UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE DERECHO

SEMINARIO DE DERECHO PENAL

"REPLANTEAR LA TIPIFICACIÓN DEL CIBERDELITO DE ROBO DE DATOS CON EL OBJETIVO DE AMPLIAR LA PROTECCIÓN AL BIEN JURÍDICO DE LOS MISMOS"

TESIS

PARA OBTENER EL TÍTULO DE:

LICENCIADO EN DERECHO

PRESENTA:

LUIS ANTONIO CISNEROS REYES

ASESOR: MTRO. RODOLFO ROMERO FLORES

CIUDAD UNIVERSITARIA 2022

Dedicatoria

A mi madre, quien ni aún en las adversidades, dejó de confiar en mí.

A todos aquellos que me han apoyado en todo momento, de forma cercana y a la distancia.

A mis compañeros, amigos y familiares, quienes sembraron en mí la curiosidad de un mundo futuro.

A esas dos personitas especiales que amo y siempre vivirán en mi corazón.

Agradezco a mi madre y padre, por darme la vida, en especial a mi adorada señora, quien a pesar de las adversidades de la vida, nos muestra lo increíble que puede ser el mundo, luchando siempre por una vida y un espacio mejor, aún recuerdo sus pies cansados y sus ojos rojos de desvelo, gracias mama.

Gracias a dios por cuidar mis pasos, por darme un soplo de vida, un sol que calentara y una esperanza de creer en alguien, y que mejor que en ti, en la bondad de tus enseñanzas.

Gracias a todas aquellas personas que a lo largo de la vida me han mostrado lo difícil y hermoso que puede llegar a ser el existir, compartiendo charlas, un camino de unas horas, jornadas enteras bajo el sol y un plato de comida.

Agradezco al Maestro Julio Téllez Valdés, por su trabajo que me permitió aclarar muchas dudas, y me abrió las puertas al futuro derecho informático.

Agradezco al Maestro Bernardo Anwar Azar López, por inspirar con su ejemplo, desde el momento en que llegue a la Facultad de Derecho.

Agradecimientos

Gracias, querida Universidad Nacional Autónoma de México, por brindarme oportunidades dentro y fuera de tus aulas, por fortalecer mis sueños, por mostrarme que la calidad humana es el honor más grande de un individuo, porque han sido miles, millones, un infinito mismo de grandes mentes y pensamientos que te han construido, y así, sintiendo su espíritu aguerrido me mantengo.

Tabla de abreviaturas

La siguiente es una lista de abreviaturas utilizadas en el presente trabajo de tesis:

Abreviatura	**Significado**
ARCO	Acceso, Rectificación, Cancelación u Oposición sobre el tratamiento de sus datos
CURP	Clave Única de Registro de Población
CC	Código de Comercio
CPDF	Código Penal para el Distrito Federal
CPES	Código Penal del Estado de Sinaloa
CPEUM	Constitución Política de los Estados Unidos Mexicanos
FELINAI	Firma Electrónica del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales
IMPI	Instituto Mexicano de la Propiedad Industrial
IMSS	Instituto Mexicano del Seguro Social
INAI	Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales
LDPPSOCDMX	Ley de Protección de Datos Personales en Posesión de Sujetos Obligados de la Ciudad de México
LIC	Ley de Instituciones de Crédito
LFDA	Ley Federal del Derecho de Autor
LFPDPPP	Ley Federal de Protección de Datos Personales en Posesión de los Particulares
LFTAIP	Ley Federal de Transparencia y Acceso a la Información Pública
LFPC	Ley Federal de Protección al Consumidor
LFPPI	Ley Federal de Protección a la Propiedad Industrial
LGPDPPSO	Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados
OEA	Organización de los Estados Americanos
OMPI	Organización Mundial de la Propiedad Intelectual
LRITF	Ley para Regular las Instituciones de Tecnología Financiera
PROFECO	Procuraduría Federal del Consumidor
PSC	Prestadores de Servicios de Certificación
RAE	Real Academia Española
RLFDDPPP	Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares
RENAPO	Registro Nacional de Población
SHCP	Secretaría de Hacienda y Crédito Público
SAT	Servicio de Administración Tributaria
UNODC	*United Nations Office on Drugs and Crime*

Índice

Pág.

Capítulo Tercero

Responsabilidad jurídica de quienes participan de forma conjunta en el robo de datos

Capítulo Cuarto

Generalidades del Robo de Datos

Capítulo Quinto

Análisis de resultados y conclusiones

Introducción

Frente a la revolución digital y los múltiples fenómenos delincuenciales asociados a la misma, esta tesis busca demostrar lo importante que es el derecho penal ante la protección de bienes jurídicos emergentes, así los datos e información.

La informática, y los delitos relacionados a esta, como parteaguas histórico, científico y social, al relacionarse con el derecho, se debe realizar una revisión del mismo en el contexto actual, lo que nos permite saber qué áreas se encuentra protegidas y cuáles no, para no ser impactados por vacíos jurídicos frente a este emergente fenómeno delictivo, que atrae conductas delictivas surgidas del mundo de la información.

La revisión jurídico conceptual, dogmática, documental o teórica, permitió obtener información de fuentes documentales, como sitios de internet, libros, documentos, revistas, tratados, manuales, videos, enciclopedias, conferencias, cursos, etc., mediante la esencia de la investigación empírica, realista o de campo, esto es, tomando fuentes de información por medio de la observación del comportamiento de las personas, cosas, instituciones o circunstancias ante un fenómeno social que repercute de manera negativa en la normativa, el delito informático, así como en el libre desarrollo de las personas físicas, morales y entes del Estado, conforme a diferentes hechos, logrando con el empleo de estas técnicas de investigación una denomina “Investigación Jurídica mixta” (García Fernández, D), utilizando los métodos de interpretación de la ley, técnicas documentales y técnicas de campo.

La presente investigación, se centra en el campo de las tecnologías de la información, así lo relacionado con los datos e información, tanto de las personas físicas, morales y entes del Estado, como de los dispositivos informáticos y sistemas de seguridad contenidos en múltiples sistemas

informáticos, señales que transportan información y medios de transporte de la misma, formas de almacenamiento, etc., para ello fue revisada una parte de la normativa tanto nacional como internacional, que nos permitirá ampliar la información y conocimientos relacionados a los temas propuestos.

De esta manera, las vertientes y especialidad de quienes cometen un ciberdelito, dificultan su estudio y tipificación, por lo que al ser revisado el delito de robo de datos en la normativa actual, se logrará ampliar la protección al bien jurídico de los datos y por ende a las personas físicas y morales.

En ese tenor, al ser revisadas las leyes de protección de datos personales, códigos penales, leyes especiales como la de la Firma Electrónica Avanzada y ley federal de protección al consumidor, leyes de otros países como el Código Penal Argentino y Código Penal de Colombia, así como nuestra Carta Magna y tratados internacionales, damos cuenta de la multiplicidad de datos e información existentes, lo que nos ha llevado a poder alimentar esta investigación con nuevos enfoques y planteamientos, para la protección del bien jurídico de los datos e información, ante el ciberdelito y robo de estos.

Como parte del primer capítulo, fue estudiado el concepto de datos, encontrándose diferente tipos, así datos relacionados con las personas físicas, morales, entes del Estado, sistemas informáticos, señales y red, mostrando el impacto que genera el robo de datos e información, así como las consecuencias de la utilización ilegal de los mismos, frente a su protección.

Dentro del segundo capítulo, protocolos normativos de las empresas, se establece que los protocolos de seguridad informática, permiten que los datos e información se encuentren protegidos ante cualquier tipo de situación que ponga en riesgo a los mismos, lo que conlleva a adoptar el denominado documento de seguridad, en el cual se establecen las medidas de seguridad técnicas, físicas y administrativas adoptadas por el responsable del tratamiento y manejo de los datos, para garantizar la confidencialidad, integridad y disponibilidad de los datos personales que Posee.

No olvidemos la importancia del análisis de riesgo que es realizado por medio de ataques controlados por las empresas, pruebas de penetración o *Pent Test* que permiten saber y documentar cuales son las brechas de seguridad, evaluando la seguridad de los sistemas informáticos, redes y aplicaciones, ya que las empresas prestadoras de servicios, en el ámbito de datos e información, tienen la responsabilidad de mantener estándares altos de seguridad, lo que conlleva no solo a analizar las nuevas formas de protección de los datos e información como la firma digital y el denominado *block chain*, sino también a revisar los términos y condiciones.

