitucionalidad de la norma o ley, mientras que el control difuso corresponde al resto de tribunales a través del principio pro-persona, en el control difuso solo existe la inaplicación de la norma o ley, pero no la inconstitucionalidad de éstas. Véase. Expediente Varios 912/2010, Sentencias y datos de expedientes, abril de 2011, https://www2.scjn.gob.mx/ConsultaTematica/PaginasPub/DetallePub.aspx?AsuntoID=121589 de 17 de noviembre de 2022, 16: 36 hrs, p. 36.

[145] Véase. Expediente 82/2021, Sentencias y datos de expedientes, abril de 2022, https://www2.scjn.gob.mx/ConsultaTematica/PaginasPub/DetallePub.aspx?AsuntoID=283367 de 17 de noviembre de 2022, 16:50 hrs.

[146] "Los datos biométricos son aquellos datos personales referidos a las características físicas, fisiológicas o conductuales de una persona que posibiliten o aseguren su identificación única". Véase. González, Ana, Datos biométricos - ¿Qué y cuáles son? ¿Cómo cumplir con la ley?, 2019, https://ayudaleyprotecciondatos.es/2019/02/15/datos-biometricos/ de 17 noviembre de 2022, 17:00 hrs.

Desde un punto de vista crítico, los delitos informáticos no solo abarcan tipos penales como la extorsión y el fraude, así como medio comisivo el teléfono celular. Los delincuentes informáticos cuentan con demasiadas herramientas para delinquir como se pudo observar en el capítulo 2 -Redes sociales y ciberseguridad-. Sin duda el PANAUT sería una herramienta infructuosa contra el combate de los delitos de naturaleza informática, además que se atentaría contra el derecho a la privacidad[147] y protección de datos personales[148].

Para dar frente a un combate contra los delitos informáticos nuestro país tendría que ser Estado Parte del Convenio de Budapest para analizar y comprender de una manera mucho más clara el estudio de los delitos informáticos. Cuyo contenido será analizado desde una perspectiva de delitos básicos y subordinados como se propone a continuación.

### 4.1.1 CONVENIO DE BUDAPEST ANALIZADO DESDE LA PROPUESTA DE DELITOS BÁSICOS Y DELITOS SUBORDINADOS

El convenio es definido como “la norma internacional más completa hasta la fecha, ya que proporciona un marco integral y coherente en contra del ciberdelito y la evidencia electrónica. Sirve como una guía para cualquier país que desea desarrollar una legislación nacional integral sobre ciberdelitos y como un marco para la cooperación internacional entre los Estados Parte de este tratado”[149].

---

[147] El derecho a la privacidad tiene como fundamento el artículo 11 número 2 de la Convención Americana de Derechos Humanos, que reza lo siguiente: “Nadie puede ser objeto de injerencias arbitrarias o abusivas en su vida privada, en la de su familia, en su domicilio o en su correspondencia, ni de ataques ilegales a su honra o reputación”. Véase. Artículo 11 número, Convención Americana sobre Derechos Humanos, 1981, https://www.cndh.org.mx/sites/default/files/doc/Programas/TrataPersonas/MarcoNormativoTrata/InsInternacionales/Regionales/Convencion_ADH.pdf de 17 de noviembre de 2022, 17:21 hrs.

[148] Los datos personales tienen su fundamento en la Ley Federal de Protección de Datos Personales en Posesión de los Particulares en su artículo 3 fracción V, “Para los efectos de esta Ley, se entenderá por: V. Datos personales: Cualquier información concerniente a una persona física identificada o identificable. Véase. Artículo 3 fracción V, Ley Federal de Protección de Datos Personales en Posesión de los Particulares, https://www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf de 17 de noviembre de 2022, 17:30 hrs.

[149] Consejo de Europa, *Adhesión al Convenio de Budapest sobre la Ciberdelincuencia: Beneficios*, 2021, https://rm.coe.int/cyber-buda-benefits-junio2021a-es/1680a2e4de de 4 noviembre de 2021, 13:27 hrs.

Cuenta con dos protocolos adicionales -1. Sobre xenofobia y racismo; 2. Refuerzo de la cooperación y divulgación de pruebas electrónicas-, hasta junio del 2021 había 66 ratificaciones por parte de países miembros del consejo de Europa entre los que destacan Alemania, Reino Unido, España, entre otros, y por parte de países no miembros tenemos a Chile, Argentina, Colombia, Costa Rica, Perú, Australia, Estados Unidos de América, etc. El Convenio de Budapest -en adelante convenio- cuenta con 4 capítulos -I. Terminología; II. Medidas que deberán adoptarse a nivel nacional; III. Cooperación internacional y; IV. Cláusulas finales- y con un total de 48 artículos.

Haciendo ahora un análisis un poco más profundo al convenio en el capítulo I que sólo consta de un artículo, se establecen las propias definiciones de a) Sistema informático; b) Datos informáticos; c) proveedores de servicios y; d) Datos relativos al tráfico. Dentro de la primera definición sobresalen las palabras dispositivo aislado, dispositivos interconectados y tratamiento automatizado de datos en ejecución de un programa. En nuestra actualidad un dispositivo aislado es raro de ver o comprender debido a que los ordenadores para tener una funcionalidad vital necesitan estar interconectados de donde sobresale la red informática, entonces para entender al dispositivo interconectado se debe analizar primero lo que es la red informática y ésta puede ser definida como una conexión entre varios dispositivos electrónicos para intercambiar, enviar o recibir información.

La conexión sería a través de los dispositivos red, usuario final y medio de conexión, donde los primeros -dispositivos red- gestionan el acceso a la información, por ejemplo: el modem de la casa, el segundo -usuario final- es aquel al cual le llega la información, por ejemplo: la computadora, televisión; y como medio de conexión es el que hace posible que los dispositivos se relacionan entre sí, destacando la red inalámbrica *wi-fi*.

Ejemplo:

María llega a su casa y rápidamente se conecta a su internet mediante wi-fi a través de su celular para chatear con su novio Antonio -aquí inmediatamente

observamos el medio de conexión y dispositivo red que es el modem y usuario final que es el celular de María-.

Como se puede apreciar con este ejemplo es posible comprender el dispositivo interconectado, respecto al dispositivo aislado[150]. Entonces no queda más que establecer lo contrario *sensu* que el dispositivo aislado es aquel que no cuenta con una red informática.

Por último, se establece el tratamiento automatizado de datos en ejecución de un programa[151]. En los datos informáticos se tienen palabras clave como representación de hechos, información o cualquier concepto que conlleve tratamiento informático; estos elementos son sujetos del tratamiento de la información que se divide en: 1. Manual; 2. Mecánica y; 3. Automática, así destacando que el tratamiento de la información automática es el que se maneja a través de los dispositivos electrónicos.

Los proveedores de servicios son aquellos que ofrecen sus servicios con la posibilidad de comunicarse a través de los sistemas informáticos y se dividen en públicos y privados, así como aquellos que procesen o guarden datos informáticos para dicho servicio. Mientras que los datos relativos al tráfico son los datos generados por los sistemas electrónicos, qué indican hora, lugar, destino, fecha, tamaño, etc.

El capítulo II contiene la parte sustantiva del artículo 2 al 13. Esta parte es medular ya que establece los delitos de carácter informático, así como la propia tentativa, complicidad y la responsabilidad de las personas jurídicas.

Los delitos contenidos en el convenio son los siguientes:

a) Acceso ilícito;
b) Interceptación ilícita;

[150] El dispositivo aislado puede estar haciendo alusión al *sandboxing*, pues éste es un aislamiento de procesos, por ejemplo: *VirtualBox* para análisis de documentos o *software* que parezcan maliciosos para así no dañar la máquina principal.
[151] Esto es una referencia a la definición dada en el capítulo I de este presente trabajo pues la informática es Información automática y que para que se dé esta información automatizada se necesita la ejecución de un *software* o programa.

c) Ataques a la integridad de los datos;
d) Abuso de los dispositivos;
e) Falsificación informática;
f) Fraude informático;
g) Delitos relacionados con la pornografía infantil y;
h) Delitos relacionados con infracciones de la propiedad intelectual y de los derechos afines.

En cuanto a los delitos de acceso ilícito, interceptación ilícita, ataques a la integridad de los datos, ataques a la integridad del sistema y abuso de los dispositivos, se estipula lo siguiente:

> Título 1. Delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos.
>
> **Artículo 2 – Acceso ilícito.**
>
> Cada parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno el acceso deliberado e ilegítimo a todo o parte de un sistema informático. Las partes podrán exigir que el delito se cometa infringiendo medidas de seguridad, con la intención de obtener datos informáticos u otra intención delictiva, o en relación con un sistema informático conectado a otro sistema informático.
>
> **Artículo 3 – Interceptación ilícita.**
>
> Cada parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno la interceptación deliberada e ilegítima por medios técnicos de datos informáticos en transmisiones no públicas dirigidas a un sistema informático, originadas en un sistema informático o efectuadas dentro del mismo, incluidas las emisiones electromagnéticas provenientes de un sistema informático que transporte dichos datos informáticos. Las partes podrán exigir que el delito se cometa con intención delictiva o en relación con un sistema informático conectado a otro sistema informático.
>
> **Artículo 4 – Ataques a la integridad de los datos.**
>
> 1. Cada parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno todo acto deliberado e ilegítimo que dañe, borre, deteriore, altere o suprima datos informáticos.

2. Las partes podrán reservarse el derecho a exigir que los actos definidos en el párrafo 1 comporten daños graves.

**Artículo 5 – Ataques a la integridad del sistema.**

Cada parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno la obstaculización grave, deliberada e ilegítima del funcionamiento de un sistema informático mediante la introducción, transmisión, daño, borrado, deterioro, alteración o supresión de datos informáticos.

**Artículo 6 – Abuso de los dispositivos.**

1. Cada parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno la comisión deliberada e ilegítima de los siguientes actos:

a. La producción, venta, obtención para su utilización, importación, difusión u otra forma de puesta a disposición de:

i. Cualquier dispositivo, incluido un programa informático, concebido o adoptado principalmente para la comisión de cualquiera de los delitos previstos en los artículos 2 a 5 del presente Convenio;

ii. Una contraseña, código de acceso o datos informáticos similares que permitan acceder a todo o parte de un sistema informático;

Con una intención de que sean utilizados para cometer cualquiera de los delitos contemplados en los artículos 2 a 5; y

b. La posesión de alguno de los elementos contemplados en los incisos i) o ii) del apartado a) del presente artículo con intención de que sean utilizados para cometer cualquiera de los delitos previstos en los artículos 2 a 5. Las partes podrán exigir en su derecho interno la posesión de un número determinado de dichos elementos para que se considere que existe responsabilidad penal.

2. No se interpretará que el presente artículo impone responsabilidad penal cuando la producción, venta, obtención para la utilización, importación difusión o cualquier otra forma de puesta a disposición mencionada en el párrafo 1 del presente artículo no tenga por objeto la comisión de uno de los delitos previstos de conformidad con los artículos 2 a 5 del presente Convenio, como en el caso de las pruebas o de la protección de un sistema informático.

3. Las partes podrán reservarse el derecho a no aplicar el párrafo 1 del presente artículo, siempre que dicha reserva no afecte a la venta, distribución o cualesquiera

otras formas de puesta a disposición de los elementos mencionados en el inciso 1 a) ii) del presente artículo[152].

Este título es fundamental de la ciberseguridad y el derecho informático debido a que representa la triada CID -Confidencialidad, Integridad y Disponibilidad- donde la confidencialidad es equivalente a privacidad y el acceso limitado a cierto tipo de agentes privilegiados, tal es el caso del acceso a la computadora privada, celular o a los sistemas informáticos de una empresa a la cual sólo los trabajadores encargados de la ciberseguridad de la propia empresa pueden tener acceso; la integridad se refiere a la confiabilidad y precisión de la información, por ejemplo un documento de *Word* con hash MD5[153] 22cdmrft546838874mniE32, pero al volver a comprobarlo cambia dicho hash a 22ertyu76883074bcodE32, eso significa que el documento ha sido modificado por alguien, con programas como *Hash Calc*, se puede comprobar la integridad de la información. Por último, la disponibilidad implica que los usuarios puedan acceder a la información cuando ellos quieran[154].

Los delitos de acceso ilícito, interceptación ilícita, ataques a la integridad de los datos y del sistema y abuso de los dispositivos contenidos en el convenio son un claro ejemplo de delitos básicos ya que la triada CID representan bienes jurídicos propios de los delitos informáticos básicos[155], o sea, de naturaleza estrictamente informática.

En el acceso ilícito se atenta contra la confidencialidad, por ende, la privacidad digital; en la interceptación ocurre el mismo caso ya que se ataca la confidencialidad; mientras que los ataques a la integridad de los datos y el sistema que como el nombre del tipo lo establece, es una violación al bien jurídico de la

[152] Artículos 2-6, *Convenio sobre la Ciberdelincuencia*, Serie de Tratados Europeos nº 185, Budapest, 2001, https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802fa41c de 6 marzo de 2022, 16:40 hrs.

[153] "Explicado grosso modo, la función *Hash* no es más que un algoritmo criptográfico aplicado al archivo que nos interese garantizar, el cual nos dará como resultado una cadena alfanumérica única. El más mínimo cambio que pudiera sufrir el archivo alteraría dicha cadena, dándonos como resultado una completamente diferente". Véase. Torné, Kike, *HASH. La función que nos garantiza la autenticidad del archivo*, ATI Spain Tips, 2017, https://www.atispain.com/blog/hash-la-funcion-que-nos-garantiza-la-autenticidad-del-archivo/ de 4 marzo de 2022, 18:40 hrs.

[154] Más adelante se dará una definición más concreta de la Triada CID.

[155] Los delitos informáticos básicos tienen varias características esenciales que los distinguen de los delitos tradicionales y uno de esos elementos distintivos es que cuentan con sus propios bienes jurídicos -Triada CID-, entre otros elementos que se verán en el capítulo 7.

integridad de los datos y los sistemas informáticos -una clara alusión al *software* y *hardware*-.

El abuso de los dispositivos es un raro caso que establece medios por los cuales se pueden cometer el acceso ilícito, interceptación de datos, ataques sobre los datos y los sistemas, por ejemplo: quien a través del *ransomware* provoca ataques a los datos y al propio sistema, pues inutiliza en su totalidad tanto *software* como *hardware*. Para ser más específico es quien produce, vende, obtiene, importe, difunde o cualquier otra forma de puesta a disposición de cualquier dispositivo, programa informático, contraseña, código de acceso o datos informáticos que permitan acceder a una parte o a todo un sistema informático. Sin duda este artículo -abuso de los dispositivos- va relacionado con la accesibilidad o disponibilidad, ya que a través del *ransomware* se atenta contra la disponibilidad, así dado que el abuso de dispositivos atenta contra la disponibilidad.

La falsificación y el fraude informático se encuentran en el título 2, denominado delitos informáticos, artículos 7 y 8 del presente Convenio.

*Título 2. Delitos informáticos.*

**Artículo 7 - Falsificación informática.**

Cada parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno la introducción, alteración, borrado o supresión deliberados e ilegítimos de datos informáticos que genere datos no auténticos con la intención de que sean tomados o utilizados a efectos legales como auténticos, con independencia de que los datos sean legibles e inteligibles directamente. Las partes podrán exigir que exista una intención dolosa o delictiva similar para que se considere que existe responsabilidad penal.

**Artículo 8 – Fraude informático.**

Las partes adoptarán las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno los actos deliberados e ilegítimos que causen perjuicio patrimonial a otra persona mediante:

a. La introducción, alteración, borrado o supresión de datos informáticos;

b. Cualquier interferencia en el funcionamiento de un sistema informático, con la intención dolosa o delictiva, de obtener de forma ilegítima un beneficio económico para uno mismo o para otra persona[156].

El análisis de estos tipos es muy peculiar porque si los anteriores representaban el claro ejemplo de los delitos básicos, el delito de fraude informático es el modelo del delito subordinado[157]. El fraude informático es una derivación del tradicional fraude, pero cometido con medios informáticos, aunque al final se atenta contra el patrimonio físico[158].

En cambio, la falsificación informática como está regulada corresponde más a un delito que atenta contra la CID correspondientemente a la integridad de los datos informáticos. Propiamente la falsificación informática debe estar en el capítulo 1 junto a los anteriores delitos y no en este segundo título -a menos que se le introduzca el carácter económico como finalidad-.

*Título 3 – Delitos relacionados con el contenido.*

**Artículo 9 – Delitos relacionados con la pornografía infantil.**

1. Cada parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno la comisión deliberada e ilegítima de los siguientes actos:
a. La producción de pornografía infantil con la intención de difundirla a través de un sistema informático;
b. La oferta o la puesta a disposición de pornografía infantil a través de un sistema informático;
c. La difusión o la transmisión de pornografía infantil a través de un sistema informático;

[156] Artículo 7-8,*Convenio sobre la ciberdelincuencia*, op, cit.
[157] El delito informático como subordinado del delito tradicional es el medio comisivo en la mayoría de las veces del delito tradicional, por ejemplo, del fraude. Donde pueden representar agravantes o atenuantes e inclusive ser tipos derivados del básico como en el caso del *Computerbetrug* del *Strafgesetzbuch*.
[158] Aunque en nuestra actualidad el patrimonio digital está en su pleno apogeo con la ropa digital; o los propios *NFT*: *"NFT* son las siglas de "*Non-Fungible Token*", "*Non-fungible*" significa que no pueden ser reemplazados por otra cosa. Un billete de un dólar puede ser reemplazado por otro o cambia un bitcoin por otro y tendrás exactamente lo mismo, en valor y liquidez". Trevilla, Manuel, ¿Qué son los NFT y porque todos hablan de ellos?, El Financiero, 2022, https://www.elfinanciero.com.mx/manuel-trevilla-fenomenos-digitales/2022/01/13/nft-tecnologia-basada-en-blockchain-que-es-mas-que-moda/ de 6 marzo de 2022, 12:54 hrs

d. La adquisición, para uno mismo o para otros, de pornografía infantil a través de un sistema informático;
e. La posesión de pornografía infantil en un sistema informático o en un dispositivo de almacenamiento de datos informáticos.

2. A los efectos del párrafo 1 anterior, se entenderá por <<pornografía infantil>> todo material pornográfico que contenga la representación visual de:

a. Un menor adoptando un comportamiento sexualmente explícito;
b. Una persona que parezca un menor adoptando un comportamiento sexualmente explícito;
c. Imágenes realistas que representen a un menor adoptando un comportamiento sexualmente explicito.

3. A los efectos del párrafo 2 anterior, se entenderá por <<menor>> toda persona menor de 18 años. Las partes podrán, no obstante, exigir un límite de edad inferior, que deberá ser como mínimo de 16 años.
4. Las partes podrán reservarse el derecho a no aplicar, en todo o en parte, los apartados d) y e) del párrafo 1 y los apartados b) y c) del párrafo 2[159].

La pornografía infantil pertenece al capítulo 3, denominado delitos relacionados con el contenido. Tal denominación es peculiar, ya que como lo indica hace referencia a lo que contiene el sistema -en este caso puede ser el celular o la computadora-. Este delito es subordinado ya que si se define a la pornografía infantil se puede entender como una representación o descripción gráfica de actividades sexuales en la que participan menores de edad. El mismo artículo de la convención en su párrafo 2 contiene las palabras “todo material pornográfico”, haciendo alusión no solo a lo informático sino también a lo físico, porque en esencia la pornografía infantil es un delito predominantemente físico que se plasma en el ciberespacio, por demás atenta contra bienes jurídicos no pertenecientes a los delitos informáticos autónomos, como el libre desarrollo de la personalidad.

*Título 4 – Delitos relacionados con infracciones de la propiedad intelectual y de los derechos afines.*

**Artículo 10 – Delitos relacionados con infracciones de la propiedad intelectual y de los derechos afines.**

[159] Artículo 9, *Convenio sobre la ciberdelincuencia*, op, cit.

1. Cada parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno las infracciones de la propiedad intelectual que defina su legislación, de conformidad con las obligaciones que haya contraído en aplicación del acta de París de 24 de julio de 1971, por la cual se revisó el Convenio de Berna para la protección de obras literarias y artísticas , del Acuerdo sobre los aspectos de los derechos de propiedad intelectual relacionados con el comercio y del tratado de la OMPI sobre Derechos de Autor, a excepción de cualquier derecho moral otorgado por dichos Convenios, cuando tales actos se cometan deliberadamente, a escala comercial y por medio de un sistema informático.

2. Cada parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno las infracciones de los derechos afines definidas en su legislación, de conformidad con las obligaciones que haya asumido en aplicación de la Convención Internacional sobre la Protección de los Artistas Intérpretes o Ejecutantes, los Productores de Fonogramas y los Organismos de Radiodifusión (Convención de Roma), del Acuerdo sobre los aspectos de los derechos de propiedad intelectual relacionados con el comercio y del Tratado de la OMPI sobre Interceptación o Ejecución y Fonogramas, a excepción de cualquier derecho moral conferido por dichos Convenios, cuando tales actos se cometan deliberadamente, a escala comercial y por medio de un sistema informático.

3. En circunstancias bien delimitadas, toda Parte podrá reservarse el derecho de no imponer responsabilidad penal en virtud de los párrafos 1 y 2 del presente artículo, siempre que se disponga de otros recursos efectivos y que dicha reserva no vulnere las obligaciones internacionales que incumban a dicha Parte en aplicación de los instrumentos internacionales mencionados en los párrafos 1 y 2 del presente artículo[160].

Este artículo es muy interesante debido al crecimiento constante de los derechos del autor y demás derechos correspondientes dentro del campo cibernético. Al abordar los derechos de autor, primero se debe saber lo que es un derecho autor, por lo tanto, la definición de éste es “el que tiene toda persona sobre la obra que produce; y especialmente el que les corresponde debido a las obras de su creación para disponer de ellas por todos los medios que le permita la ley”[161].

[160] Artículo 10, *Convenio sobre la ciberdelincuencia*, op, cit.
[161] Menchaca Córdova, Marcelo, *Derecho informático*, creative commons, Bolivia, 2014, p. 520.

De tal definición se puede desprender un elemento patrimonial que es que la persona que crea cualquier obra tiene derecho a explotarla de las formas en que la ley de cada país se lo permita, por lo tanto, al hablar de derechos de autor, inherentemente se está relacionado con el patrimonio.

Además del contenido patrimonial, los derechos de autor necesitan otros elementos esenciales como la creatividad y la originalidad -referencia clara al inventor-.

Hay otro elemento y que de éste nace la característica que une "espiritualmente" al autor con su creación y es el elemento moral, así originando la división de los derechos de autor en:

1. Derechos morales y;
2. Derechos patrimoniales[162].

Respecto al ámbito nacional mexicano tenemos la Ley Federal del Derecho de Autor, que justamente aborda sobre los derechos morales y patrimoniales[163] y que dentro del mundo informático se protege a los programas de computación y las bases de datos[164].

Por el lado punitivo, se tiene el Código Penal Federal en los artículos 424 al 429 que protegen el lado patrimonial, o sea, el bien jurídico denominado patrimonio. De esta manera es como México, protege los derechos de autor, y que a pesar de no ser parte de dicho Convenio se puede establecer que en la parte de derechos de autor se tiene una sólida defensa para su protección.

[162] Ídem, p. 530.
[163] Artículos 18-29, Ley Federal del Derecho de Autor, https://www.diputados.gob.mx/LeyesBiblio/pdf/122_010720.pdf de 6 de marzo de 2022, 17: 47 hrs.
[164] Artículo 101. "Se entiende por programa de computación la expresión original en cualquier forma, lenguaje o código, de un conjunto de instrucciones que, con una secuencia, estructura y organización determinada, tiene como propósito que una computadora o dispositivo realice una tarea o función específica". Véase. Artículo 101. Ley Federal del Derecho de Autor, op. cit.

### 4.1.2 PROTOCOLO ADICIONAL AL CONVENIO SOBRE LA CIBERDELINCUENCIA RELATIVO A LA PENALIZACIÓN DE ACTOS DE ÍNDOLE RACISTA Y XENÓFOBA COMETIDOS POR MEDIO DE SISTEMAS INFORMÁTICOS

Este protocolo adicional es vital para nuestros tiempos donde imperan las redes sociales a lo cual en éstas abundan los discursos de odio que no son más que el pan de cada día, así convirtiéndose en un lugar poco agradable las redes sociales.

La finalidad de este protocolo adicional es respecto a la tipificación de actos de índole racista y xenófoba cometidos a través de los sistemas informáticos. En cuanto a lo qué significa material racista y xenófobo, se puede encontrar su definición en el artículo 2 que establece lo siguiente:

"por "-material racista y xenófobo-" se entenderá todo material escrito, toda imagen o cualquier otra representación de ideas o teorías, que propugne, promueva o incite al odio, la discriminación o la violencia, contra cualquier persona o grupo de personas, por razón de la raza, el calor, la ascendencia o el origen nacional o étnico, así como de la religión en la medida en que ésta se utilice como pretexto para cualquiera de esos factores"[165].

El protocolo contiene los siguientes delitos:

a) Delitos relacionados con difusión de material racista y xenófobo mediante sistemas informáticos;
b) Delitos relacionados con amenazas con motivación racista y xenófoba;
c) Delitos relacionados con insultos con motivación racista y xenófoba y;

[165] Ministerio de Asuntos Exteriores y de Cooperación. Oficina de Interpretación de Lenguas, *Protocolo adicional al Convenio sobre la ciberdelincuencia relativo a la penalización de actos de índole racista y xenófoba cometidos por medio de sistemas informáticos,* España, 2005, https://www.plataformaong.org/conferencia/wp-content/uploads/2014/10/Protocolo_adicional_convencion_cibercrimen.pdf de 8 noviembre de 2021, 18:09 hrs.

d) Delitos relacionados con negación, minimización burda, aprobación o justificación del genocidio o de crímenes contra la humanidad.

El libro llamado “Los protocolos de los sabios de Sion”, cuyo contenido es antisemita y es uno de los pilares fundamentales que han creado odio hacia la comunidad judía del cual se crean falsas teorías conspiranoicas sobre supuestas reuniones de los sabios de Sion en la que en dichas reuniones éstos detallan los planes de una conspiración judeo-masónica cuyo único objetivo era hacerse con el control mundial y que fue pieza pilar para el pensamiento ideológico de *Hitler*, contra los judíos.

Se menciona este libro porque es difundido a través del internet entre grupos radicales racistas y xenófobos para seguir generando odio hacia la comunidad judía[166], por ende, dicha difusión de tal contenido es constitutivo del delito de difusión de material racista y xenófobo mediante sistemas informáticos.

Continuando con el análisis del protocolo adicional, cada parte deberá adoptar las medidas legislativas y de otro orden que sean necesarias para evitar la difusión de material racista y xenófobo (aquí por ejemplo podemos encontrar la difusión del libro ya anteriormente analizado, Los protocolos de los sabios de Sion); amenazas e insultos con motivación racista y xenófoba; así como la negación, minimización burda, aprobación o justificación del genocidio o de crímenes contra la humanidad.

[166] López, Alfred, *Los falsos textos que desde hace más de un siglo son utilizados para fomentar el odio antisemita*, Yahoo! News, 2021, https://es.noticias.yahoo.com/falsos-textos-que-desde-hace-mas-un-siglo-son-utilizados-para-fomentar-odio-antisemita-144756516.html?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_referrer_sig=AQAAAIh0C1A2L5mMeD-2sngoEml4Tw9BOxPR6_F3jkgVTwe_RFjcMlWgW7b6AyFuv8DZaDNNkScTkNLaH8EhipNK3wcMr2kGhUhllUFc-zjll4UEDYlVxOsRqhLpKQbTiU5V8eBcQHpXeXRjMj9EFhxpLN3L56_n1gGQDNn_ZkgH49Lv de 6 marzo de 2022, 18:00 hrs.

## 4.2 REGULACIÓN NACIONAL

Dentro del marco legal mexicano hay dos leyes esenciales dentro de los delitos informáticos las cuales son:

1) Ley Federal de Protección de Datos Personales en Posesión de los Particulares -en adelante LFPDPPP-;
2) Ley General de Títulos y Operaciones de Crédito -en adelante LGTyOC-.

La LFPDPPP, contiene los delitos informáticos en el capítulo XI, denominado De los delitos en materia del tratamiento indebido de Datos Personales; que van del artículo 67 al 69.

> Artículo 67.- Se impondrán de tres meses a tres años de prisión al que, estando autorizado para tratar datos personales, con ánimo de lucro, provoque una vulneración de seguridad a las bases de datos bajo su custodia.
>
> Artículo 68.- Se sancionará con prisión de seis meses a cinco años al que, con el fin de alcanzar un lucro indebido, trate datos personales mediante el engaño, aprovechándose del error en que se encuentre el titular o la persona autorizada para transmitirlos.
>
> Artículo 69.- Tratándose de datos personales sensibles, las penas a que se refiere este Capítulo se duplicarán[167].

Para analizar estos artículos se debe entender en primer lugar el significado de 1. Datos personales; 2. Base de datos; 3. Datos personales sensibles y; 4. Vulneración de seguridad.

Los datos personales son cualquier información concerniente a una persona física identificada o identificable; la base de datos es el conjunto ordenado de datos personales referentes a una persona identificada o identificable; los datos personales sensibles son aquellos datos personales que afectan a la esfera más íntima de su titular, o cuya utilización indebida pueda dar origen a discriminación o

[167] Artículos 67-69, Ley Federal de Protección de Datos Personales en Posesión de los Particulares, http://www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf de 15 noviembre de 2021, 19:04 hrs. op. cit.

conlleve un riesgo grave para éste y la vulneración de seguridad es la pérdida o destrucción no autorizada; el robo, extravío o copia no autorizada; el uso, acceso o tratamiento no autorizado, o el daño, la alteración o modificación no autorizada[168].

El delito contenido en la LFPDPPP en el artículo 67 se establece:

"Artículo 67.- Se impondrán de tres meses a tres años de prisión al que, estando autorizado para tratar datos personales, con ánimo de lucro, provoque una vulneración de seguridad a las bases de datos bajo su custodia"[169].

Del cual se desprende:

1. Persona autorizada para tratamiento de datos;

2. Ánimo de lucro y:

3. Resultado de vulneración de seguridad a las bases de datos bajo su custodia.

A lo cual la persona autorizada para obtener un lucro crea una vulneración de seguridad a la base de datos, o sea:

I. La pérdida o destrucción no autorizada;
II. El robo, extravío o copia no autorizada;
III. El uso, acceso o tratamiento no autorizado, o
IV. El daño, la alteración o modificación no autorizada.

En el artículo 68 se establece:

"Artículo 68.- Se sancionará con prisión de seis meses a cinco años al que, con el fin de alcanzar un lucro indebido, trate datos personales mediante el engaño, aprovechándose del error en que se encuentre el titular o la persona autorizada para transmitirlos"[170].

---

[168] Los datos personales, datos personales sensibles y la base de datos se encuentran en el artículo 3 de la ley, de donde fueron extraídas sus definiciones; mientras que la vulneración de seguridad fue extraída del reglamento de dicha ley en su artículo 63. Véase. Artículo 3, Ley Federal de Protección de Datos Personales en Posesión de los Particulares, op. cit.

Art. 63, Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de Particulares, https://www.diputados.gob.mx/LeyesBiblio/regley/Reg_LFPDPPP.pdf de 15 de noviembre de 2021, 19:15 hrs.

[169] Artículo 67, Ley Federal de Protección de Datos Personales en Posesión de los Particulares, op. cit.

[170] Artículo 68, Ley Federal de Protección de Datos Personales en Posesión de los Particulares, op. cit.

1. Lucro indebido;

2. Tratar datos personales mediante el engaño, aprovechándose del error en que se encuentre el titular o la persona autorizada para transmitirlos.

Así pudiendo establecer de nuevo el lucro, pero está vez será bajo el tratamiento de datos, o sea, la obtención, uso, divulgación o almacenamiento de datos personales, por cualquier medio.

El uso abarca cualquier acción de acceso, manejo, aprovechamiento, transferencia o disposición de datos personales -artículo 3, fracción XVIII-. Por último, el artículo 69 es una agravante si se llegase a tratar de datos sensibles.

El robo de datos es uno de los delitos más comunes que comete la ciberdelincuencia y que por lo general se ofrecen en grupos privados de las redes sociales o en la propia *dark web* donde se suele manejar mucho más el anonimato; el robo de datos personales se puede hacer por varios métodos pero uno de las comunes es la inyección *SQL*[171] que pertenece a *Kali linux*, simplemente es buscar en el navegador web el siguiente elemento, *inurl php id=*, al ingresar este elemento se mostrarán páginas vulnerables a tal programa -*SQLMAP*- así pudiendo realizar ataques a la bases de datos de las páginas web.

En cuanto a la Ley General de Títulos y Operaciones de crédito se tiene como claro ejemplo de delito informático el artículo 432 que es uno de los delitos informáticos más importantes de esta ley, que establece lo siguiente:

> Artículo 432.- Se sancionará con prisión de tres a nueve años y multa de treinta mil a trescientos mil días multa, al que sin causa legítima o sin consentimiento de quien esté facultado para ello, respecto de tarjetas de servicio, de crédito o en general, instrumentos utilizados en el sistema de pagos, para la adquisición de bienes y servicios, emitidos en el país o en el extranjero, por entidades comerciales no bancarias:

[171] "La inyección de SQL es un tipo de ciberataque encubierto en el cual un hacker inserta código propio en un sitio web con el fin de quebrantar las medidas de seguridad y acceder a datos protegidos. Una vez dentro, puede controlar la base de datos del sitio web y secuestrar la información de los usuarios". Véase. Belcic, Iván, *¿Qué es la inyección de SQL y cómo funciona?,* Avast, 2021, https://www.avast.com/es-es/c-sql-injection de 6 marzo de 2022, 19:00 hrs.

I. Produzca, fabrique, reproduzca, introduzca al país, imprima, enajene, aun gratuitamente, comercie o altere, cualquiera de los objetos a que se refiere el párrafo primero de este artículo;

II. Adquiera, posea, detente, utilice o distribuya cualquiera de los objetos a que se refiere el párrafo primero de este artículo;

III. Obtenga, comercialice o use la información sobre clientes, cuentas u operaciones de las entidades emisoras de cualquiera de los objetos a que se refiere el párrafo primero de este artículo;

IV. Altere, copie o reproduzca la banda magnética o el medio de identificación electrónica, óptica o de cualquier otra tecnología, de cualquiera de los objetos a que se refiere el párrafo primero de este artículo;

V. Sustraiga, copie o reproduzca información contenida en alguno de los objetos a que se refiere el párrafo primero de este artículo, o

VI. Posea, adquiera, utilice o comercialice equipos o medios electrónicos, ópticos o de cualquier otra tecnología para sustraer, copiar o reproducir información contenida en alguno de los objetos a que se refiere el párrafo primero de este artículo, con el propósito de obtener recursos económicos, información confidencial o reservada.

Para los efectos de este capítulo, se entiende por tarjetas de servicio, las tarjetas emitidas por empresas comerciales no bancarias, a través de un contrato que regula el uso de las mismas, por medio de las cuales, los usuarios de las tarjetas ya sean personas físicas o morales, pueden utilizarlas para la adquisición de bienes o servicios en establecimientos afiliados a la empresa comercial emisora[172].

Este tipo está muy relacionado con el *carding,* y que constituye un fraude donde el delincuente se hace de manera ilícita de los datos bancarios de la víctima. Este tipo de ciberdelito se ve muy claramente en los pequeños cargos que a veces se encuentran en las tarjetas bancarias de los usuarios, por ejemplo: las personas que ofrecen *Netflix*, *Spotify*, o cualquier otra aplicación de renta mensual, pagando un precio ínfimo a lo que cuesta la mensualidad, por igual dichos datos bancarios son vendidos a otras personas interesadas así encuadrando su conducta en la fracción III de este artículo.

[172] Artículo 432, Ley General de Títulos y Operaciones de Crédito, http://www.diputados.gob.mx/LeyesBiblio/pdf/145_220618.pdf de 15 noviembre de 2021, 19:30 hrs.

# CAPÍTULO V DERECHO PENAL COMPARADO. ALEMANIA Y CANADÁ

La importancia de conocer no solo el ordenamiento nacional de México sino también el de otros países para comprender y comparar los tipos penales de naturaleza informática con el que cuentan -en este caso Alemania y Canadá-.

Alemania tiene tipos de índole informática como el *Computerbetrug* -Fraude informático-, o la *Verbreitung gewalt oder tierpornographischer Inhalte* - Distribución de contenido violento o pornografía de animales-, entre otros. Mientras que Canadá tiene los *Offences Tending to Corrupt Morals* -delitos que tienden a corromper la moral-.

## 5.1 FRAUDE INFORMÁTICO

"Quien, con el propósito de obtener una ventaja patrimonial antijurídica para sí o para un tercero, perjudica el patrimonio de otro, influyendo en el resultado de un proceso de tratamiento de datos, a través de una errónea configuración del programa, a través del uso de datos incorrectos o incompletos, a través del uso no autorizado de datos, o de otra manera a través de una intervención no autorizada en el proceso, se castiga con privación de libertad de hasta cinco años o con multa"[173].

Este tipo penal se encuentra en el *Strafgesetzbuch - § 263a Computerbetrug* -¯ alemán, y de su análisis se derivan los siguientes puntos:

1. Se puede identificar el bien jurídico que es el patrimonio al establecer una ventaja pecuniaria ilegal ya sea para uno mismo o tercera persona dañando la propiedad de otro;

2. El resultado será a través del procesamiento de datos que no son más que operaciones o actividades que se llevan a cabo sobre datos de ciertos elementos para así obtener un resultado llamado información, donde se distinguen la entrada, proceso y salida;

[173] Balmaceda Hoyos, Gustavo, *El delito de estafa informática en el derecho europeo continental*, Chile, 2011, https://dialnet.unirioja.es/descarga/articulo/4200389.pdf de 13 septiembre de 2021, 12:43 hrs, p. 118.

3. Se pueden distinguir cuatro conductas como a) La errónea configuración del programa; b) El uso de datos incorrectos o incompletos; c) A través del uso no autorizado de datos y; d) A través de una intervención no autorizada en el proceso.

¿Qué es la errónea configuración del programa?, lo que destaca es la palabra programa, por ende, si se está analizando el fraude informático pues entonces la definición que se busca de programa es la de origen informático el cual se define como un "Conjunto unitario de instrucciones que permite a una computadora realizar funciones diversas, como el tratamiento de textos, el diseño de gráficos, la resolución de problemas matemáticos, el manejo de banco de datos, etc."[174]

Es así que como se entendió en el capítulo I, el programa informático puede ser entendido como parte del *software* y es aquí donde se puede citar a *Windows* -sistema operativo- como *software* de sistema -aquello que viene de fábrica, lo más elemental-, mientras que por ejemplo *Zoom*, es *software* de aplicación -programas secundarios-.

Ahora bien, si el resultado es a partir de un proceso de datos que se acabó de definir, entonces, el error residirá en la salida que es la obtención de información falsa mediante la configuración o diseño erróneo del programa, así provocando o manteniendo un error para generar ventaja patrimonial.