Dentro del capítulo tercero, se delimita la posibilidad de extender el catálogo de delitos relacionados con la delincuencia organizada, lo que conlleva a adoptar delitos informáticos realizados de forma grupal, artículo 2 de la Ley Federal contra la Delincuencia Organizada. Así mismo se revisa la coautoría y participación en los delitos informáticos, responsabilidad de los prestadores de servicios y la regulación del comercio electrónico, la importante cooperación entre Estados frente al estudio, manejo, investigación y aplicación de la ley penal.

Mientras que en el capítulo cuarto, se encontraron múltiples conductas relacionadas con los delitos informáticos, así como algunas relacionadas con el robo de datos e información, tomando parte de la normativa nacional para poder determinar aciertos y limitantes de la misma, siendo de suma importancia el concepto de sistema informático, pues él mismo nos da la pauta para delimitar los elementos que permiten el tratamiento de datos, generando, enviando, recibiendo, procesando y almacenando información de cualquier forma y por cualquier medio.

Se tomaron y analizaron elementos importantes como bienes jurídicos, sujeto activo y pasivo, conductas que permitan configurar el delito informático y por ende el robo de datos e información, así como las características del

delincuente informático como fundamento de la aplicación de penas y medidas de seguridad.

Capítulo Primero

Protección de los datos que son tratados por Empresas privadas y Órganos del Estado

I. Concepto de datos

Diversos son los datos que pueden ser robados de un ordenador o sistema, por lo que es de suma importancia que la tipificación de los mismos sea basada en las categorías entre las cuales pudiesen formar parte, esto es si son datos de información nacional, reservada o secreta, si son datos que permiten la identificación de las personas, si forman parte de la información de las empresas, así como el uso que después del hurto o robo se realice, cómo serán utilizados los mismos y sobre todo, el daño al bien jurídico, siendo característico si el mismo fue masificado, extendido a la población general o no.

El concepto de datos consultado en la Real Academia Española, nos menciona que el término dato proviene del latín *datum* que significa "lo que se da", así continuando con la misma RAE el significado actual en informática es "Información dispuesta de manera adecuada para su tratamiento por una computadora", *Google*[1] nos refiere que un dato es una representación simbólica (numérica, alfabética, algorítmica, espacial, etc.) de un atributo o variable cuantitativa o cualitativa.

Los datos describen hechos empíricos, sucesos y entidades", "es un valor o referente que recibe el computador por diferentes medios, los datos representan la información que el programador manipula en la construcción de una solución o en el desarrollo de un algoritmo"; "un dato por sí mismo no constituye información, es el procesamiento de los datos lo que nos proporciona información", por su parte Rafael Fernández en su Glosario Básico Inglés

[1]Google Sites, "Datos". Informática, *https://sites.google.com/site/informatica123325871/datos* de 25 de mayo de 2022, 09:15 p.m.

conceptualiza de forma acertada que un dato[2] es la “unidad mínima entre las que componen una información”.

Por su parte de las significaciones anteriores podemos entender que los datos son representaciones simbólicas, las cuales al ser manipuladas por medio de un computador y/o sistema informático, darán paso a la información, en ese sentido la protección al bien jurídico de los datos, es prioritaria en el contexto actual, pues por medio de datos se forman imágenes, se identifican sonidos, se comparte información entre personas físicas y morales, se determina la personalidad de las ciudadanas y los ciudadanos, se puede acceder a mapas, ubicaciones, cuentas bancarias, ciudades virtuales, monedas virtuales, prácticamente todo lo imaginable hoy es transformado en datos por quien manipule un ordenador y/o sistema.

II. Robo de datos

Obtener datos de forma ilícita, es una de las actividades delincuenciales más lucrativas en la actualidad, la responsabilidad del tratamiento de datos e información por parte de empresas privadas y Órganos del Estado, deja al descubierto que los delincuentes informáticos han desarrollado multiplicidad de técnicas y modos de operar, permitiendo con ello acceder a datos e información no solamente de la población o personas físicas, si no que de igual forma atentan contra los bienes y patrimonio de las empresas o personas morales, así como de las instituciones del Estado, poniendo en riesgo secretos industriales, economía, infraestructura, integridad de sus clientes y de la misma empresa, etc.

Las bases de datos son comercializadas obteniendo jugosas ganancias pues el uso que hacen de ellas quienes las roban o adquieren, ha permitido que diversas empresas quiebren o sean desprestigiadas con el uso

[2]Calvo, Rafael, “Glosario Básico Inglés-español para usuarios de internet”, Asociación de Tiendas de Informática, España, 4a. d., 1994-2001, *https://www.um.es/documents/3239701/10856915/glosario_internet_ingles.pdf/5eecfce7-5e5f-4800-9b8e-915678546dc7,* de 27 de mayo de 2021, 10:00 p.m.

malintencionado de su información, instituciones como la Secretaría de Hacienda y Crédito Público (en adelante SHCP), el Instituto Mexicano del Seguro Social (en adelante IMSS), el Servicio de Administración Tributaria (en adelante SAT), así como una variedad de instituciones, diferentes bancos y diversas empresas que tienen sus operaciones en el país, ha permitido un creciente robo de identidad, dando como consecuencia atentar al acceder a recursos, créditos u otros beneficios de quienes han sido víctimas del robo de sus datos e información, otras veces el acceso ilícito por medio de spams e ingeniería social, logra que las preferencias de los usuarios de servicios de internet y redes sociales, sean estudiadas y manipuladas para obtener mayor información y vulneración de los mismos, en muchos otros casos bandas de criminales, coludidos con empleados de Instituciones del Estado, roban datos e información que permitirá a su vez acceder a pensiones exorbitantes.

Actualmente nos encontramos ante un fenómeno con multiplicidad de variantes y su constante evolución, algunas de ellas penetran de forma incógnita por medio del *Wifi* e *IP*, mientras que en otras, son conectados pequeños dispositivos que enviaran la información a quien los manipule e inserten, *phishing*[3] (por ingeniería social*), spear phishing*[4], malware[5], *kayloggers*[6] (código malicioso-dispositivos-pulsaciones del teclado), *form grabbing* [7](los

[3]Cfr,. Tugurium, "Pescar, engañar. Técnica que consiste en atraer mediante engaños a un usuario hacia un sitio Web falso, con la intención de obtener información sensible", Glosario Terminología Informática, *http://www.tugurium.com/gti/termino.php?Tr=phishing,* de 31 de mayo de 2021, 07:00 p.m.

[4]Cfr., Tugurium, "Arponear. Técnica de *"phishing"* dirigida contra un objetivo concreto. El ataque se realiza contra una organización o grupo, no para robar información individual, si no para terminar obteniendo acceso a la organización. Implica una elaboración más rigurosa para lograr mayor credibilidad y la utilización más sofisticada de ingeniería social", Glosario Terminología Informática, *http://www.tugurium.com/gti/termino.php?Tr=spear%20phishing&Tp=T&Or=0*, de 31 de mayo de 2021, 07:15 p.m.

[5] Cfr., Tugurium, "*software* malicioso, código -, *[malware]*. *Software* hostil que se instala sin el consentimiento informado del usuario vía un sitio web, un correo electrónico o software gratuito como juegos o salvapantallas generalmente para beneficio de un tercero. Además de la presencia de anuncios o alteraciones en la configuración del navegador, controla la conducta del usuario en línea y transmite los datos a terceros no autorizados. Es un neologismo formado por los términos *"malicious"* y *"software"*, Glosario Terminología Informática, *http://www.tugurium.com/gti/termino.php?Tr=malware,* de 31 de mayo de 2021, 07:30 p.m.

[6]Cfr., Welivesecurity, "Qúe es un Keylogger: una herramienta para espiar. Un *keylogger* es un programa comúnmente utilizado por actores maliciosos para registrar y almacenar las pulsaciones del teclado con la intención de robar contraseñas o espiar en el equipo de la víctima", *https://www.welivesecurity.com/la-es/2021/03/04/que-es-keylogger-herramienta-para-espiar/,* de 31 de mayo de 2021, 08:15 p.m.

[7]Cfr., Kaspersky, "Agarre de forma. Técnica maliciosa que intenta robar las credenciales de autorización de un formulario de datos *web* antes de pasarlo a un servidor seguro mediante un protocolo cifrado", de *https://encyclopedia.kaspersky.com/glossary/form-grabbing/,* de 31 de mayo de 2021, 08:30 p.m.

cuales pueden ser utilizados por *bots*-uso de *botnets*[8]) siendo ayudados por otros tipos de *malwares* y trojanos, trojanos bancarios, ataques *man-in-the-browser* [9](*proxy* entre la víctima y el servicio legítimo), ofuscación de URL (técnica para ofuscar la lectura del texto), ataques de fuerza bruta y diccionario (combinación de multiplicidad de claves), clonación de páginas web, redireccionamiento *web* (redireccionar el dominio real hacia una dirección *IP* falsa [10]creada por el atacante), etc., son algunas de las formas como pueden ser robados los datos e información, como objetivo de las debilidades y vulnerabilidades del sistema, partiendo de los conocimientos de informática e infraestructura tanto material como económica del criminal.

El acceso ilícito a los sistemas informáticos, se configura con el robo de datos, en el entendido de que es la punta de lanza del robo de muchos otros tipos de datos e información, así como del uso delincuencial que se le dé a los mismos, ya sea con su venta o utilización, secuestros, desprestigio de personas, *bullying*, desvió de recursos, robo de identidad, entrega y venta de secretos empresariales, manipulación y amenazas, en fin todo aquello en que sea aplicado el antes mencionado robo, para cometer ilícitos.

Atentar contra la propiedad de las personas jurídicas y morales, como parte fundamental de este tipo de delitos, actuar sin su consentimiento contra su personalidad, contra todo bien jurídico que pudiese ser menoscabado o eliminado frente a conductas criminales consecuentes del robo de datos, vulnerando derechos humanos de las personas como son la vida, la integridad

[8]Cfr., Kaspersky, "¿Qué es un *bonet*?-Definición. La palabra *botnet* es la combinación de los términos "robot" *y "network"* en inglés. Los cibecriminales utilizan virus troyanos especiales para crear una brecha en la seguridad de los ordenadores de varios usuarios, tomar el control de cada ordenador y organizar todos los equipos infectados en una red de *"bots"* que el cibecriminal puede gestionar de forma remota", *https://www.kaspersky.es/resource-center/threats/botnet-attacks,* de 31 de mayo de 2021, 09:00 p.m.

[9]Cfr. Digital Bank LATAM, "¿Qué es *Man in the Browser (MITB)*? Es un ataque que ha evolucionado a partir del *Man In The Middle (MITM).* En concreto es un troyano que tras infectar una máquina es capaz de modificar páginas *webs*, contenidos o transacciones, de una manera invisible tanto para el usuario como para el servidor *web*", e. Banking, News, Consultado el 31/05/2021 de *https://www.ebankingnews.com/noticias/que-es-man-in-the-browser-el-nuevo-tipo-de-troyano-que-ataca-a-la-banca-006263,* de 31 de mayo de 2021, 09:15 p.m.

[10]Cfr., Mieres, J y Borghello, C, "Robo de información personal *online. "DNS: Domain Name Server* – Sistema de Nombres de Dominio. Consiste en un sistema que permite la traducción de los nombres de dominio por direcciones *IP* y viceversa", ESET para Latinoamérica, 2008, p. 9, *http://www.eset-la.com/pdf/prensa/informe/robo_informacion_online.pdf*, de 31 de mayo de 2021, 09:45 p.m.

psíquica y física, la igualdad, la propiedad personal y colectiva, la paz y la seguridad, la propiedad intelectual e industrial, y sobre todo, contra el acceso y uso de nuevas tecnologías, trasladándose en el tiempo por las huellas digitales que deja la información.

En el contexto empresarial y de Instituciones del Estado el acceso ilícito a los datos, se puede generar de diversas formas, ya sea sacando la información del área de trabajo en una memoria, poniéndola en la nube, o simplemente entrando a los sistemas de cómputo de quienes tienen acceso y hacen uso de información reservada y protegida por la empresa, por medio de formas y técnicas de acceso ilícito, descritas y no descritas anteriormente (pues constantemente se desarrollan nuevas formas), desprendiéndose la responsabilidad de estas empresas e Instituciones del Estado ante el uso y protección de todo tipo de datos que son tratados dentro y fuera de las mismas, como nos muestra la pandemia actual de COVID-19 y la nueva era acelerada de producir desde casa.

III. Posibles alcances del robo de datos

El robo de datos en alta escala, forma parte de una guerra ideológica y comercial como consecuencia del mismo desarrollo tecnológico de los Estados y todas aquellas empresas que forman parte de él o que prestan servicios al mismo, sin olvidar las que operan dentro del país y en diferentes regiones del mundo dando poder y fortaleza económica a sus socios en los lugares de donde son originarias, como consecuencia directa de una guerra de 4a y 5a generación[11], cuya principal característica es la tecnología y las intercomunicaciones.

[11]Cfr., Guevara, M, "Guerras de Cuarta y Quinta Generación en la desestabilización de Gobiernos (Siglo XXI)". "La guerra de cuarta generación" es el término usado por los analistas y estrategas militares de occidente, para describir la última fase de la guerra en el área de la tecnología informática y de las comunicaciones globalizadas. Según Martin Levi Van Creveld, historiador militar israelí e instructor de la escuela de guerra naval de EEUU", "El enfoque de la guerra de quinta generación es a través de medios electrónicos y de comunicación de masas, para generar desestabilización en la población a través de operaciones de carácter psicológico; como una táctica para mantener la desintegración política de la sociedad". Youtube, video, 2019, *https://www.youtube.com/watch?v=ci1grgq22ok&ab_channel=MagdielGuevara,* de 26 de mayo de 2021, 06:15 p.m.

Los delincuentes informáticos, al obtener los datos e información de las empresas del Estado y privadas, provocan una serie de afectaciones tanto económicas como morales a las mismas, dentro de los daños más comunes se encuentran las pérdidas económicas, secretos de producción industrial, y la confianza de sus consumidores, la reparación de daños con motivo de la pérdida de información es constante en este tipo de delitos pues existe el compromiso de garantizar el uso y tratamiento de los mismos de forma responsable, el detrimento de su imagen y prestigio es uno de los principales objetivos de la competencia desleal.

Sin embargo para los delincuentes informáticos la retribución económica de sus actos no se detiene en un solo ataque, en el entendido de que mucha de la información que se filtra como consecuencia de ataques bien preparados y con objetivos específicos, mostrando la capacidad de intercambio y obtención de información que será compartida con otros delincuentes que en un futuro podría permitir el desarrollo de nuevas formas de intrusión y ataques informáticos.

En la actualidad muchos son los ejemplos de ataques a sistemas empresariales y del Estado, los cuales han servido para desarrollar otros más, algunos como lo son *Stuxnet*[12] (que ataco a centrifugadoras para enriquecer uranio en *Natanz* Iran), *Petya*[13], *Wannacry* (*randsomware* que ataco a muchos sistemas corporativo de gran cantidad de empresas en el mundo), *Tryton* (*malware* para atacar específicamente sistemas industriales), *Crashoverride* (*malware* para atacar el sistema de distribución eléctrica de Ucrania), y muchos más que han vulnerado sistemas de control industrial, así los creadores y desarrolladores de sistemas de robo de datos e información empresarial emigran a múltiples contextos y latitudes poniendo en práctica sus conocimientos, algunas veces

[12]Cfr., Wikipedia, *"Stuxnet*. *Stuxnet* es un gusano informático que afecta a equipos con Windows, descubierto en junio de 2010 por *VirusBlokAda*, una empresa de seguridad ubicada en Bielorrusia. Es el primer gusano conocido que espía y reprograma sistemas industriales", 2021, *https://es.wikipedia.org/wiki/Stuxnet,* de 31 de mayo de 2021, 06:30 p.m.
[13]Cfr., Wikipedia, "*Petya* (*malware*). *Petya* es un *malware* de tipo *ransomware* reportado por la empresa *Heise Security. Petya* se esparce como troyano usando el popular sistema de archivos en la nube *Dropbox*.1 Mientras la mayoría de los *malware* de secuestro de computadoras selecciona los archivos a encriptar, *Petya* aumenta el daño potencial al impedir el arranque de la computadora", 2021, *https://es.wikipedia.org/wiki/Petya_(malware)*, de 31 de mayo de 2021, 06:45 p.m.

en beneficio de empresa y del Estado, mientras que la mayoría de las veces proceden a compartir sus conocimientos con futuros desarrolladores de ataques y criminales informáticos, lo que pone en constante riesgo a miles de empresas que operan en la actualidad con sistemas de seguridad que la mayoría de las veces son débiles ante los ataques más sofisticados, como consecuencia del desconocimiento de operar actual de los atacantes, la infraestructura no adecuada ante los mismos, la no actualización de los protocolos de seguridad informática, y la mala aplicación de los sistemas de seguridad más avanzados.

IV. Reglamentación

Al hablar de datos personales, entendemos que los mismos son aquellos que identifican a las personas, por lo que debemos acudir a su conceptualización, la que con base en el artículo 3º fracción IX de la Ley General de Protección de Datos Personales en posesión de Sujetos Obligados[14] (en adelante LGPDPPSO), se conceptualiza como, "*cualquier información concerniente a una persona física identificada o identificable. Se considera que una persona es identificable cuando su identidad pueda determinarse directa o indirectamente a través de cualquier información*".