El uso de datos incorrectos o incompletos es la segunda forma en el fraude informático, y para entender dicha cuestión, debemos definir lo que es el dato a lo cual se tendrá que remitir a otro delito informático del código penal alemán que es el § 202a *Ausspähen von Daten* -Espionaje de datos-, que define a los datos de la siguiente manera: *"Daten im Sinne des Absatzes 1 sind nur solche, die elektronisch, magnetisch oder sonst nicht unmittelbar wahrnehmbar gespeichert sind oder übermittelt werden"*[175] -Los datos en el sentido del párrafo 1 son solo aquellos que

[174] Real Academia Española, *Diccionario de la lengua española*, 2021, https://dle.rae.es/programa de 14 septiembre de 2021, 15:21 hrs.

[175] § 202a, *Das Deutsche Strafgesetzbuch*, *Deutschland*, 2021, https://www.gesetze-im-internet.de/stgb/__202a.html de 14 septiembre de 2021, 16:32 hrs.

se almacenan o transmiten electrónicamente, magnéticamente o de otra manera de tal manera que no son inmediatamente perceptibles-.

Si el primer error nace de la salida, en este segundo caso se da en la entrada, desde este primer momento se da la introducción de datos falsos o incompletos para después dar un proceso y una salida, por ejemplo, los Comprobantes Fiscales Digitales por Internet (CFDI) que es una factura electrónica, se da la entrada de datos incorrectos o incompletos para ser procesados por los dispositivos electrónicos y dar como salida una factura electrónica falsa.

El uso no autorizado de datos, no corresponde a que, si los datos introducidos están errados o si hay una alteración en los programas, sino más bien la persona física hace uso de datos correctos, pero sin una autorización debida, considerando que aquí se puede ejemplificar con la conducta del *carding*, donde una persona física hace uso de la tarjeta de crédito de un sujeto para hacer compras a su beneficio, este punto es muy importante si se pretende llegar a conocer en mayor profundidad el *carding* como conducta ciber delictiva en México.

Por último, la intervención o influencia no autorizada en el proceso, no hace más que la parte de la manipulación del proceso, por ejemplo, en el que una persona no autorizada tiene influencia en el proceso para dar otro tipo de información en la salida.

## 5.2 DISTRIBUCIÓN DE CONTENIDO VIOLENTO O PORNOGRAFÍA DE ANIMALES

Sección decimotercera.

Delitos contra la autodeterminación sexual.

Sección o artículo 184a. Distribución de contenido violento o pornografía de animales.

Cualquiera que tenga contenido pornográfico (artículo 11 (3)), actos de violencia o actos sexuales de personas con animales será sancionado con prisión de hasta tres años o con una multa al que

1. difunde o pone a disposición del público o

2. fabrica, adquiere, entrega, tiene en stock, ofrece, publicita o se compromete a importarlo o exportarlo para usarlo de acuerdo con el número 1 o para permitir que otra persona lo use de esta manera.

En los casos de la oración número 1, la tentativa es punible[176].

Este delito -*§ 184a Verbreitung gewalt oder tierpornographischer Inhalte*[177]- es muy peculiar debido a que, en la Ciudad de México, dicha conducta no es constitutiva de un delito, sino más bien puede ser prueba para incriminar a un sujeto, pero el poseer, así como distribuir contenido zoofílico no es delito.

Constituye delito cuando el sujeto materializa esa conducta zoofílica contra un animal en el mundo físico, encuadrando su conducta en el capítulo IV, delitos cometidos por actos de maltrato o crueldad en contra de animales no humanos del Código Penal de la Ciudad de México -en adelante CPCDMX-, pero aun así es muy deficiente su encuadramiento ya que las palabras maltrato o crueldad animal son elementos normativos jurídicos que se encuentran en los artículos 350 BIS y 350 TER, de dicho capítulo del CPCDMX, y que nos remitirán a la Ley de Protección de Animales del Distrito Federal para entender lo que es un acto de maltrato o crueldad animal[178].

---

[176] DeepL Traductor, https://www.deepl.com/es/translator de 13 septiembre de 2021, 11:43 hrs.

[177] *Mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe wird bestraft, wer einen pornographischen Inhalt (§ 11 Absatz 3), der Gewalttätigkeiten oder sexuelle Handlungen von Menschen mit Tieren zum Gegenstand hat,*

*1. verbreitet oder der Öffentlichkeit zugänglich macht oder*

*2. herstellt, bezieht, liefert, vorrätig hält, anbietet, bewirbt oder es unternimmt, diesen ein- oder auszuführen, um ihn im Sinne der Nummer 1 zu verwenden oder einer anderen Person eine solche Verwendung zu ermöglichen.*

*In den Fällen des Satzes 1 Nummer 1 ist der Versuch strafbar.* Véase. § 184a, *Das Deutsche Strafgesetzbuch*, op. cit.

[178] ARTÍCULO 350 TER. Al que cometa actos de maltrato o crueldad en contra de cualquier especie animal no humana provocándole la muerte, se le impondrán de dos a cuatro años de prisión y de doscientos a cuatrocientos días multa, así como 150 el aseguramiento de todos los animales que pudiera tener bajo su cuidado o resguardo, en términos de lo dispuesto por el artículo 54 de este Código.

En caso de que se haga uso de métodos que provoquen un grave sufrimiento al animal previo a su muerte, las penas se aumentarán en una mitad.

Se entenderá por métodos que provocan un grave sufrimiento, todos aquellos que lleven a una muerte no inmediata y prolonguen la agonía del animal.

La Ley de Protección de Animales del Distrito Federal en su artículo 24 con sus correspondientes fracciones en ninguna de ellas se establece la zoofilia, a menos que ésta se vea como sinónimo de bestialidad o brutalidad en su fracción V; ya que la zoofilia es conocida bajo esas denominaciones[179].

El derecho penal para la protección de los animales es otro tópico que está en vías de desarrollo como el derecho informático y que aún queda mucho camino por recorrer. Este tipo penal alemán puede servir para una futura reforma en nuestros códigos penales de México, quienes aún no tengan contemplada la figura de distribución de pornografía de animales como delito.

Regresando al tipo penal de Distribución de contenido violento o pornografía de animales se puede observar que es un delito de naturaleza informática ya que dicho delito establece otro artículo que es el 11 (3) del propio *Strafgesetzbuch* que plantea lo siguiente: "Los contenidos en el sentido de las regulaciones que se refieren a este párrafo son aquellos que están contenidos por escrito, en soportes de sonido o imagen, en memorias de datos, imágenes u otras realizaciones o que se transmiten independientemente del almacenamiento por medio de información o tecnología de la comunicación"[180] .

---

Por actos de maltrato o crueldad y lo relativo a este capítulo, se estará a lo dispuesto en la Ley de Protección a los Animales del Distrito Federal.

[179] Artículo 24. Se consideran actos de crueldad y maltrato que deben ser sancionados conforme lo establecido en la presente Ley y demás ordenamientos jurídicos aplicables, los siguientes actos realizados en perjuicio de cualquier animal, provenientes de sus propietarios, poseedores, encargados o de terceros que entren en relación con ellos: I. Causarles la muerte utilizando cualquier medio que prolongue la agonía o provoque sufrimiento; II. El sacrificio de animales empleando métodos diversos a los establecidos en las normas oficiales mexicanas y, en su caso, las normas ambientales; III. Cualquier mutilación, alteración de la integridad física o modificación negativa de sus instintos naturales, que no se efectúe bajo causa justificada y cuidado de un especialista o persona debidamente autorizada y que cuente con conocimientos técnicos en la materia; IV. Todo hecho, acto u omisión que pueda ocasionar dolor, sufrimiento, poner en peligro la vida del animal o que afecten el bienestar animal; V. Torturar o maltratar a un animal por maldad, brutalidad, egoísmo o negligencia grave; VI. No brindarles atención médico veterinaria cuando lo requieran o lo determinen las condiciones para el bienestar animal; VII. Azuzar a los animales para que se ataquen entre ellos o a las personas y hacer de las peleas así provocadas, un espectáculo público o privado; VIII. Toda privación de aire, luz, alimento, agua, espacio, abrigo contra la intemperie, cuidados médicos y alojamiento adecuado, acorde a su especie, que cause o pueda causar daño a un animal; IX. Abandonar a los animales en la vía pública o comprometer su bienestar al desatenderlos por períodos prolongados en bienes de propiedad de particulares; y X. Las demás que establezcan la presente Ley y demás ordenamientos jurídicos aplicables. Véase. Artículo 24, Ley de Protección a los animales de la Ciudad de México, https://paot.org.mx/centro/leyes/df/pdf/2018/LEY_PROTECCION_ANIMALES_04_05_2018.pdf de 13 de septiembre 2021, 20: 34 hrs.

[180] § 11 (3), *Das Deutsche Strafgesetzbuch*, op. cit.

## 5.3 DELITOS QUE TIENDEN A CORROMPER LA MORAL -MATERIALES OBSCENOS-

Parte V. Delitos sexuales, moral pública y conducta desordenada.

Delitos que tienden a corromper la moral.

Materiales obscenos.

163 (1) Comete un delito toda persona que haga, imprima, publique, distribuya, circule o tenga en su poder con fines de publicación, distribución o circulación cualquier material escrito obsceno, fotografía, modelo, disco fonográfico o cualquier otra cosa obscena.

Publicación obscena.

(8) Para los efectos de esta Ley, se considerará obscena toda publicación cuya característica dominante sea la explotación excesiva del sexo, o del sexo, y uno o más de los siguientes temas, a saber, el delito, el horror, la crueldad y la violencia[181].

Este tipo penal perteneciente al artículo 163 (1) (8) del código penal de Canadá es muy significativo en cuanto tiene similitudes con el artículo 227 bis del Código Penal del Estado de México surgido de un lamentable suceso ocurrido en el año de 2020, se realizó una reforma contra los contenidos violentos y que sean parte de una investigación penal para así surgir la llamada "Ley Ingrid"[182].

Artículo 227 Bis.- Al que por cualquier medio y fuera de los supuestos autorizados por la Ley, audiograbe, comercialice, comparta, difunda, distribuya, entregue, exponga, envíe, filme, fotografíe, intercambie, oferte,

[181] *Obscene materials* ***163 (1)*** *Every person commits an offence who makes, prints, publishes, distributes, circulates or has in their possession for the purpose of publication, distribution or circulation any obscene written matter, picture, model, phonograph record or any other obscene thing.*

*Obscene publication*

*(8) For the purposes of this Act, any publication a dominant characteristic of which is the undue exploitation of sex, or of sex and any one or more of the following subjects, namely, crime, horror, cruelty and violence, shall be deemed to be obscene.* Véase. 163 (1), (8), *Criminal Code of Canada*, Canada, 2021, https://laws-lois.justice.gc.ca/eng/acts/c-46/page-23.html#h-118363 de 15 octubre de 2021, 14:21 hrs.

[182] Véase. Artículo 227 bis, Código Penal del Estado de México, http://legislacion.edomex.gob.mx/sites/legislacion.edomex.gob.mx/files/files/pdf/cod/vig/codvig006.pdf de 15 de octubre de 2021, 14:30 hrs.

publique, remita, reproduzca, revele, transmita o videograbe, imágenes, audios, videos o documentos de cadáveres o parte de ellos que se encuentren relacionados con una investigación penal, de las circunstancias de la muerte o de las lesiones que éstos presentan, se le impondrán de tres a seis años de prisión y multa por un importe equivalente de cincuenta a cien veces el valor diario de la unidad de medida y actualización.

Tratándose de imágenes, audios o videos de cadáveres de mujeres, niñas o adolescentes, de las circunstancias de su muerte, de las lesiones o estado de salud, las penas previstas en este artículo se incrementarán hasta en una mitad.

Cuando el delito sea cometido por persona servidora pública integrante de cualquier institución de seguridad pública o de impartición o procuración de justicia, las penas previstas se incrementarán hasta en una tercera parte.

Recientemente, el 12 de julio de 2023 en el periódico oficial Gaceta del Gobierno del Estado de México se publicó la acción de inconstitucionalidad 136/2021 promovente la Comisión Nacional de Derechos Humanos en contra del artículo 227 bis del Código Penal del Estado de México, así siendo declarado invalido puesto que se violaba el principio de seguridad jurídica y legalidad en su vertiente de taxatividad, mínima intervención, libertad de expresión, derecho de las víctimas y ofendidos de un delito a allegarse de material probatorio, regulación sobre inclusiva[183].

Aun así, derivado de su invalidez, no me exime, ni me es prohibido hacer un estudio dogmático comparado de dicho artículo puesto que es un análisis comparativo técnico educativo que no influye en nada el estudio comparativo con el artículo del código criminal de Canadá. Ahora bien, más adelante en mi propuesta se tendrá otra justificación, punto de vista derivado de que propondré un tipo para la Ciudad de México relacionado con el artículo 227 bis del Estado de México.

[183] Véase. Periódico oficial Gaceta del Gobierno y LEGISTEL, Poder Judicial de la Federación, Suprema Corte de Justicia de la Nación, acción de inconstitucionalidad 136/202, https://legislacion.edomex.gob.mx/sites/legislacion.edomex.gob.mx/files/files/pdf/gct/2023/julio/jul121d.pdf de miércoles 12 de julio de 2023, 18:20 horas.

*Tabla 1: Cuadro comparativo del artículo 227 bis del CPEDOMEX y el artículo 163 (1) y (8) del Código criminal de Canadá*

| Características. | Artículo 227 Bis CPEDOMEX. | Artículo 163 (1) y (8) *Criminal Code of Canada*. |
|---|---|---|
| 1. Bien Jurídico. | Contra el respeto a los muertos. | Contra la moral pública. |
| 2. Sujeto activo. | Cualquier persona, con agravante de servidor/a público/a. | Cualquier persona. |
| 3. Sujeto pasivo. | Cadáver, con agravante en mujeres, niñas y adolescentes. | Sociedad. |
| 4. Medios comisivos. | Cualquier medio. | Cualquier medio. |
| 5. Verbos rectores. | audiograbar, comercializar, compartir, difundir, distribuir, entregar, exponer, enviar, filmar, fotografiar, intercambiar, ofertar, publicar, remitir, reproducir, revelar, transmitir o videograbar, imágenes, audios, videos o documentos de cadáveres. | hacer, imprimir, publicar, distribuir, circular, cualquier material escrito obsceno, fotografía, modelo, disco fonográfico o cualquier otra cosa obscena. |

Estas 5 características son las más destacables que se pueden encontrar al comparar dichos tipos penales y que ambas figuras delictivas en su configuración están correctas, pero es mucho más amplio el tipo de Canadá al definir el elemento normativo “obsceno”, abarcando conductas como la apología al delito, zoofilia, pornografía bastante gráfica, etc. Mientras que el tipo de México es más restrictivo ya que se limita al contenido de extrema violencia denominado “*gore”*.

Otra característica vital es el bien jurídico en cuanto se concuerda con el bien jurídico del Código penal del Estado de México, ya que el bien jurídico del *Criminal Code* canadiense es mucho más amplio en cuanto a la moral pública, y sí, este tipo de material afecta a la sociedad, pero en mayor grado a la víctima directa como indirecta, es por eso que se concuerda en mayor medida con el primer código -Estado de México-, solo que en vez de respeto a los cadáveres seria como bien jurídico la dignidad digital, así abarcando no solo a la víctima directa, sino también la víctima indirecta como sus familiares.

Por igual al modificar el bien jurídico también se modifica el sujeto pasivo, ya que, para el Estado Mexicano, es el cadáver, mientras que, para el Estado Canadiense, es la sociedad, pero con este cambio que se acaba de establecer, lo más correcto es que los sujetos pasivos sean tanto quien sufre el daño como el que lo resiente. En cuanto a los medios comisivos lo puede hacer un delito mixto, o sea, de características físicas como en el ciberespacio, porque cuenta con su propio bien jurídico de naturaleza informática.

# CAPÍTULO VI RESPONSABILIDAD PENAL DE LA EMPRESA EN LOS DELITOS INFORMÁTICOS

El derecho penal no es ajeno a la evolución en todos los ámbitos de la vida del humano. El progreso ha hecho que la tecnología se vuelva pilar del humano individual como organizativo -hablando desde el aspecto de la empresa- así volviendo inherente la cibernética con la empresa, el uso de la electrónica y los componentes lógicos se han vuelto elementos esenciales para que las empresas puedan cumplir con sus tareas del día a día.

Desde elaborar inventarios de las ventas realizadas en el día hasta la creación y resguardo de la base de datos de los clientes y la propia ciberseguridad de la empresa para evitar ser sujetos pasivos de los ciberdelincuentes son tareas sustanciales que se deben implementar en toda empresa.

El robo de datos es uno de los delitos más comunes que sufre todo tipo de empresa por parte de los delincuentes informáticos[184] y resulta indispensable tomar políticas para reducir lo más posible que se cometan esta clase de delitos mediante la creación del *compliance penal*.

## 6.1 LA FUNCIÓN DEL COMPLIANCE PENAL EN LOS DELITOS INFORMÁTICOS

"El *Compliance* es un conjunto de herramientas de carácter preventivo, que tienen por objeto garantizar que la actividad que realiza la empresa y quienes la conforman y actúan en su nombre lo hagan en apego a las normas legales, políticas internas, Códigos Éticos sectoriales y cualquier otra disposición que la misma esté

[184] Recientemente la empresa Mercado Libre, sufrió un hackeo que dio como resultado el acceso a la base de datos de 300,000 clientes. Aunque derivado de lo anterior la empresa aseguró que del acceso que hubo a los datos de los clientes no se encontró evidencia de robo ni filtración de éstos. Véase. Página 12, *Hackean datos Mercado Libre y Mercado Pago y hay preocupación por la filtración de datos de 300 mil usuarios*, 2022, https://www.pagina12.com.ar/406594-hackean-datos-mercado-libre-y-mercado-pago-y-hay-preocupacio de 10 marzo de 2022, 17:32 hrs.

obligada a cumplir o que haya decidido hacerlo de forma voluntaria, como parte de sus buenas prácticas"[185].

De la definición se desprenden elementos esenciales como:

1. El apego a las normas legales. De donde se puede tener como fundamento de nuestras leyes mexicanas el artículo 421 en su párrafo primero del Código Nacional de Procedimientos Penales -en adelante CNPP- que establece lo siguiente:

CAPÍTULO II

PROCEDIMIENTO PARA PERSONAS JURÍDICAS

Artículo 421. Ejercicio de la acción penal y responsabilidad penal autónoma.

Las personas jurídicas serán penalmente responsables, de los delitos cometidos a su nombre, por su cuenta, en su beneficio o a través de los medios que ellas proporcionen, cuando se haya determinado que además existió inobservancia del debido control en su organización. Lo anterior con independencia de la responsabilidad penal en que puedan incurrir sus representantes o administradores de hecho o de derecho[186].

Este artículo es el pilar de la responsabilidad para las personas jurídicas y el *compliance penal,* de donde se desprenden partes sustanciales como:

a) Delitos cometidos a su nombre;
b) Delitos cometidos por su cuenta;
c) Delitos cometidos en su beneficio;
d) Los medios que ellas proporcionen, así como;
e) La inobservancia del debido control en su organización.

[185] Garberí Penal, Boutique especializada en Derecho Penal, Compliance y Defensa Legal, *¿Qué es el compliance penal?*, 2017, https://www.garberipenal.com/corporate-programa-compliance-penal/ de 10 marzo de 2022, 17:40 hrs.
[186] Artículo 421, Código Nacional de Procedimientos Penales, https://www.diputados.gob.mx/LeyesBiblio/pdf/CNPP_190221.pdf de 10 marzo de 2022, 18:03 hrs.

Estos cuatro elementos serán base para el quinto que es propiamente el *compliance penal* -Debido control en la organización- a través de la creación de indicadores para saber a qué clase de delitos está expuesta la empresa.