En ese sentido algunos de los datos de las personas son el nombre, firma, huella, domicilio, teléfono particular o celular, etc., por lo que el reconocimiento por medio de sus datos personales, permite a quienes los utilizan como un medio de identificación, ya sea durante la venta y compra de productos, registros en las escuelas, empleos, inmobiliarias, arrendadoras, acceso a créditos, registros policiales, como muestra "Plataforma México", registros en los sistemas de salud, de Hacienda, en fin en todas aquellas empresas e instituciones tanto privadas como del Estado que hacen uso de los datos, dando el tratamiento adecuado que conforme a las leyes aplicables debe ser

[14]Artículo 3º, fracción IX, Ley General de Protección de Datos personales en Posesión de Sujetos Obligados, *https://www.dof.gob.mx/nota_detalle.php?codigo=5469949&fecha=26/01/2017*, de 01 de junio de 2021, 08:50 p.m.

realizado, los datos personales muestran las características de identificación de quienes son titulares de los mismos, siendo de suma importancia que sean protegidos pues estos van acompañados de datos sensibles que como refiere el artículo 3º fracción X[15], de la LGPDPPSO, pueden revelar *"aspectos como origen racial o étnico, estado de salud presente y futura, información genética, creencias religiosas, filosóficas y morales, afiliación sindical, opiniones políticas, preferencia sexual*", poniendo en peligro la imagen e integridad de las personas, base fundamental del derecho a la protección de los datos personales, en caso de ser utilizados de forma incorrecta.

Proteger los datos e información de las personas físicas y morales, es una labor que comienza con la concientización de responsabilidad adquirida en su tratamiento, así como en la responsabilidad jurídica en que incurren tanto las empresas como quiénes son responsables del manejo de los datos, ya que el derecho humano a la autodeterminación informativa definido, por el maestro español Pablo Murillo de la Cueva citado por Navarro, G.[16], como:

> *…el control que a cada uno de nosotros nos corresponde sobre la información que nos concierne personalmente, sea íntima o no para preservar, de este modo y en último extremo, la propia identidad, nuestra libertad y dignidad… implica necesariamente poderes que permita a su titular definir los aspectos de su vida que nos sean públicos que desea que se conozcan, así como las facultades que le aseguren que los datos que de su persona manejan informáticamente terceros son exactos, completos, actuales y que se han obtenido de modo leal y lícito.*

Este derecho a la autodeterminación informativa consiste, refiere el maestro Aveleyra Antonio, citado por Navarro, G[17].

> *… en la prerrogativa de la persona para disponer de la información que sobre sí misma exista en los registros de bases de datos, a fin de que esa información*

[15] Artículo 3, fracción X, LGPDPPSO, op. cit.
[16] Cfr., Navarro Jiménez, Gilberto R., "El derecho a la protección de información personal en México", p. 5, http://ordenjuridico.gob.mx/Congreso/2doCongresoNac/pdf/Navarro.pdf, de 07 de junio de 2021, 09:25 p.m.
[17] Navarro Jiménez, Gilberto R., Ibidem, p. 6.

sea veraz, actualizada, no intrusiva y con las garantías de seguridad y uso conforme a la finalidad para la que fue proporcionada…

En ese contexto la protección de los datos personales de todas las ciudadanas y ciudadanos, así como de las personas morales, es un derecho inherente, plasmado en el artículo 16 segundo párrafo de nuestra Constitución Política de los Estados Unidos Mexicanos (CPEUM), como se transcribe a continuación:

Toda persona tiene derecho a la protección de sus datos personales, al acceso, rectificación y cancelación de los mismos, así como a manifestar su oposición, en los términos que fije la ley, la cual establecerá los supuestos de excepción a los principios que rijan el tratamiento de datos, por razones de seguridad nacional, disposiciones de orden público, seguridad y salud públicas o para proteger los derechos de terceros.[18]

Bajo ese contexto el Estado debe garantizar dicha protección, ante la responsabilidad de todos aquellos sujetos obligados pertenecientes al orden federal, descritos por la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados en su artículo 1, párrafo quinto, de la siguiente forma, "Son sujetos obligados por esta Ley, en el ámbito federal, estatal y municipal, cualquier autoridad, entidad, órgano y organismo de los Poderes Ejecutivo, Legislativo y Judicial, órganos autónomos, partidos políticos, fideicomisos y fondos públicos"[19], así como la responsabilidad de los particulares descritos en el artículo 2 de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (en adelante LFPDPPP), *"sean personas física o morales de carácter privado que lleven a cabo el tratamiento de datos personales"*[20], exceptuando las mencionadas en el artículo 2, numerales I y II[21], *"I. Las sociedades de información crediticia en los supuestos de la Ley para Regular las Sociedades de Información Crediticia y demás disposiciones aplicables, y II. Las personas que lleven a cabo la recolección y*

[18]Artículo 16, segundo párrafo, Constitución Política de los Estados Unidos Mexicanos, http://www.diputados.gob.mx/LeyesBiblio/pdf/1_110321.pdf, de 07 de junio de 2021, 09:45 p.m.
[19] Artículo 1º, párrafo quinto, LGPDPPSO, op. cit.
[20]Artículo 2, Ley Federal de Protección de Datos Personales en Posesión de los Particulares, *http://www.diputados.gob.mx/LeyesBiblio/pdf/LGPDPPSO.pdf*, de 7 de junio de 2021, 10:26 p.m.
[21] Artículo 2, fracciones I y II, LFPDPPP, ídem.

almacenamiento de datos personales, que sea para uso exclusivamente personal, y sin fines de divulgación o utilización comercial".

Ambas leyes buscan la protección de los datos personales, ya que durante el tratamiento de estos, los mismos pueden ser vulnerados causando diferentes tipos de daños a sus titulares, en ese sentido el artículo 73, fracción XXIX-O de la CPEUM[22], establece facultades al Congreso para legislar en materia de protección de datos personales en posesión de particulares, permitiendo la expedición de las leyes en comentó.

Otras leyes que complementan la protección de los datos en la CDMX y nuestro país a nivel federal son:

- Ley Federal de Transparencia y Acceso a la Información Pública (LFTAIP)[23].
- Ley Federal del Derecho de Autor (Capítulo IV, De los Programas de Computación y las Bases de Datos)[24].
- Ley de Protección de Datos Personales en Posesión de Sujetos Obligados de la CDMX[25] .
- Constitución Política de la Ciudad de México (Artículo 7, fracción E. Derecho a la privacidad y a la protección de los datos personales)[26].

Por su parte la página del Instituto de Transparencia, Acceso a la Información Pública, Protección de Datos Personales y Rendición de Cuentas de la Ciudad de México[27], nos señala que "*adicionalmente a la Ley en la materia, el procedimiento de acceso a la información pública así como los*

[22] Artículo 73, fracción XXIX-O, CPEUM, op. cit.
[23]Ley Federal de Transparencia y Acceso a la Información Pública, *https://www.diputados.gob.mx/LeyesBiblio/pdf/LFTAIP_200521.pdf*, de 7 de junio de 2021, 11:05 p.m.
[24] Capítulo IV, De los Programas de Computación y las Bases de Datos, Ley Federal del Derecho de Autor, *https://www.diputados.gob.mx/LeyesBiblio/pdf/122_010720.pdf*, 7 de junio de 2021, 11:20 p.m.
[25]Ley de Protección de Datos Personales en Posesión de Sujetos Obligados de la Ciudad de México, *https://www.congresocdmx.gob.mx/media/documentos/cd915f7948067a106b79515413589b47568196cc.pdf*, de 7 de junio de 2021, 11:45 p.m.
[26] Artículo 7, fracción E, CPEUM, op. cit.
[27]Instituto de Transparencia, Acceso a la Información Pública, Protección de Datos Personales y Rendición de Cuentas de la Ciudad de México, "Otros documentos normativos", *http://www.infodf.org.mx/index.php/otrosnormativos-pdp.html*, de 7 de junio de 2021, 12:36 p.m.

procedimientos de denuncia, recurso de revisión, revocación y reconsideración, se sujetarán a lo previsto en":

NORMA	DOCUMENTO
Ley	Ley de Transparencia, Acceso a la Información Pública y Rendición de Cuentas de la Ciudad de México (LTAIPRC). Ley General de Transparencia y Acceso a la Información Pública (LGTAIP).
Reglamentos	Reglamento de la LTAIPDF (documento Word) Reglamento del INFODF en Materia de Transparencia y Acceso a la Información Pública (documento Word). Reglamento Interior del INFODF (documento Word).
Lineamientos	Lineamientos para la gestión de solicitudes de información pública y de datos personales a través del sistema INFOMEX del Distrito Federal (documento Word). Lineamientos que regirán la operación del Centro de Atención Telefónica del Instituto de Acceso a la Información Pública del Distrito Federal (documento Word).
Reglas de procedimiento	Procedimiento para la atención de las denuncias de un posible incumplimiento a las obligaciones de oficio establecidas en la LTAIPDF (documento Word). Procedimiento para la Recepción, Substanciación, Resolución y Seguimiento de los Recursos de Revisión interpuestos ante el INFODF (documento Word).
Criterios	Criterios y metodología de evaluación de la información pública de oficio que deben dar a conocer los Entes Obligados en sus portales de Internet (PDF). Criterios y metodología de evaluación de la información pública de oficio que deben dar a conocer los Partidos Políticos en sus portales de Internet (PDF).
Criterio que deberán de aplicar los Entes Obligados, respecto a la clasificación de información en la modalidad Confidencial (documento Word).	