Para la Doctora Erika Bardales Lazcano, el *compliance penal*, se debe aplicar en tres momentos diversos los cuales son:

1. Realización;
2. Mejora continua y;
3. Defensa de la empresa ante un hecho penal[187].

La realización es el punto clave para la elaboración del *compliance*, debido al siguiente punto que nos proporciona la definición:

2. Las políticas internas, Códigos Éticos sectoriales y cualquier otra disposición que la misma esté obligada a cumplir o que haya decidido hacerlo de forma voluntaria, como parte de sus buenas prácticas.

Este punto es casuístico debido a que el *compliance penal* debe contener documentos *sine qua non* como el código de ética, políticas de prevención, canal de denuncias, entre otros.

Es así que durante su realización es obligación llevar a cabo el diagnóstico y dentro de éste se deberá cumplir con el análisis y creación de indicadores conforme a los tipos penales y que en este caso son los de naturaleza informática, pero no sin antes haber analizado el fuero de la empresa debido a que la responsabilidad de la persona jurídica de la empresa es *numerus clausus* respecto a los tipos del orden federal[188], mientras que en el orden local se regirá bajo los códigos penales

[187]Dra. Bardales Lazcano, Erika et al, ***Mesa 1: "COMPLIANCE"***, II Congreso Internacional Virtual de Derecho Penal, 2021, https://fb.watch/bGnSrE7Lyj/ de 10 marzo de 2022, 18:14 hrs.

[188] Los delitos que puede cometer la empresa en el orden federal se encuentran en el código penal federal en el artículo 11 bis de donde destacan delitos como Fraude, Encubrimiento, Operaciones con recursos de procedencia ilícita, contra el ambiente, en materia de derechos de autor, entre otros. En cuanto al principio de *numerus clausus*, como su nombre lo indica son un número cerrado de tipos penales que puede cometer la empresa -en este caso en concreto-, en contrasentido sería el *numerus apertus*. Aunque el principio *numerus clausus* radica principalmente en la naturaleza de los delitos, para eso solo una clase de delitos se pueden cometer de naturaleza culposa. Véase. Artículo 19, Código Penal para la Ciudad de México, https://www.congresocdmx.gob.mx/media/documentos/9cd0cdef5d5adba1c8e25b34751cccfdcca80e2c.pdf de 17 de noviembre de 2022, 20:01 hrs.

locales -dependiendo de cada código local se sabrá si es *numerus clausus* o *apertus* respecto de los delitos que puede cometer la empresa-.

Teniendo giro comercial y fuero se analizarán y crearán los indicadores por tipo informático con base en bien jurídico, de donde se desprenderán preguntas vitales como:

1. ¿La empresa puede cometer delitos informáticos a su nombre?;
2. ¿La empresa puede cometer delitos informáticos por su cuenta?;
3. ¿La empresa puede cometer delitos en su beneficio? y;
4. ¿La empresa puede proporcionar medios para cometer delitos de naturaleza informática?[189]

Con la creación del *compliance penal*, se protege a la empresa mediante su debido control en su organización. Es por eso por lo que los tipos penales informáticos son importantes para la creación del cumplimiento penal y así reducir al máximo que la persona jurídica sea sujeto pasivo o activo de delitos informáticos mediante la realización, la mejora continua y la defensa de la empresa para la atenuación o exoneración de la persona jurídica.

## 6.2 ARTÍCULO 12. CONVENCIÓN DE BUDAPEST

El artículo 12 del convenio de Budapest,[190] establece que:

**Artículo 12 – Responsabilidad de las personas jurídicas**

[189] Desde un punto de vista objetivo la empresa no delinque, pero sí la persona que pertenece a ella, pero eso no exime que la persona jurídica no tenga una sanción por no haber observado su compliance penal -he ahí la importancia de éste-

[190] Convenio ya analizado en el capítulo 3, respecto a los tipos de carácter informático los cuales eran:

a) Acceso ilícito;
b) Interceptación ilícita;
c) Ataques a la integridad de los datos;
d) Abuso de los dispositivos;
e) Falsificación informática;
f) Fraude informático;
g) Delitos relacionados con la pornografía infantil y;
h) Delitos relacionados con infracciones de la propiedad intelectual y de los derechos afines.

1. Cada parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para que pueda exigirse responsabilidad a las personas jurídicas por los delitos previstos en aplicación del presente Convenio, cuando éstos sean cometidos por cuenta de las mismas por una persona física, ya sea a título individual o como miembro de un órgano de dicha persona jurídica, que ejerza funciones directivas en su seno, en virtud de:

a. Un poder de representación de la persona jurídica;
b. Una autorización para tomar decisiones en nombre de la persona jurídica;
c. Una autorización para ejercer funciones de control en el seno de la persona jurídica.

2. Además de los casos previstos en el párrafo 1 del presente artículo, Cada parte adoptará las medidas las medidas necesarias para garantizar que pueda exigirse responsabilidad a una persona jurídica cuando la ausencia de vigilancia o de control por parte de cualquier física mencionada en el párrafo 1 haya permitido la comisión de un delito previsto en aplicación del presente Convenio por una persona física que actúe por cuenta de dicha persona jurídica y bajo su autoridad.
3. Dependiendo de los principios jurídicos de cada Parte, la responsabilidad de una persona jurídica podrá ser penal, civil o administrativa.
4. Dicha responsabilidad se entenderá sin perjuicio de la responsabilidad penal de las personas físicas que hayan cometido el delito[191].

Del análisis de este presente artículo se desprenden cuestiones muy interesantes que concuerdan con nuestras leyes mexicanas respecto de la responsabilidad penal para las personas jurídicas como:

1. Se reconoce responsabilidad penal, civil o administrativa por parte de la empresa cuando la persona física ya sea como ente individual o miembro de un órgano de dicha empresa cometa un delito del presente convenio, los cuales son:
   a) Acceso ilícito;
   b) Interceptación ilícita;
   c) Ataques a la integridad de los datos;
   d) Abuso de los dispositivos;
   e) Falsificación informática;
   f) Fraude informático;

[191]Artículo 12, *Convenio sobre la ciberdelincuencia*, op, cit.

g) Delitos relacionados con la pornografía infantil y;
h) Delitos relacionados con infracciones de la propiedad intelectual y de los derechos afines.

2. "Ausencia de vigilancia o de control" hace alusión al *compliance penal* de donde destaca el *compliance officer*, quien es la persona encargada de velar, vigilar o controlar el cumplimiento penal;
3. "Permitido la comisión de un delito", se desprende la figura del garante -desde altos directivos, oficial de cumplimiento o cualquier empleado perteneciente a la empresa como organización que afronta riesgos-;
4. "Que actúe por cuenta de dicha persona jurídica y bajo su autoridad". Este punto recalca uno de los elementos fundamentales que se deben analizar en el análisis y creación de indicadores en su forma de intervención delictiva[192] durante la realización de compliance penal y;
5. La responsabilidad de la empresa será sin perjuicio de la responsabilidad penal de las personas físicas que hayan cometido el delito. De esta última cuestión se puede inferir la diferenciación de sanción penal de la persona jurídica a la física.

Estos 5 puntos son esenciales dentro de toda responsabilidad para la persona jurídica y que es destacable que el Convenio de Budapest desde que entró en vigor en 2004 ya trataba con toda claridad la responsabilidad penal en contra de la empresa por delitos de carácter informático, así trayendo como resultado que desde el momento de la creación del *compliance* toda empresa deberá analizar los tipos contenidos en el presente convenio y que a pesar de que nuestro país no es Parte de dicho documento legal pueden servir como guía para el establecimiento de los bienes jurídicos de naturaleza informática[193], así como la comparación de los tipos de las leyes nacionales con los del convenio.

[192] a) Delitos cometidos a su nombre;
b) Delitos cometidos por su cuenta;
c) Delitos cometidos en su beneficio; y
d) Los medios que ellas proporcionen.

[193] De donde predomina la Triada CID como bienes jurídicos de naturaleza informática.

## 6.3 BIENES JURÍDICOS INFORMÁTICOS DURANTE LA REALIZACIÓN DEL *COMPLIANCE*

De los fundamentos anteriores se ha vuelto común el primer paso de los tres momentos en la aplicación del *compliance penal* que es la realización propiamente. Una de las principales tareas dentro de la realización es el análisis y creación de indicadores y es aquí donde destaca la creación de una tabla conforme a bienes jurídicos contenidos en el Código Penal Federal y en los locales donde ejerza su giro la empresa -he ahí la importancia de conocer el fuero de ésta-.

Por ejemplo, el bien jurídico de la vida y la integridad corporal entran los delitos de: 1. Homicidio; 2. Lesiones; 3. Ayuda o inducción al suicidio; 4. Aborto y; 5. Feminicidio[194]. En el caso del bien jurídico de la libertad personal tenemos el: 1. Secuestro; 2. Privación de la libertad personal; 3. Privación de la libertad con fines sexuales; 4. Desaparición forzada de personas; 5. Tráfico de menores y; 6. Retención y sustracción de menores o incapaces.

En el caso del análisis de los bienes jurídicos informáticos se tendrá que partir de la Triada CID para localizar inmediatamente dichos bienes -esencia de los delitos básicos-, y en segundo lugar partir de bienes jurídicos tradicionales para la localización de otros delitos informáticos -delitos subordinados-. De dicho estudio se puede desprender delitos como violación de la comunicación privada, fraude, extorsión, acceso ilícito a sistemas y equipos de informática, ciberacoso, entre otros.

Derivado de lo anterior, se propone la siguiente tabla desde un punto de vista enunciativo y educativo, pero no limitativo, por demás se utilizarán tipos del Código penal de la Ciudad de México, Yucatán, el Código penal Federal, entre otras leyes[195].

[194] En el caso del feminicidio hay un concurso de bienes jurídicos el cual hace que este delito encuadre en la vida y dignidad, bienes jurídicos de distinta índole, pero dicho concurso es elemento esencial para distinguir al homicidio del feminicidio.
[195] El Código penal de Yucatán será utilizado debido a que es uno de los mejores códigos penales del país en tener una regulación de los delitos informáticos.

*Tabla 2: Cuadro ilustrativo y educativo de los tipos en la elaboración de un compliance penal*

| Bien jurídico | Artículo |
|---|---|
| **Confidencialidad digital.**<br><br>Se puede entender a la confidencialidad digital como el derecho que todo cibernauta -ente privado o público- tiene para decidir qué tipo de contenido, datos quiere hacer públicos y cuáles no. | 181 Quintus, 213 y 334 del Código Penal de la Ciudad de México.<br><br>243 bis 2, 243 bis 3, 243 bis 6, 243 bis 7 y 243 bis 10 del Código penal de Yucatán.<br><br>211 BIS-1 párrafo 2; 211 BIS-2 párrafo 2 y 3; 211 BIS-3 párrafo 2 y 3; 211 BIS-4 párrafo 2 y 211 BIS-5 párrafo 2 del Código Penal Federal |
| **Integridad digital.**<br><br>Todos los datos deben mantenerse íntegros y nadie que no esté autorizado debe modificarlos o destruirlos.<br><br>**Disponibilidad digital.**<br><br>Los usuarios puedan disponer de la información cada momento que lo requieran | 243 bis 5; 243 bis 6; 243 bis 8 y 243 bis 9 del Código penal de Yucatán;<br><br>211 BIS-1 párrafo 1; 211 BIS-2 párrafo 1; 211 BIS-3 párrafo 1; 211 BIS-4 211 párrafo 1; 211 BIS-5 párrafo 1 del Código Penal Federal. |
| **Patrimonio.**<br><br>Conjunto de bienes, derechos y obligaciones que conforman una universalidad perteneciente a una persona física o jurídica. | 230 fracción XIV y 236 del Código Penal de la Ciudad de México;<br><br>424 bis del Código Penal Federal;<br><br>223 de la Ley de la Propiedad Industrial;<br><br>112 bis, Quáter, 113 Bis de la Ley de Instituciones de Crédito; |

| | |
|---|---|
| | 432, 433 y 434 de la Ley General de Títulos y Operaciones de Crédito. |
| **Dignidad.**<br><br>Reconocimiento al prójimo como merecedor de respeto y reconocimiento. | 179 bis del Código Penal de la Ciudad de México;<br><br>243 bis 12 del Código Penal de Yucatán; |

De la anterior tabla se desprende que la Confidencialidad, Integridad y Disponibilidad son los bienes jurídicos predominantes en los delitos informáticos como delitos básicos, mientras que los bienes jurídicos como el patrimonio y la dignidad son bienes tradicionales de donde solo la tecnología e informática son medios de los delitos tradicionales, por ende, subordinados[196], por lo tanto, en los delitos como subordinados su análisis dentro de la realización del *compliance* no representará algún problema porque se analiza el delito como un todo y no por agravantes, atenuantes o medios.

[196] Es importante dejar en claro, que dicho cuadro contiene algunos tipos de carácter informático que no son parte propiamente de la elaboración formal de un compliance penal -he ahí el carácter educativo-, por ende, se estableció desde los primeros puntos que al momento de la elaboración de un compliance penal primeramente se debe delimitar el fuero de la empresa y de ahí partir al análisis de la responsabilidad para saber si es clausus o apertus ésta. No se pueden mezclar tipos de diferentes entidades federativas, por ejemplo, si la empresa solo radica en Yucatán, se hará un compliance basado en el código penal de dicha entidad federativa, pero si dicha empresa tiene filiales en otros estados, dichas filiales deberán por igual elaborar su propio compliance conforme al código penal de donde se ubican para limitar la responsabilidad y no afecte a la matriz.
Además, para la realización de este presente capítulo 6 se tuvo como base, referencia la siguiente obra inédita de la Dra. Erika Bardales Lazcano. Bardales Lazcano, Erika, *Metodología para la realización de un compliance penal en México. Propuesta* (libro inédito), 2021.

# CAPÍTULO VII PROBLEMÁTICAS DE LA REGULACIÓN JURÍDICA EN EL MUNDO INFORMÁTICO

Aún hay muchos retos para la regulación del ciberespacio y este trabajo está siendo una modesta parte de todo lo que integra el mundo de las crecientes tecnologías. Derivado de esto aún quedan muchos temas por comprender y uno de ellos es el problema de la Autoría y participación -*Täterschaft und Teilnahme*- no tanto por su solución jurídica si no por los resultados que producen.

Otro punto esencial es que toda regulación jurídica al ciberespacio en su mayoría de veces conlleva una restricción a los Derechos Humanos, o al menos se piensa eso, y, por último, no se ha desarrollado aún con grandes creces el estudio dogmático en el campo informático.

## 7.1 EL PROBLEMA DE LA AUTORÍA EN EL CIBERESPACIO

La autoría dentro del derecho penal mexicano[197]se divide en:

a) Autoría inmediata. Quien ejecuta el hecho por sí mismo;
b) Autoría mediata. Quien instrumentaliza la voluntad de otro y se sirve de él para delinquir y;
c) Coautoría. Quienes actúan conjuntamente para delinquir.

Dentro de la participación tenemos:

a) Partícipe inductor. Quien determina dolosamente al autor a cometer el delito;

b) Complicidad. Quien dolosamente presta ayuda o auxilio al autor para cometer el delito.

En la participación, la figura central es el participe inductor -lo que se conoce erróneamente como autor intelectual- y que para el Dr. Francisco Pavón

[197] Véase. Artículo 22, Código Penal para la Ciudad de México, op. cit.

Vasconcelos, la inducción o instigación comprende, como subclases: a) El mandato; b) La orden; c) La coacción; d) El consejo, y f) La asociación[198].

En la autoría, destaca la figura de autoría mediata donde predomina la instrumentalización de la voluntad y que "se entiende en sentido estricto que la realización de la conducta punible es obra del "hombre de atrás", que se vale de quien ejecuta la conducta punible. Es por ello por lo que se considera que el delito es obra suya, porque lo realiza como propio. En este sentido, el ejecutor material de la conducta, instrumento, no es autor penalmente responsable; si lo fuera estaríamos en el caso de la coautoría, o de un autor directo con un determinador detrás suyo, de un autor directo con un cómplice. Por ello, en este caso quien obra como instrumento no es penalmente responsable porque no puede imputársele la realización del tipo por ausencia de conocimiento o por ausencia de voluntad"[199].

La autoría mediata forma parte de la teoría del dominio del hecho y se da mediante el dominio de la voluntad a través del:

a) Error;
b) Coacción;
c) Inimputables y;
d) Aparatos organizados de poder -especialmente este último inciso es parte de la teoría mediata del Dr. Claus Roxin-[200].

Dentro del mundo informático se puede encontrar una forma muy clara de autoría y participación que es a través de la ciberguerra, donde encuadran los atacantes organizados ya sean como delincuentes informáticos externos o internos. En este caso el tema se centrará en los atacantes organizados en cuanto a terroristas y patrocinados por parte del Estado que son parte fundamental de la *cyberwarfare*.

[198] Pavón Vasconcelos, Francisco, op. cit., p. 701.
[199] Escuela Judicial Rodrigo Lara Bonilla, *Teoría del Delito*, Colombia, 2010, p.96.
[200] Zambrano Pasquel, Alfonso, *La Teoría de la Autoría Mediata del Profesor Claus Roxin*, 2015, https://www.youtube.com/watch?v=c58MiMMp0zw de 13 marzo de 2022, 21:00 hrs.

La *cyberwarfare* o ciberguerra es el uso de tecnologías para atentar contra la estructura informática (desmantelar o inhabilitar) de un país, en especial su estructura crítica entendida como elementos esenciales que son parte de los Estados para el mantenimiento de actividades vitales, cuyo daño o destrucción afectaría gravemente al Estado y a su población.

Se tienen ejemplos de ataques a infraestructuras críticas como *Stuxnet* que atentó contra infraestructura crítica de Irán, en este caso sus plantas nucleares[201]. Otro ejemplo es el de un delincuente informático que accedió de manera ilícita al sistema de tratamiento de agua de *Oldsmar*, Florida, aumentando los niveles de hidróxido de sodio, por suerte un encargado se dio cuenta a tiempo y lograron establecer los niveles químicos debidos[202], pero de haber ocurrido tal suceso tal vez estamos hablando de lesiones e inclusive homicidios a través de sistemas informáticos. Este caso es el más vivo ejemplo de que se pueden cometer tentativas o delitos consumados de lesiones u homicidios a través de medios informáticos y se verán muchos más ejemplos con los vehículos autónomos en un futuro no muy lejano.

Continuando con el tema de autoría y participación, se propone el caso *Cloud Hopper* que se presume es un caso de delincuencia cibernética por parte de un grupo denominado APT10 y que son financiados por el propio gobierno chino con el fin de obtener datos de los clientes de las empresas encargadas de servicios gestionados[203].En este caso podemos establecer una autoría mediata por aparatos organizados de poder -*Mittelbare Täterschaft Kraft organisatorischer Machtapparate*-.

En cuanto a la autoría mediata por aparatos organizados se tiene por presupuestos:

---

[201] Caso ya analizado en el capítulo 1 y debidamente sustentando.

[202] Vera, Amir, et al., *Alguien trató de envenenar con lejía a la población de una ciudad de Florida hackeando el sistema de tratamiento de agua, dice el sheriff*, 2021, https://cnnespanol.cnn.com/2021/02/08/florida-envenenar-lejia_oldsmar/ de 20 noviembre de 2021, 15:32 hrs.

[203] Resiliente Digital, *Cloud Hopper: La pesadilla de ciberespionaje chino que nunca acaba*, 2020, https://resilientedigital.com/cloud-hopper-la-pesadilla-de-ciberespionaje-chino-que-nunca-acaba/ de 13 marzo de 2022, 14:54 hrs.

a) El que da la orden tiene que ejercer poder de mando en el marco de la organización;
b) La organización tiene que haberse separado del derecho en el ámbito de sus actividades relevantes para el derecho penal y;
c) El ejecutante individual tiene que ser reemplazable (fungible), de manera que, en caso de que no actuare, otro ocuparía su lugar[204].

En el *Cloud Hopper* es dable identificar como autores mediatos a quienes tienen dominio del hecho por parte del gobierno chino como autores mediatos -siendo que lo lleven a cabo sirviéndose de otro como instrumento- y a quienes ejecutan el delito, o sea, los atacantes organizados patrocinados por el Estado, como autores directos -lo realicen por sí- porque son autores inmediatos aun así cuando hayan actuado por encargo e interés de otro.

Otro punto de suma importancia es de los resultados que producen, pues en el caso de la pornografía infantil, sus efectos son permanentes hasta que no se encuentre la forma de eliminar ciertos contenidos de internet de manera permanente, algo que hasta el momento es imposible de conseguir.

En el caso de México, las imágenes de una chica que fue víctima de feminicidio y que de tan lamentable suceso surgió una reforma en el Estado de México para punibilizar conductas como la difusión de contenido de cadáveres y que hasta la actualidad las imágenes se pueden encontrar en el internet a pesar de que son constitutivas de delito[205].

En síntesis, a pesar de que ya existen los tipos penales correspondientes a estas conductas, la efectividad de la aplicación de estos, como una correcta investigación sobre los hechos es algo que falta por lograr.

[204] Díaz Aranda, Enrique y Roxin, Claus, op. cit., p. 541.
[205] Morán Breña, Carmen, *La "Ley Ingrid" se aprueba antes de que se resuelva el "caso Ingrid"*, El País, 2021, https://elpais.com/mexico/2021-02-25/la-ley-ingrid-se-aprueba-antes-de-que-se-resuelva-el-caso-ingrid.html de 13 marzo de 2022, 16:07 hrs .

El caso -Ingrid- es reflexivo para la victimología y los Derechos Humanos Digitales como el derecho al olvido[206], pues hasta cierto punto la persona seguirá siendo víctima hasta que dicho contenido no desaparezca del internet, o sea, morirá como víctima y mucho más allá del deceso se atentará contra su dignidad y su derecho al olvido al seguir con la difusión de las imágenes.

Lo antes expuesto demuestra que la autoría y participación es un gran problema al momento de producir sus resultados, ya sea bajo cualquier modalidad desde quien produce el delito por sí mismo hasta quien lo auxilie; y esta situación se agrava en gran medida cuando los resultados que se ocasionan por internet son devastadores y se unen al infinito mundo ciberespacial.

## 7.2 A MAYOR SEGURIDAD Y REGULACIÓN JURÍDICA EN EL MUNDO INFORMÁTICO MÁS VULNERACIÓN A LOS DERECHOS HUMANOS

Otro tema de reflexión es propiamente la ciberseguridad, sobre qué tanto se está dispuesto a sacrificar la libertad de expresión y privacidad digital por seguridad. Casos ya expuestos como el proyecto *Identify and Disrupt* -identificar e interrumpir- de Australia y el caso PANAUT de México son ejemplos claros de combate a la ciberdelincuencia, pero a la vez parecieran ser modelos de censura en el internet.

Es así como se deberá dar un repaso a los derechos humanos en sus generaciones para comprender que actualmente ante el uso constante de la

[206] El derecho al olvido digital es un derecho de nueva data debido al creciente uso del internet. Nuestra vida en internet forma parte de una consciencia colectiva. Para la Maestra Elvia Celina Guerrero Santillán, el derecho al olvido es "la posibilidad de retirar información personal publicada en internet, cuando el titular de esos datos personales lo estime pertinente". Véase. Guerrero Santillán, Elvia Celina, El derecho al olvido digital en México, https://www.itei.org.mx/v3/micrositios/cdc/wp-content/uploads/2020/04/7_2018_7_guerrero.pdf de 20 de noviembre de 2022, 10:13 hrs.
En materia penal se puede ejemplificar el derecho al olvido digital con las medidas de protección respecto a la eliminación, interrupción, bloqueo o destrucción de imágenes, audios o todo contenido multimedia relacionado con la víctima, Véase. Artículo 72 TER fracción II, Ley de acceso de las mujeres a una vida libre de violencia de la Ciudad de México, https://paot.org.mx/centro/leyes/df/pdf/2021/LEY_ACCESO_MUJERES_VIDA_LIBRE_VIOLENCIA_GOCDMX_02_09_2021.pdf de 20 de noviembre de 2022, 10:30 hrs.
Aunque, ¿verdaderamente son efectivas tales medidas?, el lamentable caso de un feminicidio ocurrido en 2020 cuyas imágenes dieron origen a una reforma en el Código penal del Estado de México siguen siendo divulgadas hasta hoy en día y fácilmente encontradas en la web superficial debido al hecho de las descargas.
El derecho al olvido digital será infructuoso mientras no se tengan las herramientas suficientes que identifiquen a quienes descargan y divulgan contenidos constitutivos de un delito… dando como resultado la lucha constante entre el derecho a la privacidad contra una mayor seguridad en el ciberespacio.

tecnología y el internet está saliendo de nuevo a tema de discusión una cuarta generación de derechos humanos, así como la sección 230 *Communications Decency Act* -Ley de Decencia en las Comunicaciones- que protege a las grandes empresas de las redes sociales ante los posibles delitos que se puedan cometer en las plataformas del internet y que países como Rusia están imponiendo sanciones a redes sociales encuadrando sus acciones a tipos penales, mientas que en el caso de China se cuenta con el gran escudo dorado y con un internet nacional (limitando el libre acceso al internet, pero otorgando una mayor seguridad al ciudadano chino) así pudiendo tal vez delimitar el ámbito espacial en el que podría actuar el derecho penal de un país.

### 7.2.1 LA CUARTA GENERACIÓN DE LOS DERECHOS HUMANOS

Los Derechos Humanos se dividen en tres generaciones las cuales son:

a) Primera generación: Son denominados derechos civiles y políticos y surgieron con la revolución francesa, siglo XVIII; entre los Derechos Humanos de primera generación podemos encontrar; el derecho a la vida; a la libertad y seguridad; a votar y ser votado; libertad de expresión; etc.
b) Segunda generación: Son denominados derechos económicos, sociales y culturales y éstos se deben a la revolución industrial que data de mediados del siglo XVIII; de entre dichos derechos podemos encontrar el derecho a la salud; educación; trabajo; nivel digno de vida, seguridad social; etc.
c) Tercera generación: Son denominados derechos colectivos, del pueblo o la solidaridad, dicha tercera generación empieza a surgir a finales del siglo XX con la finalidad de establecer la necesidad de cooperación entre las naciones para vivir en paz basándose en que la humanidad es un todo, así como lograr también el progreso social y elevar el nivel de vida, por eso aquí se encuentran los derechos ambientales; entre dichos derechos podemos encontrar el derecho a un medio ambiente saludable, a la paz, a

la identidad nacional, derecho de las minorías; la libre autodeterminación de los pueblos indígenas; etc[207].

Los Derechos humanos relacionados con la tecnología forman parte de la cuarta generación y es muy interesante saber que existe un convenio contra la ciberdelincuencia, pero no una Declaración Universal sobre los Derechos Humanos en el Ciberespacio, a pesar de que en 1997 hubo un primer proyecto con el nombre de Declaración de los Derechos Humanos en el Ciberespacio, propuesto por *Robert B. Gelman*[208].

De todo lo anterior entonces se puede empezar a abordar sobre una futura cuarta generación enfocada en la tecnología, especialmente los derechos que nos ofrece ésta como la CID -Confidencialidad, Integridad y Disponibilidad-. así anteponiendo como primeros derechos humanos digitales la propia Confidencialidad, Integridad y Disponibilidad digital de los datos informáticos.

Otros ejemplos son la libertad de prensa y expresión o la privacidad de las comunicaciones, aunque estos derechos son parte de la primera generación solo cambia el medio por el cual se transmite la libertad de expresión y el cómo se protege la comunicación y que está totalmente ligada a la confidencialidad, por lo tanto "se plantean dos clases de derechos: (i) varios derechos que ya han logrado el reconocimiento en muchos países como la libertad de expresión, el derecho a la protección de los datos sensibles, a la privacidad, al secreto de las comunicaciones, entre otros; y, (ii) otros derechos de nueva data que recién están naciendo, como los derechos del cibernauta en el mundo digital"[209].

Derivado de todo esto, se puede distinguir dos clases de derechos humanos digitales: 1. Como medios y; 2. Nueva data, por ejemplo, en los derechos de nueva data se puede establecer el derecho al olvido, que justamente se relaciona con el

---

[207] Véase. Aguilar Cuevas, Magdalena, *Las tres generaciones de los Derechos Humanos*, https://revistas-colaboracion.juridicas.unam.mx/index.php/derechos-humanos-emx/article/viewFile/5117/4490 de 13 marzo de 2022, 21:03 hrs.

[208] Véase. Martínez-Villalba, Juan Carlos Riofrío, "La cuarta ola de Derechos Humanos: Los Derechos Digitales", *Revista Latinoamericana de Derechos Humanos*, 2014, Volumen 25, I Semestre 2014, https://www.corteidh.or.cr/tablas/r33897.pdf de 20 noviembre, 2021, 16:34 hrs.

[209] Ibídem, p. 16.

problema de los resultados que produce la autoría en los delitos cometidos en el ciberespacio; otra pauta de derecho de nueva data es el derecho al internet.

En cuanto a la Confidencialidad o Privacidad en la modalidad de Derecho Digital Humano es donde se centran más las autoridades en vulnerar dicho derecho, por ejemplo, en Australia con el proyecto *Identify and Disrupt* -identificar e interrumpir- que por demás también atenta contra la Integridad y Disponibilidad Digital debido a que las autoridades podrían modificar y eliminar contenidos, datos de los sujetos investigados[210].

En México, se tiene la intervención de comunicaciones privadas[211]. Dicha intervención tiene su fundamento en el artículo 252, fracción III del Código Nacional de Procedimientos Penales y el artículo 16 constitucional en sus párrafos 12 y 13.

En el artículo 252 sobresale como acto de control que requiere control judicial y en el artículo 16 se establece que las comunicaciones privadas son inviolables y solo serán admitidas cuando quienes hayan participado en tal comunicación privada las aporten de manera voluntaria y por demás dichas pruebas deban estar relacionadas con la comisión de un delito, como segundo elemento importante es que solo la autoridad judicial federal puede facultar la intervención de comunicaciones privadas.

Otra cuestión interesante de analizar es propiamente el poder que tienen los gigantes corporativos de las redes sociales sobre los propios gobiernos de los países, y es que es prácticamente imposible imputarles una responsabilidad penal por cualquier contenido que sea publicado por parte de sus usuarios, justificándose bajo la sección 230 de la *Communications Decency Act* -Ley de Decencia en las Comunicaciones- que establece lo siguiente: “Ningún proveedor o usuario de un

[210] Esparragoza, Luis, *Identificar e interrumpir: así funciona la nueva ley de vigilancia en Australia*, Criptonoticias, 2021, https://www.criptonoticias.com/regulacion/identificar-interrumpir-asi-funciona-nueva-ley-vigilancia-australia/ de 14 marzo de 2022, 12:37 hrs.

[211] Se puede entender a la comunicación como el acto de intercambiar información por diferentes medios, en nuestro caso es por medio de los dispositivos electrónicos.

servicio de ordenadores interactivo deberá ser tratado como el publicador o emisor de ninguna información de otro proveedor de contenido informativo"[212].

Además de la inmunidad que les otorga la sección 230 de la *Communications Decency Act* a las grandes empresas de las redes sociales, por igual éstas tienen el poder de bloquear y eliminar contenidos que consideren inadecuados basadas en sus políticas, pero, aun así, son muy carentes sus criterios de censura.

El ejemplo de actualidad es la lamentable situación de guerra entre Rusia y Ucrania, pues la red social de *Facebook -Meta-*, suavizó sus normas sobre los discursos de odio, así incitando a todo tipo de contenido violento contra Rusia y sus militares y altos mandos[213].

Dadas estas acciones, por primera vez un gobierno -ruso- propone medidas penales contra una empresa tecnológica de redes sociales por incitar al odio y a la violencia. La Fiscalía rusa, pidió clasificar a *Meta*, con el conjunto de sus redes sociales, como una "organización extremista", conforme a los delitos contenidos en el Código Penal Ruso en los artículos 205.1 Facilitación de actividades terroristas y 280 Convocatorias públicas para llevar a cabo actividades extremistas[214].

De tales acciones se puede desprender que los únicos afectados son los ciudadanos en sus derechos como el acceso a la información desde el momento en

---

[212] González, Sara, *Trump y Twitter: ¿Qué es la sección 230 y por qué estás oyendo hablar de ella?,* 2020, https://www.newtral.es/trump-y-twitter-que-es-la-seccion-230-y-por-que-estas-oyendo-hablar-de-ella/20200529/ de 21 noviembre de 2021, 17:23 hrs.

[213] Deutsche Welle, *Facebook suaviza normas que permiten discursos violentos*, 2022, https://www.dw.com/es/facebook-suaviza-normas-que-permiten-discursos-violentos/a-61090134 de 14 marzo de 2022, 13:34 hrs.

[214] La facilitación de actividades terroristas se relaciona con el tipo de actos terroristas (artículo 205) a quien cometa acciones como explosiones o incendios con el fin de aterrorizar al pueblo y desestabilizar las actividades de las autoridades; así como la amenaza de cometer estas acciones con el propósito de influir en las decisiones de las autoridades, por ende, la facilitación de actividades terroristas es la inducción, reclutamiento, ayuda y financiación de actos terroristas contenidos en el artículo 205, entre otros. Véase. Artículo 205, 205.1, Código Penal de la Federación Rusa, https://www.consultant.ru/document/cons_doc_LAW_10699/23e558e632eb102b26427dffe3575b4e87f7067b/ de 14 de marzo de 2022, 14:02 hrs.

En cuanto a las convocatorias públicas para llevar a cabo actividades extremistas tiene como fundamento el artículo 13 de la Constitución de la Federación Rusa. En el cual se prohíbe la fundación y las reuniones cuyas finalidades y acciones persiguen el propósito de combatir a través de la fuerza el régimen constitucional, dañar la integridad de la federación rusa, socavar la seguridad del Estado, crear ejércitos o provocar discordias sociales, religiosas, raciales y étnicas. Véase. Artículo 13 de la Constitución de Federación de Rusia, 2014, https://www.constituteproject.org/constitution/Russia_2014.pdf?lang=es de 14 de marzo de 2022, 14:23 hrs.

Ante esto el artículo 280 castiga tales hechos dando como medios comisivos el uso de medios de comunicación masiva o redes de la información y telecomunicaciones. Véase. Artículo 280, Código Penal de la Federación Rusa, op. cit.

que tanto Rusia como Occidente se encuentran bloqueando y censurando contenidos en una guerra ya no solo convencional sino ahora mediática.

### 7.2.2 El ESCUDO DORADO. INTERNET NACIONAL, CENSURA O SOLUCIÓN CONTRA LA INMUNIDAD DE LAS GRANDES EMPRESAS TECNOLÓGICAS

China está combatiendo fuertemente contra las grandes corporaciones tecnológicas, dando sus primeros intentos de crear un internet nacional con su gran Escudo Dorado, así censurando contenidos que no le convienen al gobierno chino[215].

Por lo tanto, el problema no es la creación de barreras, muros digitales, sino la censura a los contenidos que no le convienen al gobierno cuando éste es quien controla el internet; porque el diseño de internet soberano es lo más idóneo para comenzar a establecer barreras dentro del ciberespacio, pero por otro lado eso no asegura que vaya a haber una mayor protección de los Derechos Humanos Digitales.

La nacionalización del internet -en el caso de China- ha hecho que empresas como *Meta* se vean impedidas de brindar sus redes sociales en el gigante asiático lo cual ha generado la creación de redes sociales nacionales como *Weibo*, *WeChat*, así dejando de lado *Facebook, Twitter* y *WhatsApp*; y que poco a poco países como

[215] "El sistema de restricciones chino es mejor conocido como el Gran Cortafuegos chino, del inglés *'Great Chinese Firewall'*, que es una referencia a la Gran Muralla china, una estructura que durante siglos sirvió como un escudo impenetrable que protegía al gigante asiático de las invasiones.

La nueva Gran Muralla, del siglo XXI, sirve a otro propósito: 'proteger' a la población china de las influencias negativas de internet y evitar que ciertos tipos de contenido de la red global desconcierten a los usuarios del país asiático.

Esta es la razón por la que centenares de millones de chinos no tienen acceso a los servicios -en la mayoría absoluta son estadounidenses- tan populares en el resto del mundo como, por ejemplo, Twitter, YouTube y Facebook". Lukyanov, Denis, *El Gran Hermano te vigila: el impenetrable Escudo Dorado de China que "protege" su internet de EEUU*, Sputnik News, 2019, https://www.derechos.org/privacy/doc/chn1.html de 14 marzo 2022, 15:47 hrs.

Turquía, Irán, India, Rusia están por igual planteando la idea de un internet nacionalizado[216].

En el caso de Rusia, se ha ido radicalizando de una manera mucho más exponencial derivado de la guerra ruso – ucraniana que se está librando en pleno 2022, pues se ha dado el bloqueo de *Meta* y sus redes sociales -principalmente *Facebook* e *Instagram*- por promover conductas terroristas. De esto se ha derivado un principal interés de Rusia de seguir el camino de China con la nacionalización del internet, por demás el país ruso ya cuenta con sus propias redes sociales como *VK* y *Rutube*, así tal vez en unos meses o años posteriores, Rusia por igual realice su gran escudo contra las redes de occidente[217].

Al final, tanto ciudadanos chinos como rusos están siendo afectados en sus derechos fundamentales como la privacidad y la libertad de elección y que como bien lo expresó Oscar Robles Garay, ejecutivo de LACNIC[218], "los Estados están utilizando iniciativas de seguridad como excusa para sus programas de sobrevigilancia. Dijo que muchas de esas iniciativas suenan a los oídos bastante plausibles, por la obligación del Estado de proteger la seguridad nacional, de combatir la pornografía infantil o la trata de personas, sin embargo, por esos programas "comenzamos todos a ser vigilados y observados y cada uno de nuestros movimientos comienzan a ser registrados"[219].

Los Derechos Humanos Digitales se ven inmiscuidos en estos temas, puesto que el acceso al internet tiene como principio fundamental el que sea global, pero tal vez ya no sea así en un futuro no muy lejano. Otra cuestión que se considera esencial es que, aunque a mayor regulación jurídica en el ciberespacio habrá mayor vulneración a los Derechos Humanos Digitales ya sean como medios o como nueva data, como la Confidencialidad o Privacidad, Acceso a la información o Libertad de

[216] RT Documentales, *Censura Virtual, ¿cuál es el futuro del internet?*, 2021, https://www.youtube.com/watch?v=ED_zIizL8zo de 15 marzo de 2022, 19:21 hrs.
[217] Quintero, Carla, *Cuáles son las redes sociales más populares de Rusia*, marketin4ecommerce mx, 2022, https://marketing4ecommerce.mx/cuales-son-las-redes-sociales-mas-populares-de-rusia/ de 15 marzo de 2022, 19:38 hrs.
[218] LACNIC, es una organización no gubernamental internacional encargada del Registro de Direcciones de Internet de América latina y Caribe.
[219] Robles Garay, Oscar, *El riesgo de "nacionalizar" internet*, lacnic News, 2017, https://prensa.lacnic.net/news/gobernanza-de-internet/el-riesgo-de-nacionalizar-internet de 15 marzo de 2022, 19:56 hrs.

expresión o prensa por parte de las grandes corporaciones de las redes sociales, pero por igual con los gobiernos como en China y Rusia.