El cuadro anterior fue realizado con información obtenida de la página del Instituto de Transparencia, Acceso a la Información Pública, Protección de Datos Personales y Rendición de Cuentas de la Ciudad de México. Consultado el 13/06/2021 de http://www.infodf.org.mx/index.php/otros-documentos-normativos.html

V. Justificación

La justificación de la protección de los datos que son tratados por Empresas privadas y Órganos del Estado, parte del daño real, actual e inminente que se causa ante la obtención, uso y tratamiento ilegal de los mismos.

Entender la protección de los datos personales como salvaguarda de la intimidad, privacidad y autodeterminación informativa, consecuencia de la procuración de la dignidad y personalidad humana, es prioritario en el desarrollo de la cultura de su protección, comprendiendo que no solamente son los datos

de las personas físicas, sino que de igual forma, como refiere la tesis aislada P. II/2014 (10a.) de nombre "*Personas morales tienen derecho a la protección de los datos que puedan equipararse a los personales, aun cuando dicha información haya sido entregada a una autoridad*", las personas morales tiene ciertos derechos de protección de datos e información:

> *El derecho a la protección de datos personales podría entenderse, en primera instancia, como una prerrogativa de las personas físicas, ante la imposibilidad de afirmar que las morales son titulares del derecho a la intimidad y/o a la vida privada; sin embargo, el contenido de este derecho puede extenderse a cierta información de las personas jurídicas colectivas, en tanto que también cuentan con determinados espacios de protección ante cualquier intromisión arbitraria por parte de terceros respecto de cierta información económica, comercial o relativa a su identidad que, de revelarse, pudiera anular o menoscabar su libre y buen desarrollo*[28]*...*

Por lo que se debe tomar en cuenta el derecho de cómo, cuándo y hasta cuándo se darán a conocer los datos personales de las personas físicas y morales. Eduardo Martínez Altamirano citado por Estrada, J., define el derecho a la intimidad de la siguiente manera:

> *El derecho a la privacidad o a la intimidad es, en lato sensu, aquel derecho humano por virtud del cual la persona, llámese física o moral, tiene la facultad o el poder de excluir o negar a las demás personas, del conocimiento de su vida personal, además de determinar en qué medida o grado esas dimensiones de la vida personal pueden ser legítimamente comunicados a otros… El mismo se divide en: derecho a la inviolabilidad del domicilio, derecho a la inviolabilidad de la correspondencia, derecho a la intimidad frente a las escuchas telefónicas, derecho a la propia imagen, y el derecho a la intimidad frente a la informática o derecho a la libertad informática…*[29]

Uno de los conceptos base de la protección de datos es el tratamiento que debe darse como responsables cuando se poseen y manipulan los mismos, es el señalado en la LGPDPPSO en su artículo 3, fracción XXXIII, que nos dice:

> *Tratamiento: Cualquier operación o conjunto de operaciones efectuadas mediante procedimientos manuales o automatizados aplicados a los datos personales, relacionadas con la obtención, uso, registro, organización, conservación, elaboración, utilización, comunicación, difusión,*

[28] Tesis P. II/2014, Semanario Judicial de la Federación y su Gaceta, Décima Época, t. I, 14 de febrero de 2014, p. 274, *https://sjf.scjn.gob.mx/SJFSem/Paginas/Reportes/ReporteDE.aspx?idius=2005522&Tipo=1*, de 08 de junio de 2021, 06:15 p.m.

[29] Estrada, Jorge, "El derecho a la intimidad y su necesaria inclusión como garantía individual", p. 3, *http://www.ordenjuridico.gob.mx/Congreso/pdf/86.pdf*, de 14 de junio de 2021, 08:17 p.m.

almacenamiento, posesión, acceso, manejo, aprovechamiento, divulgación, transferencia o disposición de datos personales[30]

De igual forma, deben ser aplicadas dentro del tratamiento de datos, medidas de seguridad necesarias para protegerlos, las cuales son descritas en la LGPDPPSO, artículo 3, fracción XX, como, "conjunto de acciones, actividades, controles o mecanismos administrativos, técnicos y físicos que permitan proteger los datos personales"[31], diferenciando el nivel de protección de los datos dependiendo del tipo de que se trate, en el artículo 62 de los Lineamientos Generales sobre Protección de Datos Personales en Posesión de Sujetos Obligados de la Ciudad de México[32], se categorizan los datos personales, de forma enunciativa más no limitativa, de la siguiente forma: I. Identificación, II. Electrónicos, III. Laborales, IV. Patrimoniales, V. Datos sobre procedimientos administrativos y/o jurisdiccionales, VI. Datos académicos, VII. Datos de tránsito y movimientos migratorios, VIII. Datos sobre la salud, IX. Datos biométricos, X. Datos especialmente protegidos (sensibles), y XI. Datos personales de naturaleza pública.

Por su parte, conforme a los cursos impartidos por el INFO, existen los tipos y categorías de datos siguientes: - Identificativos. Nombre, edad, domicilio, estudios, etc.; - Financieros. Bienes, cuentas bancarias, información fiscal, reporte de buro de crédito, declaraciones de impuestos; - Datos electrónicos. La dirección IP, los correos electrónicos e incluso la geolocalización, y Sensibles. Origen racial, estado de salud, creencias religiosas, opiniones políticas, preferencia sexual y datos biométricos.

De lo anterior se desprenden los grados y medidas de protección de protección de los datos, siendo clasificados conforme al artículo 25 de la LDPPSOCDMX, además de establecer los tipos y niveles de seguridad que deben aplicarse en

[30] Artículo 3º fracción XXXIII, LGPDPPSO, op.cit.
[31] Artículo 3º fracción XX, LGPDPPSO, op.cit.
[32]Artículo 62, Lineamientos Generales sobre Protección de Datos Personales en Posesión de Sujetos Obligados de la Ciudad de México, *https://www.infocdmx.org.mx/images/PDF/2021/Lineamientos-Generales-sobre-Datos-Personales-en-Posesin-de-Sujetos-Obligados-de-la-CDMX.pdf*, 14 de junio de 2021, 10:23 p.m.

el tratamiento de datos personales contenidos en los sistemas, de la siguiente manera, "*estas medidas tendrán al menos los siguientes niveles de seguridad*":

> *I. Básico: relativas a las medidas generales de seguridad cuya aplicación será obligatoria para el tratamiento y protección de todos los sistemas de datos personales en posesión de los sujetos obligados.*
>
> *II. Medio: se refiere a las medidas de seguridad requeridas para aquellos sistemas de datos relativos a la comisión de infracciones administrativas o penales, hacienda pública, servicios financieros, datos patrimoniales, así como los sistemas que contengan datos con los que se permita obtener evaluación de personalidad o perfiles de cualquier tipo en el presente pasado o futuro.*
>
> *III. Alto: corresponde a las medidas de seguridad aplicables a sistemas de datos concernientes a ideología, religión, creencias, afiliación política, origen racial o étnico, salud, biométricos, genéticos o vida sexual, así como los que contengan datos recabados para fines policiales, de seguridad, prevención, investigación y persecución de delitos*[33]*.*

Es fundamental que el aviso de privacidad[34], constituido de forma física, electrónica o cualquier otro formato, deba ser generado por empresas privadas u órganos del Estado, siendo puesto a disposición de forma clara ante el titular de los datos personales, antes de que los mismos sean tratados, ello conforme a las leyes aplicables en la materia, ya que de esta forma el propietario sabrá que su información personal será recabada y utilizada para ciertos fines, dando o negando su consentimiento, derecho fundamental a la protección de datos personales[35], pues el artículo 6 de LFPDPPP, nos menciona que "*los responsables en el tratamiento de datos personales, deberán observar los principios de licitud, consentimiento, información, calidad, finalidad, lealtad, proporcionalidad y responsabilidad, previstos en la Ley*", de esta manera el aviso de privacidad, conforme al artículo 16 de la LFPDPPP, deberá contener, al menos, la siguiente información:

> *I. La identidad y domicilio del responsable que los recaba;*

[33] Artículo 25, LDPPSOCDMX, op. cit.
[34] Cfr. Artículo 3, fracción I, LFPDPPP, "Aviso de Privacidad: Documento físico, electrónico o en cualquier otro formato generado por el responsable que es puesto a disposición del titular, previo al tratamiento de sus datos personales, de conformidad con el artículo 15 de la presente Ley", op.cit.
[35] Cfr. Tribunal Constitucional de España, "El concepto del derecho fundamental a la protección de datos personales se entiende como el poder de disposición que faculta a su titular a decidir cuáles de sus datos proporciona a un tercero, así como saber quién posee esos datos y para qué, pudiendo oponerse a esa posesión o uso". Sentencia 292/2000, de 30 de noviembre, *http://hj.tribunalconstitucional.es/es-ES/Resolucion/Show/4276,* 15 de junio de 2021, 07:18 p.m.

II. Las finalidades del tratamiento de datos;

III. Las opciones y medios que el responsable ofrezca a los titulares para limitar el uso o divulgación de los datos;

IV. Los medios para ejercer los derechos de acceso, rectificación, cancelación u oposición, de conformidad con lo dispuesto en esta Ley;

V. En su caso, las transferencias de datos que se efectúen, y

VI. El procedimiento y medio por el cual el responsable comunicará a los titulares de cambios el aviso de privacidad, de conformidad con lo previsto en esta Ley.[36]

Por lo anterior los derechos ARCO (acceso, rectificación, cancelación u oposición sobre el tratamiento de sus datos), serán garantizados, por mandato de ley, en relación a la protección de los datos que son tratados por empresas privadas y órganos del estado, así como sujetos obligados.

Capítulo Segundo

Protocolos normativos de las empresas

I. Protocolos de seguridad dentro del tratamiento, almacenamiento y uso de datos

Para poder entender el significado y uso de los protocolos de seguridad informática, y por ende los de tratamiento, almacenamiento y uso de datos, debemos acudir a la raíz etimológica de la palabra protocolo, la cual se encuentra en el vocablo latino *protocollum,* el cual a su vez deriva del griego "*protokollon*", siendo formado por *"protos"*, significado de "primero", y *"kollea"* sinónimo de "pegamento o cola", refiriendo el Diccionario Jurídico Mexicano del Instituto de Investigaciones Jurídicas de la UNAM[37], *"la primera hoja encolada o pegada*", destacando de igual manera lo siguiente, "*serie ordenada de escrituras matrices y otros documentos que un notario autoriza y custodia con ciertas formalidades*".

[36] Artículo 16, fracción XXXIII, LGPDPPSO, op.cit.
[37] Soberanes,José Luis, concepto, en (coord.), "Diccionario Jurídico Mexicano", 4a ed, Porrúa-UNAM, México, 1991, p. 2629.

Sin embargo, en la actualidad un protocolo también es un reglamento, normativa, documento, manual de procedimientos, o en su caso instrucciones formadas mediante un convenio[38]. En ese sentido un protocolo permite armonizar dentro de la responsabilidad, derivada de la recopilación de conductas, acciones y técnicas necesarias para enfrentar la problemática a solucionar u objetivo, así como la correcta actuación ante la misma, y en estricto sentido prevenir y enfrentar una emergencia, como estrategias a seguir para ejecutar diferentes medidas de protección.

Refiriéndonos a datos, nos encontramos ante la responsabilidad, tanto de las empresas como del Estado, razones sociales, sujetos obligados, organismos e instituciones públicas y privadas, adquirida en el tratamiento, almacenamiento y uso de los datos e información, por lo que garantizar el uso adecuado de los mismos permitiría una correcta autorización del titular de estos, impactando directamente en la corresponsabilidad de todos aquellos individuos que manipularan la información, en ese tenor nos podemos potencialmente regir ante una imprescindible variedad de protocolos, los cuales deben ser formados, construidos, realizados, y alimentados por la normativa nacional e internacional, como consecuencia directa de los acuerdos e intereses de las partes involucradas, ya sean razones sociales, personas físicas, empleados, empleadores, contratistas, contratantes, almacenadores, en fin, todos aquellos prestadores de servicios y responsables de los datos e información concernientes en el negocio, ya que al hablar de información, nos encontramos ante la disyuntiva de sistemas informáticos, *hardwares* y *softwares*, y todas aquellas herramientas esenciales en la actualidad para el manejos de esta, como consecuencia de la protección de interés de clientes, usuarios o licenciatarios.

[38] Cfr., Artículo 1792, Código Civil Federal, “Convenio es el acuerdo de dos o más personas para crear, transferir, modificar o extinguir obligaciones”, Artículo 1793, CCF, “Los convenios que producen o transfieren las obligaciones y derechos, toman el nombre de contratos”, *https://www.diputados.gob.mx/LeyesBiblio/pdf/2_110121.pdf*, de 14 de febrero de 2022, 07:07 p.m.

Al hablar de personas físicas y morales, así como de la protección de su identidad, infraestructura, economía, datos de identificación, etc., somos testigos e integrantes de una fuerte estructura de redes interconectadas, que por su esencia, por sus características, como la potencialidad de desarrollo económico, infraestructura, concepto y varias más que conforman a dichas personas, desprendiéndose del contexto actual, cientos de bases de datos e información, deberán ser aseguradas, pues nos encontramos en la era de la información[39].

Los protocolos de seguridad informática, como herramienta de acceso, clasificación, protección, almacenamiento y resguardo, en relación al concepto de tratamiento de datos personales y en base al artículo 3, fracción XXXIII, de la LGPDPPSO[40], que nos dice, tratamiento: es "cualquier operación o conjunto de operaciones efectuadas mediante procedimientos manuales o automatizados aplicados a los datos personales, relacionadas con la obtención, uso, registro, organización, conservación, elaboración, utilización, comunicación, difusión, almacenamiento, posesión, acceso, manejo, aprovechamiento, divulgación, transferencia o disposición de datos personales", dependiendo del tratamiento de los datos personales que se quiera o busque dar, serán varios los tipos de protocolos que nos permitirán lograr nuestros objetivos.

Algunos nos ayudarán a proteger las redes de información, por medio de las cuales funcionan y se interconectan múltiples aplicaciones y plataformas, así como sistemas, que manipulan, controlan, acceden, intercambian información a la distancia alimentándose los unos de los otros, almacenan, comparten, etc., diferentes tipos de datos, como en el caso del IMSS con sistemas y aplicaciones

[39] Cfr., Espinosa, Alejandra, "La Era de la Información. La "era de la información", también llamada era digital o era informática, designa al periodo en el que el movimiento de información se volvió más rápido que el movimiento físico, gracias a la creación y desarrollo de las tecnologías digitales de la información y la comunicación (TICs)", ATI, Tecnología Integrada, 2021, *https://tecnologiaintegrada.com.mx/2016/10/24/la-era-la-informacion/*, de 07 de febrero de 2022, 03:42 p.m.
[40] Artículo 3º, fracción XXXIII, LGPDPPSO, op. cit.

de afiliación, vigencia, cobranza, jurídico, cardiología, salud en el trabajo, etc., conformantes de la red sistémica de dicho Instituto.

El entorno informático y de telecomunicación, converge con la necesidad de sistematizar normas adecuadas, reguladoras del intercambio de información y comunicación entre dos o más sistemas, lo que conlleva a la formación de protocolos de lenguajes o códigos de comunicación entre diversos sistemas informáticos, los cuales permitirán un correcto intercambio y flujo de información que a su vez deberán ser protegidos, y en el tema que nos ocupa, de seguridad dentro del tratamiento, almacenamiento y uso de datos. Dichos protocolos, como refiere Helmut, en la página de *Lifeder*[41], deben poseer las siguientes características:

- Basado en reglas. Reglas y preceptos informáticos específicos.
- Estándares. Se especifica un estándar para la comunicación, brindando información detallada sobre los procedimientos involucrados en la transmisión de datos. Dicha información incluye: Naturaleza del proceso, tipo de tarea, gestión de dispositivos, tipo de datos, velocidad del flujo de datos.
- Transferencia de datos. "*El flujo continuo de bytes*[42] *o mensajes que se van a transferir son envueltos por el protocolo en paquetes, llamados también segmentos, para ser transmitidos al dispositivo de destino. Para ello se usan en los mensajes técnicas de conmutación de paquetes, que son mensajes partidos en pedazos empaquetados, que se vuelven a ensamblar en su destino*".
- Confiabilidad. Se debe poder recobrar de una transmisión de datos corrompidos en la red.