Después de todo, los únicos perjudicados son los ciudadanos que terminan pagando las consecuencias de quienes toman el control del internet.

## 7.3. EL DELITO INFORMÁTICO

El delito informático que como se escribió en líneas anteriores, también cuenta con sus propias características al momento de la tipificación, pues esto quiere decir que sus grandes cambios se encuentran en los elementos del tipo y no en la antijuridicidad y culpabilidad que son generales de todos los delitos.

El Dr. Julio Téllez Valdés, define al delito informático como concepto atípico y típico, y bajo este orden de ideas, “los delitos informáticos son "actitudes ilícitas que tienen a las computadoras como instrumento o fin" (concepto atípico) o las "conductas típicas, antijurídicas y culpables que tienen a las computadoras como instrumento o fin" (concepto típico)”[220].

El delito informático es el acceso, obtención, interceptación, distribución, alteración, destrucción o secuestro de datos informáticos no autorizados mediante medios informáticos, así como el acceso no autorizado a los objetos de internet, ya sea para ser básicos o subordinados.

Esta última definición es muy casuística, pero trata de abarcar la mayor parte de conductas que se dan en el ciberespacio desde la obtención hasta el secuestro de datos y si se logra apreciar con mayor detalle, se verá la Triada CID como fundamento principal de la definición de delito informático al tratar la obtención y distribución como violación a la Confidencialidad, mientras que la alteración, destrucción y secuestro de datos atentan contra la Integridad y Disponibilidad.

[220] Téllez Valdés, Julio, *Derecho informático*, cuarta edición, Mc Graw Hill, México, 2008, p. 188.

Además, se añade como elemento novedoso los objetos de internet, o sea, lo que se conoce actualmente como *IoT*[221], así ampliando mucho más el campo de los delitos informáticos.

Ahora bien, también se concuerda con la definición del Dr. Julio Téllez Valdés, al proponer los delitos informáticos como instrumento -medio- y fin. Debido a que, por ejemplo, la obtención, distribución pueden ser medios -posibles tipos subordinados- de delitos tradicionales como el fraude o la extorsión, así como el acceso, alteración o destrucción pueden ser delitos básicos.

### 7.3.1 DELITOS INFORMÁTICOS COMO SUBORDINADOS DEL DELITO TRADICIONAL

Los tipos subordinados informáticos o derivados del básico son "en atención a alguna particularidad o elemento accidental, agraven o atenúen la pena"[222] del tipo básico[223], claro ejemplo basándose en el *Strafgesetzbuch* -código penal alemán-, el *Betrug* -fraude-, actúa como tipo básico de donde deriva el *Computerbetrug* -fraude informático- como tipo derivado o subordinado. En el caso de nuestro país el fraude informático como tal se describe en el artículo 230 que se complementa con el 231 fracción XIV del CPCDMX CPDF (ahora CDMX) que establece lo siguiente:

CAPÍTULO III

FRAUDE

> ARTÍCULO 230. Al que por medio del engaño o aprovechando el error en que otro se halle, se haga ilícitamente de alguna cosa u obtenga un lucro indebido en beneficio propio o de un tercero, se le impondrán: …

[221] El IoT -Internet of Things- o el internet de las cosas es un concepto que hace referencia a la interconexión con los objetos cotidianos de la vida, por ejemplo: la conexión con los televisores, las impresoras, las aspiradoras e inclusive con toda la casa o los autos.

[222] LP Pasión por el derecho, *¿Cuáles son las clases de tipos penales? Bien explicado*, https://lpderecho.pe/cuales-son-las-clases-de-tipos-penales-bien-explicado/ de 7 octubre de 2022, 14:20 hrs.

[223] Como particularidad o elemento accidental puede ser el medio que en nuestro caso es el uso de la informática para delinquir, ejemplo: Fraude informático.

ARTÍCULO 231. Se impondrán las penas previstas en el artículo anterior, a quien:

XIV. Para obtener algún beneficio para sí o para un tercero, por cualquier medio accese, entre o se introduzca a los sistemas o programas de informática del sistema financiero indebidamente realice operaciones, transferencias o movimientos de dinero o valores, independientemente de que los recursos no salgan de la Institución…[224].

Como se puede apreciar en el código local de la CDMX el fraude informático es parte del tipo básico. Otro ejemplo es la propia extorsión que establece lo siguiente en el artículo 236 del ya citado código:

CAPÍTULO VI

EXTORSIÓN

ARTÍCULO 236. Al que obligue a otro a dar, hacer, dejar de hacer o tolerar algo, obteniendo un lucro para sí o para otro causando a alguien un perjuicio patrimonial, se le impondrán de cinco a diez años de prisión y de mil a dos mil unidades de medida y actualización…

Asimismo, las penas se incrementarán en dos terceras partes cuando se utilice como medio comisivo la vía telefónica, el correo electrónico o cualquier otro medio de comunicación electrónica[225].

De nuevo se actualiza como medio comisivo del delito tradicional de extorsión como agravante, o sea, delito dependiente del básico.

CAPÍTULO III

PORNOGRAFÍA

ARTÍCULO 187. Al que procure, promueva, obligue, publicite, gestione, facilite o induzca, por cualquier medio, a una persona menor de dieciocho años de edad o persona que no tenga la capacidad de comprender el significado del hecho o de persona que no tiene capacidad de resistir la conducta, a realizar actos sexuales o de exhibicionismo corporal con fines lascivos o sexuales, reales o simulados, con el

[224] Artículos 230, 231fracción XIV, Código Penal de la Ciudad de México, op. cit.

[225] Artículo 236.Código Penal de la Ciudad de México, op. cit.

objeto de video grabarlos, audio grabarlos, fotografiarlos, filmarlos, exhibirlos o describirlos a través de anuncios impresos, sistemas de cómputo, electrónicos o sucedáneos; se le impondrá de siete a catorce años de prisión y de dos mil quinientos a cinco mil días multa, así como el decomiso de los objetos, instrumentos y productos del delito, incluyendo la destrucción de los materiales mencionados.

Si se hiciere uso de violencia física o moral o psicoemocional, o se aproveche de la ignorancia, extrema pobreza o cualquier otra circunstancia que disminuya o elimine la voluntad de la víctima para resistirse, la pena prevista en el párrafo anterior se aumentará en una mitad.

Al que fije, imprima, video grabe, audio grabe, fotografíe, filme o describa actos de exhibicionismo corporal o lascivos o sexuales, reales o simulados, en que participe una persona menor de dieciocho años de edad o persona que no tenga la capacidad de comprender el significado del hecho o de persona que no tiene capacidad de resistir la conducta, se le impondrá la pena de siete a doce años de prisión y de mil a dos mil días multa, así como el decomiso y destrucción de los objetos, instrumentos y productos del delito.

Se impondrán las mismas sanciones a quien financie, elabore, reproduzca, almacene, distribuya, comercialice, arriende, exponga, publicite, difunda, adquiera, intercambie o comparta por cualquier medio el material a que se refieren las conductas anteriores.

Al que permita directa o indirectamente el acceso de un menor a espectáculos, obras gráficas o audiovisuales de carácter lascivo o sexual, se le impondrá prisión de uno a tres años y de cincuenta a doscientos días multa.

No constituye pornografía el empleo en los programas preventivos, educativos o informativos que diseñen e impartan las instituciones públicas, privadas o sociales, que tengan por objeto la educación sexual, educación sobre la función reproductiva, prevención de infecciones de transmisión sexual y embarazo de adolescentes[226].

El tipo de pornografía es medio en esta situación debido al almacenaje y distribución que no podría darse si no fuera por los medios informáticos.

[226] Artículo 187, Código Penal de la Ciudad de México, op. cit.

## 7.3.2 DELITOS INFORMÁTICOS BÁSICOS

Estos delitos se caracterizan por:

1. Tener sus propios bienes jurídicos predominantes donde destaca la Confidencialidad. Se puede entender a la confidencialidad digital como el derecho que todo cibernauta -ente privado o público- tiene para decidir qué tipo de contenido, datos quiere hacer públicos y cuáles no y;
2. Finalidad de dañar el objeto material -persona o dispositivo- o información que contenga éste; como lo expresa el Dr. Alberto Enrique Nava Garcés citando a la autora María de la Luz Lima Malvido, no son más que "Conductas criminógenas dirigidas contra la entidad física del objeto o máquina electrónica o su material con objeto de dañarla"[227].

Establecidas las características se analizarán algunos tipos penales básicos informáticos y se hará con dos delitos que se puede decir son el más vivo ejemplo de delitos informáticos básicos y que son recientes en nuestro país.

CAPÍTULO VII

CONTRA LA INTIMIDAD SEXUAL

Artículo 181 Quintus. Comete el delito contra la intimidad sexual:

I. Quien videograbe, audiograbe, fotografíe, filme o elabore, imágenes, audios o videos reales o simulados de contenido sexual íntimo, de una persona sin su consentimiento o mediante engaño.

II. Quien exponga, distribuya, difunda, exhiba, reproduzca, transmita, comercialice, oferte, intercambie y comparta imágenes, audios o videos de contenido sexual íntimo de una persona, a sabiendas de que no existe consentimiento, mediante materiales impresos, correo electrónico, mensajes telefónicos, redes sociales o cualquier medio tecnológico.

[227] Nava Garcés, Alberto Enrique, *Delitos informáticos*, Cuarta edición, Porrúa, México, 2018, p. 139.

A quien cometa este delito, se le impondrá una pena de cuatro a seis años de prisión y multa de quinientas a mil unidades de medida y actualización…"[228].

Este tipo penal data del 2020, es muy reciente como se puede apreciar y deriva de los vulgarmente denominados packs, paketazos, cajita feliz, *nudes*, etc. Que se habían hecho muy populares a través de las redes sociales, donde mayormente el sujeto pasivo es la mujer y que por lo general derivaban del *sexting.*

La comercialización de contenido intimo en el tan conocido *marketplace* de *facebook* no es constitutivo de este delito, pues es contenido consentido a través de un precio, para encontrar este tipo de contenido se insertan palabras como paketazos, cajita feliz, *mystery box* e inclusive haciendo alusión a contenido de comida y ropa como pack de camisas, ricas donas glaseadas, entre otras tantas palabras.

Lo mismo ocurre en otros sitios web como el tan famoso *Only Fans,* al final de todo dichas conductas son consideradas como trabajo sexual digital, y no por eso deben ser recriminadas las personas, sino como bien lo establece el tipo, se recrimina a quienes distribuyen dichos contenidos sin el consentimiento del titular, pues atentan contra la Confidencialidad digital, y ojo, no porque vendan su contenido quiera decir que sea público, no es así, ya que por ejemplo en el caso de *Only fans*, el acceso es solo a quienes pagan, haciéndolo un contenido privado a quienes no pagan; si fuese público el contenido sería visible para todos y todas y este no es el caso, pero eso tampoco da lugar a quienes ya hayan accedido, a distribuir el contenido pues éste es solo para quienes pagaron y no para difusión entre toda la web.

Otra característica es que en este artículo se puede constituir un concurso de delitos, por ejemplo, contra la intimidad y extorsión que pueden ser los más comunes dando como resultado un delito informático mixto.

[228] Artículo 181 Quintus, Código Penal de la Ciudad de México, op. cit.

Otro delito informático como básico es el que se establece en el Código Penal del Estado de México:

> Artículo 227 Bis.- Al que por cualquier medio y fuera de los supuestos autorizados por la Ley, audiograbe, comercialice, comparta, difunda, distribuya, entregue, exponga, envíe, filme, fotografíe, intercambie, oferte, publique, remita, reproduzca, revele, transmita o videograbe, imágenes, audios, videos o documentos de cadáveres o parte de ellos que se encuentren relacionados con una investigación penal, de las circunstancias de la muerte o de las lesiones que éstos presentan, se le impondrán de tres a seis años de prisión y multa por un importe equivalente de cincuenta a cien veces el valor diario de la unidad de medida y actualización.
>
> Tratándose de imágenes, audios o videos de cadáveres de mujeres, niñas o adolescentes, de las circunstancias de su muerte, de las lesiones o estado de salud, las penas previstas en este artículo se incrementarán hasta en una mitad.
>
> Cuando el delito sea cometido por persona servidora pública integrante de cualquier institución de seguridad pública o de impartición o procuración de justicia, las penas previstas se incrementarán hasta en una tercera parte[229].

Este tipo penal nace de un lamentable suceso ocurrido el 9 de febrero de 2020, derivado de un feminicidio donde se compartieron imágenes sobre el cuerpo de la víctima, generando un morbo mediático y que de tan funesto suceso se pone de nuevo en tela de juicio, el hasta dónde llega la libertad de expresión y para ser más específicos, la denominada libertad de prensa, ya que si se apega a dicho tipo, entonces todos los periódicos de nota roja y los sitios *gore* tendrían serios problemas legales, porque toda muerte de forma no natural o lesión conlleva una investigación criminal.

Ahora bien, un código penal muy interesante que crea su propia división de delitos informáticos en su capítulo V TER. - Delitos informáticos y cibernéticos que van del 243 bis 5 al 243 bis 12, es el código penal de Yucatán, que se analizó de manera corta en el tema del *ciberbullying*.

---

[229] Artículo 227 bis, Código Penal del Estado de México, México, 2021, http://legislacion.edomex.gob.mx/sites/legislacion.edomex.gob.mx/files/files/pdf/cod/vig/codvig006.pdf de 5 de octubre de 2021, 10:42 hrs.

Este código plantea 8 artículos de manera general sin establecer qué tipo de conducta constituye cada tipo, sino que simplemente, los tipifica de manera general como delitos informáticos y cibernéticos, así planteando varias dudas, una de ellas es, ¿Cuáles son los delitos cibernéticos?, si la informática es inherente al *software*, y la electrónica al *hardware* y de éste derivan los delitos informáticos, o sea, los dispositivos electrónicos para delinquir necesitan sí o sí de la informática, pero y, ¿la referencia a cibernéticos?, la cibernética ha variado su significado con la evolución tecnológica y no es más que una clara referencia a nuestra nueva realidad digital.

La RAE, define como cibernético de la siguiente manera: "adj. Creado y regulado mediante computadora; adj. Perteneciente o relativo a la realidad virtual; así como f. Ciencia que estudia las analogías entre los sistemas de control y comunicación de los seres vivos y los de las máquinas"[230], o bien, "si atendemos a la etimología de la palabra, el vocablo cibernético tiene su origen en la voz griega *Kybernetes* "piloto" y *Kybernes,* concepto referido al arte de gobernar. Esta palabra alude a la función del cerebro respecto a las máquinas"[231].

Sin duda, la cibernética es inherente a las dos ramas antes mencionadas, pero que sin vacilación es mucho más amplia, en pocas palabras la cibernética desde mi punto de vista es el caso general y la electrónica y la informática es el caso particular, así que no es correcto llamarlos delitos cibernéticos porque es ampliar el campo de lo que correctamente deben llamarse delitos informáticos para así delimitar los campos. Ahora se pasa a analizar el siguiente cuadro para ver cómo debe ser nombrada cada conducta en su artículo correspondiente.

[230] Real Academia Española, *Diccionario de la Lengua Española*, 2020, https://dle.rae.es/cibern%C3%A9tico de 25 octubre de 2021, 15:28 hrs.

[231] Téllez Valdés, Julio, op. cit., p. 5

*Tabla 3: Nombres apropiados para el tipo de los delitos informáticos y cibernéticos del Código Penal de Yucatán.*

| **Código penal de Yucatán.**<br><br>**Capítulo V. TER. Delitos informáticos y cibernéticos.** | | |
|---|---|---|
| Artículo. | Descripción del tipo. | Nombres apropiados para el tipo. |
| Artículo 243 bis 5 | Al que, sin autorización, para beneficio propio o ajeno, modifique, destruya o provoque pérdida de información contenida en sistemas o equipos informáticos protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a dos años de prisión y de mil a dos mil días – multa. | Daño informático. |
| Artículo 246 bis 6 | Al que sin autorización se introduzca por cualquier medio a un sistema o equipo de informática protegido por algún mecanismo de seguridad, para beneficio propio o ajeno, para sustraer, eliminar o cambiar información contenida en él; con la intención de provocar un desperfecto en su funcionamiento que lo deje total o parcialmente inoperable; intercepte comunicaciones privadas con la intención recabar información personal o financiera, se le impondrán de uno a tres años de prisión y de mil a dos mil días - multa. | Acceso ilícito a sistemas y equipos de informática. |
| | Al que, estando autorizado para acceder a sistemas y equipos de informática del Estado, sustraiga información para beneficio personal o ajeno, o quien facilite esto a un tercero que no cuente con | |

| | | |
|---|---|---|
| Artículo 243 bis 7 | autorización, se le impondrán de uno a cuatro años de prisión y de mil a dos mil quinientos días - multa. | Robo de datos informáticos. |
| Artículo 243 bis 8 | Al que, estando autorizado para acceder a sistemas y equipos de informática del Estado, indebidamente modifique o provoque perdida de información para beneficio personal o ajeno, se le impondrán de uno a cuatro años de prisión y de mil a dos mil días - multa. | Daño informático contra el Estado. |
| Artículo 243 bis 9 | Al que, estando autorizado para acceder a sistemas y equipos de informática, indebidamente modifique o provoque pérdida de información que contengan, se le impondrán de dos a cuatro años de prisión y de mil a dos mil días - multa. | Daño informático contra los particulares. |
| Artículo 243 bis 10 | Se impondrán de dos a cuatro años de prisión y de dos mil a tres mil días - multa a quien utilizando información que aparente provenir de instituciones financieras o empresas de servicios informáticos o electrónicos o dependencias del Poder Ejecutivo u otro poder u organismo del estado: I.- Provoque la instalación de programas informáticos en ordenadores o teléfonos inteligentes a fin de acceder a la información contenida en ellos o la que se genere por llamadas, mensajes, servicios que utilicen Internet o la ubicación en tiempo real mediante el sistema de posicionamiento global (GPS). II.- Provoque la sustracción o revelación de audio, video, fotografías digitales o información personal o financiera. | Espionaje informático. |

| | | |
|---|---|---|
| | | |
| Artículo 243 bis 11 | Las sanciones contenidas en los artículos 243 Bis 7 y 243 Bis 8 de este código, se duplicarán cuando la conducta tenga la intención de obstruir, entorpecer, obstaculizar, limitar o imposibilitar la procuración o impartición de justicia, o recaiga sobre los registros relacionados con un procedimiento penal resguardados por las autoridades competentes. Además de lo establecido en el párrafo anterior, si el sujeto activo es un servidor público, se impondrá la destitución del cargo o empleo y la inhabilitación para obtener otro en el servicio público por un término de hasta ocho años. | Agravantes del robo de datos y daño informático contra el Estado. |
| Artículo 243 bis 12 | Comete el delito de ciberacoso quien intimide y asedie a cualquier persona, a pesar de su oposición, por medio de las Tecnologías de la Información y Comunicación, tales como redes sociales, mensajería instantánea, correo electrónico o cualquier otro medio digital; mediante el envío de mensajes de texto, videos, impresiones gráficas, sonoras o fotografías. Este delito se sancionará de seis meses a tres años de prisión y de cincuenta a doscientos días-multa. Cuando el delito sea cometido en contra de un menor de dieciocho años de edad, la pena y la sanción establecida se aumentarán hasta en una mitad. Este delito se perseguirá a petición de parte ofendida, salvo que la víctima sea menor de edad o por cualquier | Ciberacoso. |

| | | |
|---|---|---|
| | circunstancia sea incapaz de comprender el delito, en cuyo caso se perseguirá de oficio[232]. | |

[232] Artículos 243 bis 5 – 243 bis 12, Código Penal de Yucatán, México, 2021, http://187.157.158.150:3001/legislacion/codigos/13af0b6e2a69c4eafc8911c477281295_2021-10-01.pdf de 25 de octubre de 2021, 15:40 hrs.