Los protocolos informáticos tiene como objetivo lograr una correcta interoperabilidad (relación entre uso, almacenaje, analizar y comprender los

[41]Lifeder, "Protocolo en informática: características, tipos, ejemplos", 2021, https://www.lifeder.com/protocolo-informatica/, de 17 de junio de 2021, 09:32 p.m.
[42]Cfr., Diccionario informático, "Byte: Es la unidad básica de información. En la práctica, se puede considerar que un byte es la cantidad de espacio necesaria para almacenar una letra. Tiene múltiplos como el Kilobyte, Megabyte, Gigabyte y Terabyte. Internamente, corresponde a 8 bits", Diccionario informático.

datos), regular el control de flujo (administrar la velocidad de transmisión de los datos entre dos dispositivos), administrar congestiones (disminución de la calidad de servicio de red), administrar la verificación de errores (métodos para entregar de forma correcta los datos), establecer estrategias de seguridad o cifrado, etc. Por otro lado Helmut, de la página de Lifeder, nos refiere los siguientes tipos de protocolos informáticos[43]: 1. Administradores de redes. "*Involucrados con los variados dispositivos que componen una red, como microcomputadoras, servidores y enrutadores, para garantizar que la red como un todo funcione óptimamente*", con funciones de incorporación de enlaces[44], conexión[45] y solución de problemas[46]; 2. Comunicación. "*Su uso es tanto en las comunicaciones digitales como analógicas, para metodologías que van desde la transferencia de archivos entre dispositivos hasta el acceso a Internet*" (mensajería instantánea, *bluetooth*), y; 3. Seguridad. "*Trabajan para garantizar que la red y los datos enviados por ella estén protegidos de usuarios no autorizados*", mediante transporte (proteger los datos mientras están siendo transportados por la red desde un dispositivo hasta otro) y cifrado (proteger los datos y también mantener las áreas seguras, al exigir a los usuarios que ingresen una contraseña secreta para acceder a esa información). De igual manera refiere los siguientes tipos de protocolos:

I. *Protocolo de transferencia de archivos (FTP). Permite copiar archivos entre un sistema local y cualquier otro sistema que se pueda acceder en la red.*
II. *Protocolo de control de transmisión (TCP). Protocolo desarrollado para que en Internet se reciban los datos de un dispositivo de red a otro. TCP utiliza una estrategia de retransmisión para asegurar que los datos no se pierdan en la transmisión.*
III. *Protocolo de internet (IP). Permite el envío de datos entre dispositivos a través de Internet. Internet no podría funcionar como lo hace actualmente sin el IP.*
IV. *Protocolo de control de transmisión/internet (TCP/IP). Es un conjunto de protocolos, incluyendo TCP, desarrollado para Internet en los años 70 para obtener datos de un dispositivo de red a otro.*

[43] Lifeder, op.cit.
[44] Cfr., Lifeder, Permitir combinar múltiples conexiones de red en un solo enlace, para así aumentar la fuerza de la conexión", op. cit.
[45] Cfr., Lifeder, "Constituir conexiones y cuidar que las mismas sean estables entre los diferentes dispositivos de la red", op. cit.
[46] Cfr., Lifeder, "Identificar errores que afecten a la red, evaluar la calidad de conexión y además determinar cómo se puede solucionar cualquier problema", op.cit.

V. *Protocolo de transferencia de hipertexto (HTTP). Es un protocolo que utiliza TCP para transferir solicitudes de hipertexto e información entre servidores y navegadores de Internet.*

VI. *Telnet. Es el protocolo utilizado para el servicio de conexión de terminal remoto, permitiendo a un usuario que se encuentre en un sitio interactuar con sistemas en otros sitios diferentes, como si ese terminal estuviera directamente conectado a esas computadoras.*

VII. *Protocolo de voz por internet (VoIP). Permite hacer llamadas telefónicas comunes a través de una red informática o Internet, permitiendo así a las personas hablar con prácticamente cualquier otra persona que tenga un teléfono.*

VIII. *"POP (Post Office Protocol). Específico para servicios de correo electrónico, permite recuperar los mensajes almacenados en un servidor remoto (Servidor POP), especialmente en conexiones intermitentes o muy lentas"*[47]*.*

Por otro lado en la página de "Concepto", nos menciona, como los protocolos de red son diseñados para la comunicación dentro de las redes, y cómo se transmite la información fragmentándose para poder ser transportada.

> *Los protocolos de red están especialmente diseñados para la comunicación a través de redes de computadoras, que operan fragmentando la información enviada en pequeñas partes, en lugar de todo de golpe. Las partes son fáciles y rápidas de transmitir, pero deben almacenarse en su orden indicado para conservar el sentido y operar en conjunto.*[48]

Por otro lado encontramos en la página de "imágenes y especialistas"[49] una serie de tópicos que nos permiten desarrollar un protocolo para el tratamiento de datos de forma adecuada, siendo los siguientes: I. Definiciones, II. Objeto; III. Ámbito de aplicación, IV. Destinatarios de la presente norma; V. Principios aplicables al tratamiento de datos personales; VI. Derechos de los titulares de los datos; VII. Deberes de los destinatarios de esta norma respecto de las bases de datos de carácter personal cuando ostenten la calidad de responsables y encargados; VIII. Procedimiento de *habeas data* para el ejercicio de los derechos de información, acceso, actualización, rectificación, cancelación y oposición; IX. Registro central de bases de datos personales; X. Tratamiento

[48] Etecé, "Protocolo Informático", Concepto, *https://concepto.de/protocolo-informatico/*, de 25 de junio de 2021, 08:45 p.m.

[49] Imágenes y especialistas, "Protocolo para Tratamiento de Datos", *https://imagenesyespecialistas.com/protocolo-para-tratamiento-de-datos/,* de 27 de junio de 2021, 10:23 p.m.

de datos personales; XI. Prohibiciones; Transferencia internacional de datos; XIII. Roles y responsabilidades en el cumplimiento de la protección de datos personales; XIV. Temporalidad del dato personal; XV. Medidas de seguridad; XVI. Procedimiento y sanciones; XVII. Entrega de datos personales a autoridades; XVIII. Restricciones en el uso de esta norma, y; XIX. Vigencia.

Dándonos de igual forma el significado de lo que es el tratamiento de datos como, "*cualquier operación o conjunto de operaciones y procedimientos técnicos de carácter automatizado o no que se realizan sobre datos personales, tales como la recolección, grabación, almacenamiento, conservación, uso circulación, modificación, bloqueo, cancelación, entre otros*[50]."

Resaltamos la importancia de la seguridad, esencial en cualquier tipo de protocolo de tratamiento, almacenamiento y uso de datos, pues como señala la Estrategia Nacional de Ciberseguridad, en su concepto de seguridad de la información, esta es "la capacidad de preservar la confidencialidad, integridad y disponibilidad de la información, así como su autenticidad[51], auditabilidad[52], protección a la duplicación[53], no repudio[54] y legalidad"[55].

En concordancia con los principios rectores manifiestos en dicha Estrategia Nacional de Ciberseguridad, fundados en la perspectiva de derechos humanos (como promoción, respeto y cumplimiento de los mismos), un enfoque basado en la gestión de riesgos (capacidad de manejar escenarios de incertidumbre por medio de enfoques preventivos y correctivos, como respuesta a las cambiantes amenazas y riesgos del ciberespacio), así como colaboración

[50]Imágenes y especialistas, op.cit.
[51] Cfr., Imágenes y especialistas, "Busca asegurar la validez de la información en tiempo, forma y distribución. Asimismo, garantiza el origen de la información, validando el emisor para evitar la suplantación de identidades", op.cit.
[52] Cfr., Imágenes y especialistas, "Define que todos los eventos de un sistema deben poder ser registrados para su control posterior", op.cit.
[53] Cfr., Imágenes y especialistas, "Consiste en asegurar que una transacción sólo se realiza una vez, a menos que se especifique lo contrario, así como en impedir que se grabe una transacción para su posterior reproducción, con el objeto de simular múltiples peticiones del remitente original", op.cit.
[54] Cfr., Imágenes y especialistas, Se refiere a evitar que una entidad, órgano o persona que haya enviado o recibido información alegue ante terceros que no la envió o recibió", op.cit.
[55] Cfr., Imágenes y especialistas, "Referido al cumplimiento del marco jurídico al que está sujeta la institución de que se trate", op.cit.

multidisciplinaria y de múltiples actores (colaboración entre actores y sectores, con enfoque de gobernanza de internet en materia de Ciberseguridad).