# CONCLUSIONES

**PRIMERA.** Se plantea la necesidad de conocer la historia de la electrónica y la informática, así comprendiendo que la primera es el *Hardware* y la segunda es el *Software*. Volviéndose inherentes ambas para la comisión de los delitos informáticos.

**SEGUNDA.** Se analiza la importancia que juegan las redes sociales y la ciberseguridad al momento de la constitución de los delitos informáticos.

**TERCERA.** De la teoría del delito se desprenden los sujetos que integran al delito informático, así como las conductas que se emplean para delinquir, por igual saber que el delito informático varia en su definición y elementos típicos, pero no en la antijuridicidad o culpabilidad propiamente, debido a que no puede haber una *Rechtswidrigkeit* o una *Schuld* especial para cada delito.

**CUARTA.** El convenio de Budapest es el mayor ordenamiento jurídico internacional para una efectiva lucha contra el cibercrimen. De dicho Convenio se hizo un estudio de los delitos que lo conforman, que van desde los delitos que atentan contra la Triada CID hasta delitos tradicionales como la pornografía infantil.

**QUINTA.** Se hace un estudio de tipos penales de Alemania como el *Computerbetrug* -fraude informático- y la *Verbreitung gewalt oder tierpornographischer Inhalte* -distribución de contenido violento o pornografía con animales-, así como el delito de *Obscene materials* -materiales obscenos- por parte de Canadá.

**SEXTA.** Del análisis de los tipos penales de Alemania y Canadá se puede observar la complejidad que envuelve el tipo de fraude informático alemán y la comparación del tipo de materiales obscenos canadiense con el artículo 227 bis del Código Penal del Estado de México.

**SÉPTIMA.** El *compliance penal* es vital en los delitos informáticos -más allá de ser temas novedosos- por el simple hecho de que durante sus tres aplicaciones se debe hacer un estudio de los tipos informáticos para el análisis y creación de los indicadores que van a conformar el diagnóstico parte de la realización del

*compliance penal*. Es así como por igual se establece una tabla de bienes jurídicos que conforman los tipos informáticos como guía, y el artículo 12 del Convenio de Budapest, en cuanto se refiere a la responsabilidad penal de las personas jurídicas inmiscuidas en los delitos informáticos.

**OCTAVA.** Se propone una definición de delito informático basada en los verbos rectores que predominan en los delitos informáticos, añadiendo como elemento novedoso el *IoT*.

**NOVENA.** Se establecen los delitos informáticos subordinados, así como los delitos básicos.

**DÉCIMA.** Los delitos básicos deben cumplir con dos características las cuales son:

1. Cuentan con sus propios bienes jurídicos como la Confidencialidad, Integridad y Disponibilidad digital y;
2. Tienen la finalidad de dañar el objeto material.

# PROPUESTA DE ESTUDIO DOGMÁTICO DEL DERECHO PENAL INFORMÁTICO PARA LA DIVISIÓN DE LOS DELITOS EN BÁSICOS Y SUBORDINADOS PARA FUTUROS TIPOS PENALES DE ÍNDOLE INFORMÁTICA

Derivado de la lectura sobre los delitos básicos y subordinados informáticos es que la presente propuesta gira en torno al estudio dogmático que se puede hacer analizando los tipos según su clasificación en tipos básicos y subordinados de éste, pues a través de la lectura de esta tesis se deja en claro que el delito básico es independiente en cuanto a análisis y con un propio bien jurídico de naturaleza predominantemente informática.

Los delitos básicos informáticos deben cumplir con dos características esenciales las cuales son:

1. Cuentan con sus propios bienes jurídicos como la confidencialidad, integridad y disponibilidad digital y;
2. Tienen la finalidad de dañar el objeto material.

Es por eso por lo que destacan los delitos contra la confidencialidad, integridad y disponibilidad de los datos informáticos, mientras que el delito subordinado informático depende del básico y que agrava o atenúa la pena, por ejemplo, el fraude informático -*Computerbetrug*- en el código penal de Alemania, es derivado del básico que es propiamente el fraude genérico -*Betrug*- y que tiene como bien jurídico el patrimonio.

Teniendo estas características sencillas y fáciles de comprender es como se podrá identificar al momento de la tipificación si se trata de un delito básico o subordinado, así como tipificar ciertos delitos de naturaleza informática, por ejemplo, se propone la distribución y posesión de contenido violento y la distribución y posesión de contenido violento o pornográfico con animales para el código penal del Distrito Federal (ahora Ciudad de México), para quedar de la siguiente manera:

| TEXTO VIGENTE | TEXTO PROPUESTO |
| --- | --- |
| TITULO DECIMO<br>DELITOS CONTRA LA DIGNIDAD DE LAS PERSONAS<br>CAPITULO ÚNICO<br>DISCRIMINACIÓN<br>(…)<br>CAPÍTULO II<br>TORTURA<br>(…)<br>SE AÑADE TEXTO PROPUESTO | CAPITULO III<br>DISTRIBUCIÓN Y POSESIÓN DE CONTENIDO VIOLENTO<br><br>Artículo 206 SEXTUS. A quien distribuya, posea, comercialice contenido multimedia que contenga conductas como torturas, homicidios, feminicidios, lesiones o cualquier otra conducta que implique violencia extrema, se le impondrá de 3 a 5 años de prisión.<br><br>La pena aumentará de 6 a 10 años al que siendo servidor público posea, distribuya contenido multimedia violento parte de una investigación penal relacionada con la o las víctimas.<br><br>No se impondrá pena alguna a quien por ejercicio de un derecho se allega de dichos materiales para material probatorio dentro de una investigación penal.<br><br>Se entenderá por contenido violento todo aquel contenido audiovisual que contenga violencia extrema para exaltar, promover conductas |

| | |
|---|---|
| | consideradas como delitos, infunda miedo a la población. |

| TEXTO VIGENTE | TEXTO PROPUESTO |
|---|---|
| TITULO VIGESIMO QUINTO<br>DELITOS CONTRA EL AMBIENTE, LA GESTIÓN AMBIENTAL Y LA PROTECCIÓN A LA FAUNA<br>CAPITULO I<br>DELITOS CONTRA EL AMBIENTE<br>(…)<br>CAPITULO II<br>DELITOS CONTRA LA GESTION AMBIENTAL<br>(…)<br>CAPITULO III<br>DISPOSICIONES COMUNES A LOS DELITOS PREVISTOS EN EL PRESENTE TITULO<br>(…)<br>CAPITULO IV<br>DELITOS COMETIDOS POR ACTOS DE MALTRATO O CRUELDAD EN CONTRA DE ANIMALES NO HUMANOS<br>(…)<br>SE AÑADE TEXTO PROPUESTO | DELITOS COMETIDOS POR ACTOS DE MALTRATO O CRUELDAD EN CONTRA DE ANIMALES NO HUMANOS<br><br>Artículo 350 QUATER. A quien posea, distribuya, comercialice contenido violento como actos de violencia o pornográfico por parte de personas en contra de animales, se le impondrá de 3 a 5 años de prisión.<br><br>No se impondrá pena alguna a quien por ejercicio de un derecho se allega de dichos materiales para material probatorio dentro de una investigación penal. |

Estos dos tipos propuestos son necesarios en el territorio de la Ciudad de México, por ejemplo, el tipo penal de contenido violento ya está legislado en el Código Penal del Estado de México, aunque recientemente se ha declarado invalido, dicho tipo es de ámbito restringido solamente a contenido relacionado con las investigaciones penales, mientras que el que propongo es más extenso pues aquí será acreedor de una pena todo sujeto que tenga contenido multimedia esté o no bajo una investigación penal debido a la constante difusión de contenido extremo sin alguna responsabilidad para quienes posean y difundan tales contenidos, claro está que si el artículo 227 bis del Código Penal del Estado de México es invalido, el artículo propuesto al ser más extenso pareciera violar la libertad de expresión, pero en atención al contexto que envuelve al Estado Mexicano se tiene que profundizar respecto a las conductas ciber delictivas para una mejor tipificación de los actos ilícitos que se generan en el ciberespacio. La lucha constante entre la tipificación de conductas ciber delictivas contra la libertad de expresión por medios digitales.

México está envuelto en una ola de violencia y que casos como el de Ingrid y la alza de distribución de contenido violento extremo para provocar miedo, pánico y alarma social al pueblo se ha convertido en una ardua tarea para legislar en materia de delitos informáticos por su constante choque con los derechos humanos.

La propuesta del delito de distribución y posesión de contenido violento contiene como sujeto pasivo a la víctima directa sin contener una calidad especifica en la victima en la mayoría de las veces, así como indirectas y que atenta contra el respeto y dignidad de éstas como bienes jurídicos por ende se puede añadir como el artículo 206 SEXTUS del Título décimo del Código Penal de la Ciudad de México denominado delitos contra la dignidad de las personas.

El tipo penal de distribución y posesión de contenido o pornográfico con animales es un delito pero solo del orden físico, o sea, solo es punible la zoofilia o los actos de violencia contra los animales en la Ciudad de México, pero no quienes posean, distribuyan, comercialicen tales contenidos dentro del orden informático y esto es de suma relevancia para beneficio de los animales puesto que desde todas

las perspectivas se debe lograr una protección a los animales porque de muy poco sirve que se castigue a quienes realicen actos violentos o zoofílicos contra animales si quien compra y promueve la realización de tales contenidos se escapa del castigo.

La propuesta de distribución y posesión de contenido violento o pornográfico con animales cuenta con un sujeto especial pasivo que en este caso son los animales y el sujeto activo la persona humana, en lo que respecta al bien o bienes jurídicos afectados son la vida, integridad, respeto y dignidad de los animales.

# BIBLIOGRAFÍA


1. Amuchategui Requena, Irma Griselda, *Derecho penal*, cuarta edición, Oxford, México, 2012.
2. Arreola García, Adolfo, *Ciberseguridad ¿por qué es importante para todos?*, Siglo XXI, México, 2019.
3. Bardales Lazcano, Erika, *Guía para el estudio del sistema penal acusatorio. Nuevo sistema de justicia penal*. Primera reimpresión a la sexta edición, Editorial Flores, México, 2018.
4. Baumann, Jürgen, *Derecho penal conceptos fundamentales y sistema, introducción a la sistemática sobre la base de casos*, cuarta edición, trad. de A. Finzi, Conrado, Editorial DEPALMA, Buenos Aires, 1972.
5. Castellanos Tena, Fernando et al., *Lineamientos elementales del derecho penal parte general*, 55ª edición, Porrúa, México, 2020.
6. Cervantes, Pere y Tauste Solá, Oliver, internet negro, Paidós, 2016.
7. Cossío Zazueta, Luis et al, *Enciclopedia Jurídica de la Facultad de Derecho*, Porrúa, Tomo IX Derecho Penal, México, 2018.
8. Díaz Aranda, Enrique y Roxin, Claus, *Teoría del delito funcionalista*, Flores Editor, México, 2017.
9. Donna, Edgardo Alberto, *Teoría del delito y de la pena tomo 2 Imputación objetiva*, Editorial Astrea, tomo 2, Buenos Aires, 1995.
10. Escuela Judicial Rodrigo Lara Bonilla, *Teoría del delito*, Colombia, 2010.
11. Flores Prada, Ignacio, *Criminalidad informática: Aspectos sustantivos y procesales,* Tirant lo Blanch, 2012.
12. Franco Guzmán, Ricardo, *Delito e injusto. Formación del concepto de antijuridicidad*, segunda edición, Porrúa, México, 2012.
13. Gallas, Wilhelm, *Teoría del delito en su momento actual*, trad. de Córdoba Roda, Juan, Editorial HEBO, Ciudad de México, 2022.
14. Jakobs, Gunthër, *Derecho penal parte general. Fundamentos y teoría de la imputación*, segunda edición corregida, trad. de Cuello Contreras, Joaquín y Serrano González de Murillo, José Luis, Editorial Marcial Pons, Madrid, 1997.

15. Menchaca Córdova, Marcelo, *Derecho informático*, creative commons, Bolivia, 2014.
16. Nava Garcés, Alberto Enrique, *Delitos informáticos*, Cuarta edición, Porrúa, México, 2018.
17. Pavón Vasconcelos, Francisco, *Manual de derecho penal mexicano. Parte general*, Ciudad de México, Porrúa, 2016.
18. Peña Gonzáles, Oscar y Almanza Altamirano, Frank, *Teoría del delito: Manual práctico para su aplicación en la teoría del caso,* Perú, Asociación Peruana de Ciencias Jurídicas y Conciliación, 2010.
19. ROXIN, Claus, *Autoría y dominio del hecho en derecho penal*, séptima edición alemana, trad. de Cuello Contreras, Joaquín y Serrano González de Murillo, José Luis, Editorial Marcial Pons, Madrid, 2000.
20. Roxin, Claus, *Derecho penal. Parte general, Tomo I. Fundamentos. La estructura de la teoría del delito*, segunda edición, trad. Luzón Peña, Diego-Manuel et al, Editorial Civitas, Tomo I, Madrid, 1997.
21. Téllez Valdés, Julio, *Derecho informático*, cuarta edición, Mc Graw Hill, México, 2008.
22. Von Frank, Reinhard*, Estructura del Concepto de Culpabilidad*, Editorial HEBO, Ciudad de México, 2022.
23. Welzel, Hans, *Derecho penal parte general,* trad. de Fontán Balestra, Carlos, Roque Depalma, Buenos Aires, 1956.
24. Welzel, Hans, *Teoría de la acción finalista*, Editorial DEPALMA, Buenos Aires, 1951.
25. Zaffaroni, Eugenio Raúl et al., *Manual de derecho penal parte general*, 2da edición, EDIAR, Buenos Aires, 2007.

LEGISLACIÓN.

Internacional.


1. Código Penal de la Federación Rusa, https://www.consultant.ru/document/cons_doc_LAW_10699/23e558e632eb102b26427dffe3575b4e87f7067b/.
2. Constitución de Federación de Rusia, 2014, https://www.constituteproject.org/constitution/Russia_2014.pdf?lang=es .
3. Convenio sobre la Ciberdelincuencia, Serie de Tratados Europeos nº 185, Budapest,2001,https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802fa41c .
4. *Criminal Code of Canada*, Canada, 2021, https://laws-lois.justice.gc.ca/eng/acts/c-46/page-23.html#h-118363 .
5. *Das Deutsche Strafgesetzbuch*, *Deutschland*, 2021, https://www.gesetze-im-internet.de/stgb/__202a.html .
6. Ministerio de Asuntos Exteriores y de Cooperación. Oficina de Interpretación de Lenguas, *Protocolo adicional al Convenio sobre la ciberdelincuencia relativo a la penalización de actos de índole racista y xenófoba cometidos por medio de sistemas informáticos,* España, 2005, https://www.plataformaong.org/conferencia/wp-content/uploads/2014/10/Protocolo_adicional_convencion_cibercrimen.pdf

Nacional


1. Código Nacional de Procedimientos Penales, México, 2021, http://www.diputados.gob.mx/LeyesBiblio/pdf/CNPP_190221.pdf .
2. Código Penal de Yucatán, México, 2021, http://187.157.158.150:3001/legislacion/codigos/13af0b6e2a69c4eafc8911c477281295_2021-10-01.pdf .
3. Código Penal del Estado de México, http://legislacion.edomex.gob.mx/sites/legislacion.edomex.gob.mx/files/files/pdf/cod/vig/codvig006.pdf .
4. Código Penal para el Estado de Veracruz de Ignacio de la Llave, México, 2021,https://www.legisver.gob.mx/leyes/LeyesPDF/CPENAL15112021.pdf
5. Código Penal para la Ciudad de México, https://paot.org.mx/centro/codigos/df/pdf/2022/COD_PENAL_DF_10_06_2022.pdf .
6. Ley de Protección a los animales de la Ciudad de México, https://paot.org.mx/centro/leyes/df/pdf/2018/LEY_PROTECCION_ANIMALES_04_05_2018.pdf .
7. Ley Federal de Protección de Datos Personales en Posesión de los Particulares, https://www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf de 17 de noviembre de 2022, 17:30 hrs
8. Ley Federal del Derecho de Autor, https://www.diputados.gob.mx/LeyesBiblio/pdf/122_010720.pdf .
9. Ley General de Títulos y Operaciones de Crédito, http://www.diputados.gob.mx/LeyesBiblio/pdf/145_220618.pdf .
10. Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de Particulares, https://www.diputados.gob.mx/LeyesBiblio/regley/Reg_LFPDPPP.pdf .

## OTRAS FUENTES


1. Acurio del Pino, Santiago, *Delitos informáticos generalidades*, 2016, https://www.oas.org/juridico/spanish/cyb_ecu_delitos_inform.pdf .
2. Ada Byron, Augusta, *Nota G del bosquejo de la Máquina Analítica (El primer programa de ordenador)*, trad. de Rodríguez Alberich, Gabriel, https://notage.org/ .
3. Aguilar Cuevas, Magdalena, *Las tres generaciones de los Derechos Humanos*,https://revistascolaboracion.juridicas.unam.mx/index.php/derechos-humanos-emx/article/viewFile/5117/4490 .
4. Ahorra seguros, *¿Cómo prevenir el carding al contratar un seguro de auto?,* 2020, https://ahorraseguros.mx/blog/que-es-carding/ .
5. Almanza Altamirano, Frank, *Clase gratuita sobre Imputación objetiva*, https://www.youtube.com/watch?v=66zdlgXt0J8 .
6. Amazon Web Services, *¿Qué es DNS?*, https://aws.amazon.com/es/route53/what-is-dns/ .
7. Balmaceda Hoyos, Gustavo, *El delito de estafa informática en el derecho europeo continental*, Chile, 2011, https://dialnet.unirioja.es/descarga/articulo/4200389.pdf .
8. Bautista García, Iván Jahel, *VPN: ¿Qué es y para qué sirve?,* https://www.servnet.mx/blog/vpn-que-es-y-para-que-sirve .
9. Belcic, Iván, *¿Qué es la inyección de SQL y cómo funciona?,* Avast, 2021, https://www.avast.com/es-es/c-sql-injection .
10. Belcic, Iván, *Guía esencial del phishing: cómo funciona y cómo defenderse,* Avast, 2021, https://www.avast.com/es-es/c-phishing .
11. Belloch Ortí, Consuelo, *Las Tecnologías de la Información y Comunicación*, https://www.uv.es/~bellochc/pdf/pwtic1.pdf .
12. BrightPlanet, *Clearing up confusion – Deep web vs Dark web,* 2014, https://brightplanet.com/2014/03/27/clearing-confusion-deep-web-vs-dark-web/ .

13. Ciberseguridad,*Hacktivismo*,https://ciberseguridad.com/amenzas/hacktivismo/ .
14. CISCO, *¿Qué es la ciberseguridad?*, https://www.cisco.com/c/es_mx/products/security/what-is-cybersecurity.html .
15. CISCO, *¿Qué es un Router?*, https://www.cisco.com/c/es_mx/solutions/small-business/resource-center/networking/what-is-a-router.html .
16. CISCO, disponible en: https://contenthub.netacad.com/legacy/I2CS/2.1/es/index.html#1.3.1.2 .
17. Consejo de Europa, *Adhesión al Convenio de Budapest sobre la Ciberdelincuencia: Beneficios*, 2021, https://rm.coe.int/cyber-buda-benefits-junio2021a-es/1680a2e4de .
18. COPADATA, *¿Qué es SCADA?,* https://www.copadata.com/es/productos/zenon-software-platform/visualizacion-control/que esscada/#:~:text=SCADA%20es%20el%20acr%C3%B3nimo%20de,registrar%20datos%20de%20sus%20operaciones. .
19. Cyberbullying, *¿Qué es el cyberbullying?,* 2016, https://www.gob.mx/ciberbullying/articulos/que-es-el-ciberbullying .
20. Daza, Santiago, *¿Qué es John the Ripper?*, 2021, https://behacker.pro/que-es-john-the-ripper/ .
21. De la Hera, Cristina, *Historia de las redes sociales: cómo nacieron y cuál fue su evolución*, 2022, https://marketing4ecommerce.net/historia-de-las-redes-sociales-evolucion/ .
22. Deutsche Welle, *Facebook suaviza normas que permiten discursos violentos*, 2022, https://www.dw.com/es/facebook-suaviza-normas-que-permiten-discursos-violentos/a-61090134 .
23. Diario informe, *¿Qué significa "Meatspace" ?*, https://diarioinforme.com/que-significa-meatspace/ .

24. Diccionario panhispánico del español jurídico, *Concepto neoclásico de delito*, https://dpej.rae.es/lema/concepto-neoclásico-de-delito .
25. Doménech Pujol, Álvaro et al., *Un viaje a la historia de la informática*, Editorial Universitat Politécnica de Valéncia, España, 2016, https://museo.inf.upv.es/wp-content/uploads/2021/04/Un-viaje-a-la-historia-de-la-informatica.pdf .
26. Dr. Villazán Olivarez, Francisco José, *Manual de informática I*, https://www.upg.mx/wp-content/uploads/2015/10/LIBRO-31-Manual-de Informatica.pdf .
27. Dra. Bardales Lazcano, Erika et al, *Mesa 1: "COMPLIANCE"*, II Congreso Internacional Virtual de Derecho Penal, 2021, https://fb.watch/bGnSrE7Lyj/
28. Equipo de soporte de SSL, *¿Qué es HTTPS?*, https://www.ssl.com/es/preguntas-frecuentes/que-es-https/ .
29. ESGEEKS, *¿Qué es un Script Kiddie? Características y peligros*, https://esgeeks.com/script-kiddie-que-es/ .
30. Esparragoza, Luis, *Identificar e interrumpir: así funciona la nueva ley de vigilancia en Australia*, Criptonoticias, 2021, https://www.criptonoticias.com/regulacion/identificar-interrumpir-asi-funciona-nueva-ley-vigilancia-australia/ .
31. Estrella Contreras, Antonio, *La calculadora programable Programma 101*, https://museo.inf.upv.es/programma-101-4/ .
32. Expediente 82/2021, Sentencias y datos de expedientes, abril de 2022, https://www2.scjn.gob.mx/ConsultaTematica/PaginasPub/DetallePub.aspx?AsuntoID=283367 .
33. Expediente Varios 912/2010, Sentencias y datos de expedientes, abril de 2011,https://www2.scjn.gob.mx/ConsultaTematica/PaginasPub/DetallePub.aspx?AsuntoID=121589 .
34. ExpressVPN, *¿Qué es un túnel VPN?*, 2021, https://www.expressvpn.com/es/what-is-vpn/vpn-tunnel .
35. Facultad de biblioteconomía y documentación, *Ada Byron 1815 – 1852,* https://www.ugr.es/~anamaria/mujeres-doc/biogabyron.htm .

36. Garberí Penal, Boutique especializada en Derecho Penal, Compliance y Defensa Legal, *¿Qué es el compliance penal?*, 2017, https://www.garberipenal.com/corporate-programa-compliance-penal/ .
37. GCFGlobal, *¿Qué es Hardware y software?*, https://edu.gcfglobal.org/es/informatica-basica/que-es-hardware-y-software/1/ .
38. Gobierno de Argentina, *Grooming Qué es y cómo prevenirlo*, 2021, https://www.argentina.gob.ar/grooming .
39. Gómez, Fernanda y Luchadoras MX, *Violencia sexual digital. Un balance de la Ley Olimpia en CDMX*, 2019, https://luchadoras.mx/un-balance-de-la-ley-olimpia-en-cdmx/ .
40. González, Ana, Datos biométricos - ¿Qué y cuáles son? ¿Cómo cumplir con la ley?, 2019, https://ayudaleyprotecciondatos.es/2019/02/15/datos-biometricos/ .
41. González, Sara, *Trump y Twitter: ¿Qué es la sección 230 y por qué estás oyendo hablar de ella?,* 2020, https://www.newtral.es/trump-y-twitter-que-es-la-seccion-230-y-por-que-estas-oyendo-hablar-de-ella/20200529/ .
42. Grustniy, Leonid, *Darknet, Darkweb, Deep web y Surface web: las diferencias*, https://latam.kaspersky.com/blog/deep-web-dark-web-darknet-surface-web-difference/20962/ .
43. Guerrero Santillán, Elvia Celina, El derecho al olvido digital en México, https://www.itei.org.mx/v3/micrositios/cdc/wp-content/uploads/2020/04/7_2018_7_guerrero.pdf .
44. Hidden wiki, *Hidden wiki*, https://thehiddenwiki.org.
45. Historia de la informática, *La crisis del Software,* 2011, https://histinf.blogs.upv.es/2011/01/04/la-crisis-del-software/ .
46. Instituto de Ingeniería UNAM, *Hackers*, http://www.ii.unam.mx/es-mx/AlmacenDigital/CapsulasTI/Paginas/hackers.aspx .
47. Instituto Nacional de Ciberseguridad, *Phishing*, España, https://www.incibe.es/aprendeciberseguridad/phishing .

48. Instituto Nacional de Ciencias Penales, *Delitos informáticos*, https://www.youtube.com/watch?v=ggg0v65j474
49. Jiménez Holguín, Noel Orlando, *Delito instantáneo, permanente y continuado*, 2018, https://www.youtube.com/watch?v=xQp5xi2Q5sE .
50. *Kali Linux Revealed. Mastering the Penetration Testing Distribution*, 2021, https://kali.training/downloads/Kali-Linux-Revealed-2021-edition.pdf .
51. Kaspersky, *¿Qué es el pharming y cómo evitarlo?*, 2021, https://latam.kaspersky.com/resource-center/definitions/pharming .
52. Kaspersky, *Doxing: definición y explicación*, https://latam.kaspersky.com/resource-center/definitions/what-is-doxing .
53. Kaspersky, *Hackers de sombrero negro, blanco y gris: definición y explicación*, 2021, https://latam.kaspersky.com/resource-center/definitions/hacker-hat-types
54. Kaspersky, *Qué es una dirección IP: definición y explicación*, 2021, https://www.kaspersky.es/resource-center/definitions/what-is-an-ip-address .
55. Kaspersky, *Stuxnet: Los orígenes*, 2014, https://latam.kaspersky.com/blog/stuxnet-los-origenes/4553/ .
56. La Secretaría de Seguridad ciudadana de la CDMX en su comunicado 1894, "invita a sensibilizar a los jóvenes sobre los riesgos de compartir fotos de su cuerpo en redes sociales", Secretaría de Seguridad Ciudadana, *1894: Para evitar que los menores de edad caigan en engaños de sexting, la SSC alerta a la ciudadanía y padres de familia, sobre cuentas apócrifas de personas públicas*, 2020, https://www.ssc.cdmx.gob.mx/comunicacion/nota/1894-para-evitar-que-los-menores-de-edad-caigan-en-enganos-de-sexting-la-ssc-alerta-la-ciudadania-y-padres-de-familia-sobre-cuentas-apocrifas-de-personas-publicas .
57. López, Alfred, *Los falsos textos que desde hace más de un siglo son utilizados para fomentar el odio antisemita*, Yahoo! News, 2021, https://es.noticias.yahoo.com/falsos-textos-que-desde-hace-mas-un-siglo-son-utilizados-para-fomentar-odio-antisemita-144756516.html?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuZ29vZ

2xlLmNvbS8&guce_referrer_sig=AQAAAIh0C1A2L5mMeD-2sngoEml4Tw9BOxPR6_F3jkgVTwe_RFjcMlWgW7b6AyFuv8DZaDNNkScTkNLaH8EhipNK3wcMr2kGhUhllUFc-zjll4UEDYlVxOsRqhLpKQbTiU5V8eBcQHpXeXRjMj9EFhxpLN3L56_n1gGQDNn_ZkgH49Lv .

58. Loredo González, Jesús Alberto y Ramírez Granados, Aurelio*, Delitos informáticos: Su clasificación y una visión general de las medidas de acción para combatirlo*, 2013, http://eprints.uanl.mx/3536/1/Delitos_informaticos.pdf .
59. LP Pasión por el derecho, *¿Cuáles son las clases de tipos penales? Bien explicado*, https://lpderecho.pe/cuales-son-las-clases-de-tipos-penales-bien-explicado/
60. Lukyanov, Denis, *El gran hermano te vigila: el impenetrable escudo dorado de china que "protege" su internet de EEUU,* Sputnik, 2019, https://mundo.sputniknews.com/20190523/escudo-dorado-de-china-protege-su-internet-de-eeuu-1087364992.html .
61. M., José Manuel, *Diferencias entre software de sistema y software de aplicación*, 2018, https://pc-solucion.es/2018/04/16/diferencias-entre-software-de-sistema-y-software-de-aplicacion/
62. Malumbres Cervera, Eduardo Pérez, *Carding, ¿Cómo nos la lían?*, https://derechodelared.com/carding/ .
63. Marker, Graciela, *Software libre vs Software propietario*, https://www.tecnologia-informatica.com/software-libre-propietario/ .
64. Martínez, Raúl, *Ataques al navegador del usuario usando BEEF*, 2016, https://noticiasseguridad.com/hacking-incidentes/ataques-al-navegador-del-usuario-usando-beef/
65. Martínez-Villalba, Juan Carlos Riofrío, "La cuarta ola de Derechos Humanos: Los Derechos Digitales", *Revista Latinoamericana de Derechos Humanos*, 2014, Volumen 25, I Semestre 2014, https://www.corteidh.or.cr/tablas/r33897.pdf .

66. McAfee, *9 tipos de hackers y sus motivaciones*, 2019, https://www.mcafee.com/blogs/languages/espanol/9-tipos-de-hackers-y-sus-motivaciones/ .
67. Morales-Luna, Guillermo, *Números computables y números reales,* https://miscelaneamatematica.org/download/tbl_articulos.pdf2.8895cee46b870f64.353630322e706466.pdf .
68. Morán Breña, Carmen, *La "Ley Ingrid" se aprueba antes de que se resuelva el "caso Ingrid"*, El País, 2021, https://elpais.com/mexico/2021-02-25/la-ley-ingrid-se-aprueba-antes-de-que-se-resuelva-el-caso-ingrid.html .
69. Oxford Languages, https://www.lexico.com/es/definicion/red_social .
70. Página 12, *Hackean datos Mercado Libre y Mercado Pago y hay preocupación por la filtración de datos de 300 mil usuarios*, 2022, https://www.pagina12.com.ar/406594-hackean-datos-mercado-libre-y-mercado-pago-y-hay-preocupacio .
71. Pandasecurity, *¿Qué es un exploit?,* https://www.pandasecurity.com/es/security-info/exploit/ .
72. Parliament of Australia, *Serveillance Legislation Amendment (Identify and Disrupt) Bill 2021*, Australia, 2021, https://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/Bills_Search_Results/Result?bId=r6623 .
73. Parra, Edgar, *Manual de Armitage en español*, 2014, https://www.dragonjar.org/manual-de-armitage-en-espanol.xhtml .
74. Pascual Estapé, Juan Antonio, *Qué es una distribución Linux, en qué se diferencian y cómo elegir una*, 2017, https://computerhoy.com/noticias/software/que-es-distribucion-linux-que-diferencian-como-elegir-54784 .
75. Patrizio, Andy, *¿Qué es una dirección IP?*, 2022, https://www.avast.com/es-es/c-what-is-an-ip-address
76. Periódico oficial Gaceta del Gobierno y LEGISTEL, Poder Judicial de la Federación, Suprema Corte de Justicia de la Nación, acción de inconstitucionalidad 136/2021 de miércoles 12 de julio de 2023,

https://legislacion.edomex.gob.mx/sites/legislacion.edomex.gob.mx/files/files/pdf/gct/2023/julio/jul121d.pdf

77. Pérez, Christian, “Colossus, el primer ordenador a gran escala que ayudó a ganar la segunda guerra mundial”, *Muy interesante*, 2020, https://www.muyinteresante.es/tecnologia/articulo/colossus-el-primer-ordenador-a-gran-escala-que-ayudo-a-ganar-la-segunda-guerra-mundial-251600107042 .
78. Plascencia Villanueva, Raúl, *Teoría del delito*, UNAM Instituto de Investigaciones Jurídicas, México, 2004, https://archivos.juridicas.unam.mx/www/bjv/libros/1/44/5.pdf .
79. Quintero, Carla, *Cuáles son las redes sociales más populares de Rusia*, marketin4ecommerce mx, 2022, https://marketing4ecommerce.mx/cuales-son-las-redes-sociales-mas-populares-de-rusia/ .
80. Real Academia Española, *Diccionario de la Lengua Española*, 2020, https://dle.rae.es/cibern%C3%A9tico .
81. Real Academia Española, *Diccionario de la lengua española*, 2021, https://dle.rae.es/programa .
82. Real Academia Española, https://dle.rae.es/red .
83. Resiliente Digital, *Cloud Hopper: La pesadilla de ciberespionaje chino que nunca acaba*, 2020, https://resilientedigital.com/cloud-hopper-la-pesadilla-de-ciberespionaje-chino-que-nunca-acaba/ .
84. Rizaldos, Héctor, *Qué es metasploit framework*, 2018, https://openwebinars.net/blog/que-es-metasploit/ .
85. Rizaldos, Héctor, *Qué es un payload*, https://openwebinars.net/blog/que-es-payload/ .
86. Robles Garay, Oscar, *El riesgo de “nacionalizar” internet*, Iacnic News, 2017, https://prensa.lacnic.net/news/gobernanza-de-internet/el-riesgo-de-nacionalizar-internet .
87. Rodríguez Magariños, Faustino Gudin, *Nuevos delitos informáticos: Phishing, Pharming, Hacking y Cracking*,

https://web.icam.es/bucket/Faustino%20Gud%C3%ADn%20-%20Nuevos%20delitos%20inform%C3%A1ticos.pdf .

88. Rojas – Quiñones, Sergio y Mojica – Restrepo, Juan Diego, “De la causalidad adecuada a la imputación objetiva en la responsabilidad civil colombiana”, 2014, núm. 129, junio – diciembre 2014, Colombia, https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwjpydS4_av7AhXSKEQIHTZRCEMQFnoECCYQAQ&url=https%3A%2F%2Frevistas.javeriana.edu.co%2Findex.php%2Fvnijuri%2Farticle%2Fview%2F11949%2F9784&usg=AOvVaw3E-PnaQmKd81Df5-NCHBzc .
89. Romero, Sarah, *¿Cuántos tipos de hackers existen?,* Muy interesante, 2019, https://www.muyinteresante.es/tecnologia/articulo/que-es-un-hacker-de-sombrero-gris-831473842564 .
90. RT Documentales, *Censura Virtual, ¿cuál es el futuro del internet?*, 2021, https://www.youtube.com/watch?v=ED_zIizL8zo .
91. Save the Children, *Grooming qué es, cómo detectarlo y prevenirlo,* 2019, https://www.savethechildren.es/actualidad/grooming-que-es-como-detectarlo-y-prevenirlo .
92. Secretaría de Seguridad Ciudadana, *2452: La Policía Cibernética de la SSC informa sobre los riesgos de descargar y utilizar aplicaciones de préstamos a través de la red pública de internet*, 2021, https://www.ssc.cdmx.gob.mx/comunicacion/nota/2452-la-policia-cibernetica-de-la-ssc-informa-sobre-los-riesgos-de-descargar-y-utilizar-aplicaciones-de-prestamos-traves-de-la-red-publica-de-internet .
93. System & Software Engineering, *La Máquina Analítica de Babbage*, https://www.gtd.es/es/blog/la-maquina-analitica-de-babbage .
94. The Tor Project, Inc., *Navegar en privado. Explora libremente*, https://www.torproject.org/ .
95. Torné, Kike, *HASH. La función que nos garantiza la autenticidad del archivo*, ATI Spain Tips, 2017, https://www.atispain.com/blog/hash-la-funcion-que-nos-garantiza-la-autenticidad-del-archivo/ .

96. Trevilla, Manuel, ¿Qué son los NFT y porque todos hablan de ellos?, El Financiero, 2022, https://www.elfinanciero.com.mx/manuel-trevilla-fenomenos-digitales/2022/01/13/nft-tecnologia-basada-en-blockchain-que-es-mas-que-moda/ .
97. Universidad Autónoma de Madrid, *¿Tienes clara la diferencia entre Darkweb, Deepweb y Darknet?*, https://www.uam.es/uam/vida-uam/bibliotecas/biblioteca-politecnica/noticias/diferencias-darkweb-deepweb-darknet .
98. Universidad de Cádiz, *Introducción al derecho penal,* España, https://ocw.uca.es/mod/book/view.php?id=1237&chapterid=14 .
99. Universidad de Jaén, *Nombres de dominio (DNS),* https://www.ujaen.es/servicios/sinformatica/catalogo-de-servicios-tic/nombres-de-dominio-dns .
100. Universidad de Navarra, *Elementos subjetivos del injusto*, España, http://www.unav.es/penal/crimina/topicos/elementossubjetivosdelinjusto.html .
101. Universidad Internacional de Valencia, *¿Qué se considera una infraestructura crítica?*, https://www.universidadviu.com/es/actualidad/nuestros-expertos/que-se-considera-una-infraestructura-critica#:~:text=Las%20estructuras%20cr%C3%ADticas%20incluyen%20las,la%20electricidad%20o%20el%20gas .
102. Universidad Libre Colombia, *La evolución del computador*, 2015, https://www.unilibre.edu.co/bogota/ul/noticias/noticias-universitarias/256-la-evolucion-del-computador.
103. Valencia Santiago, Iván, *Hacker, Crackers, Lamers, Script Kiddies y Phreakers ¿Quiénes son?*, 2018, https://seguridad.cicese.mx/alerta/335/Hacker,-Crackers,-Lamers,-Script-Kiddies-y-Phreakers-Quienes-son .
104. Valverde Esquinas, Patricia, “Conditio sine qua non y concreción del riesgo en el resultado: cómo eliminar un paso repetitivo en el análisis de la

imputación objetiva al tipo", *Revista Penal México*, Vol. 8, núm. 14-15, marzo 2018 – febrero 2019, México, https://revistaciencias.inacipe.gob.mx/index.php/01/article/view/295/253 .

105. Vera, Amir, et al., *Alguien trató de envenenar con lejía a la población de una ciudad de Florida hackeando el sistema de tratamiento de agua, dice el sheriff*, 2021, https://cnnespanol.cnn.com/2021/02/08/florida-envenenar-lejia oldsmar/ .

106. Wilder Tukey, John, "The teaching of concrete mathematics", *The American mathematical monthly*, 1958, Vol. 65, No. 1, https://www.maa.org/sites/default/files/pdf/CUPM/first_40years/1958-65Tukey.pdf .

107. Wilson, Bill, *John Blankerbaker, El hombre que creó la primera computadora personal de la historia*, BBC News, 2015, https://www.bbc.com/mundo/noticias/2015/11/151109_tecnologia_john_blankenbaker_hombre_creo_primera_computadora_personal_lv .

108. Wireshark, *About Wireshark*, 2021, https://www.wireshark.org/

109. Zambrano Pasquel, Alfonso, *La Teoría de la Autoría Mediata del Profesor Claus Roxin*, 2015, https://www.youtube.com/watch?v=c58MiMMp0zw