De la misma forma se hace mención de su convergencia y complemento, en la "Declaración de Principios", contenidos en el documento "WSIS-03/GENEVA/4-S", del 12 de mayo del 2004, resultado de la Cumbre Mundial Sobre la Sociedad de la Información, Ginebra 2003-Túnez 2005[56], en su inciso B5, numerales 35., y 36. "*el fomento a un clima de confianza que se extiende a la seguridad de la información, seguridad de las redes, autenticación, privacidad y protección de los consumidores, es requisito para que se desarrollé la sociedad*" (35), *"impedir que se utilicen estas tecnologías con fines incompatibles con el mantenimiento de la estabilidad y seguridad internacionales, evitando que las tecnologías y los recursos de la información se utilicen para fines criminales o terroristas, respetando siempre los derechos humanos*" (36).

Cabe mencionar la importancia de unificar y homologar los protocolos de seguridad que las empresas del Estado, razones sociales, sujetos obligados, organismos e instituciones públicas y privadas, utilicen dentro del tratamiento, almacenamiento y uso de datos, como personas físicas y morales responsables, entendiéndose de igual forma como responsables a los proveedores de servicios[57], todos aquellos que se comprometen ante un contrato como responsables, encargados y usuarios, desarrolladores y diseñadores de programas, de softwares y su encriptación, aplicaciones, etc., logrando con ello medidas de seguridad administrativas, técnicas y físicas necesarias en el contexto actual y futuro, de los datos y la información, sin olvidar a quienes son partícipes del comercio digital y todas sus variantes. La

[56]Declaración de Principios, Documento "WSIS-03/GENEVA/4-S", 12 de mayo del 2004, Cumbre Mundial Sobre la Sociedad de la Información, Ginebra 2003-Túnez 2005, *https://www.itu.int/net/wsis/docs/geneva/official/dop-es.html*, de 27 de junio de 2021, 07:32 p.m.

[57]Cfr., Artículo 1, fracción b, Convenio de Budapest, "Proveedor de servicios: i. toda entidad pública o privada que ofrezca a los usuarios de sus servicios la posibilidad de comunicar a través de un sistema informático, y ii. Cualquier otra entidad que procese o almacene datos informáticos para dicho servicio de comunicación o para los usuarios del mismo", *http://documentostics.com/documentos/convenio_cibercriminalidad.pdf,* de 28 de junio de 2021, 06:43 p.m.

Ley de Protección de la Persona Frente al Tratamiento de Sus Datos, Ley n.º 8968, de Costa Rica, en su artículo 12 nos dice:

> *Protocolos de actuación. Las personas físicas y jurídicas, públicas y privadas, que tengan entre sus funciones la recolección, el almacenamiento y el uso de datos personales, podrán emitir un protocolo de actuación en el cual establecerán los pasos que deberán seguir en la recolección, el almacenamiento y el manejo de los datos personales, de conformidad con las reglas previstas en esta ley.*
>
> *Para que sean válidos, los protocolos de actuación deberán ser inscritos, así como sus posteriores modificaciones, ante la Prodhab. La Prodhab podrá verificar, en cualquier momento, que la base de datos esté cumpliendo cabalmente con los términos de su protocolo.*
>
> *La manipulación de datos con base en un protocolo de actuación inscrito ante la Prodhab hará presumir, "iuris tantum", [58]el cumplimiento de las disposiciones contenidas en esta ley, para los efectos de autorizar la cesión de los datos contenidos en una base[59].*

Por otro lado en nuestro país, se encuentra regulado lo que se conoce como el "documento de seguridad", en el cual se encuentran las medidas de seguridad que son implementadas por quienes son responsables del tratamiento de datos, los cuales con el fin de protegerlos contra daño, pérdida, alteración, destrucción o su uso, acceso o tratamiento no autorizado, deberán adoptar el documento de seguridad más adecuado para su empresa (protocolo de seguridad). La Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, en relación al documento de seguridad como figura jurídica, en su artículo 3, fracción XIV, señala lo siguiente:

> *Artículo 3. Para los efectos de la presente Ley se entenderá por:*
>
> *XIV: Documento de seguridad: Instrumento que describe y da cuenta de manera general sobre las medidas de seguridad técnicas, físicas y administrativas adoptadas por el responsable[60] para garantizar la confidencialidad, integridad y disponibilidad de los datos personales que Posee[61].*

[58] Cfr., iuris tantum Can. "Presunción solo de derecho que ordena admitir como probado en juicio un hecho, mientras no se tenga prueba de lo contrario". *Iuris tantum*, Diccionario panhispánico del español jurídico, *https://dpej.rae.es/lema/iuris-tantum,* de 18 de julio de 2021, 07:32 p.m.

[59]Ley de Protección de la Persona Frente al Tratamiento de sus Datos Personales, *https://www.oas.org/es/sla/ddi/docs/CR4%20Ley%20de%20Protecci%C3%B3n%20de%20la%20Persona%20frente%20al%20Tratamiento%20de%20sus%20Datos%20Personales.pdf*, de 28 de junio de 2021, 09:48 p.m.

[60] Cfr., Artículo 3, Fracción XXIV, LGPDPPSO, "Responsable: Persona física o moral de carácter privado que decide sobre el tratamiento de datos personales", op.cit.

[61] Artículo 3º, fracción XIV, LGPDPPSO, op.cit.

La necesidad de documentar los instrumentos de seguridad empleados por quienes son responsables del tratamiento y manejo de los datos, deberá permitir la puesta al día y actualización de la documentación en materia de seguridad partiendo desde tres aspectos, como refiere Del Peso, Emilio, lo siguiente:

> *Técnico. Mejora en la seguridad con la implantación de mecanismos de detección o de identificación puede variar por los protocolos de acceso a edificios o a lugares con acceso restringido.*
>
> *Organizativo. Cambios en el organigrama, desaparición de departamentos o funciones o la introducción de otras nuevas e incluso el traslado de determinadas tareas o responsabilidades a un tercero a través del outsourcing o cualquier otro sistema actualmente en el mercado basado en esta filosofía, pueden suponer alteraciones en procedimientos que supongan actualizaciones de la documentación.*
>
> *Jurídico. La proliferación de normas legales que afectan a aspectos que cada día inciden de forma más directa en la actividad habitual de toda organización, ya sea sobre Propiedad Intelectual, Firma electrónica, Comercio electrónico o la propia Ley de Protección de datos, lleva a la necesidad de una mejor formación y concienciación de nuestro personal en relación con las labores que desempeña*[62]

Por su parte la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, en su artículo 19, párrafo primero señala:

> *Todo responsable que lleve a cabo tratamiento de datos personales deberá establecer y mantener medidas de seguridad administrativas, técnicas y físicas que permitan proteger los datos personales contra daño, pérdida, alteración, destrucción o el uso, acceso o tratamiento no autorizado*[63]*.*

De esta forma las medidas de seguridad administrativas, técnicas y físicas, tienen como objetivo primordial la protección de los datos personales, estas medidas son descritas en el Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, lo que con base en su artículo 2, fracciones V, VI y VII, se muestra a continuación:

> *V. Medidas de seguridad administrativas: "Conjunto de acciones y mecanismos para establecer la gestión, soporte y revisión de la seguridad de la información*

[62] Del Peso, Emilio, "El documento de Seguridad", IEE. Informáticos Europeos Expertos, Ediciones Díaz de Santos, S. A. Madrid España. 2004. Libro electrónico, GOOGLE, Libros, p.p. 40 y 41, https://books.google.com.mx/books?id=4I2Cdi_8wgcC&printsec=frontcover&dq=documentos+de+seguridad+EMILIO+DEL+PESO+NAVARRO&hl=es&sa=X&redir_esc=y#v=onepage&q=documentos%20de%20seguridad%20EMILIO%20DEL%20PESO%20NAVARRO&f=false, de 05 de octubre de 2021, 09:34 p.m.

[63] Artículo 19, párrafo primero y artículo 2, fracciones V, VI, VII, LFPDPPP, op. cit.

a nivel organizacional, la identificación y clasificación de la información, así como la concienciación, formación y capacitación del personal, en materia de protección de datos personales;

VI. Medidas de seguridad físicas: Conjunto de acciones y mecanismos, ya sea que empleen o no la tecnología, destinados para: a) Prevenir el acceso no autorizado, el daño o interferencia a las instalaciones físicas, áreas críticas de la organización, equipo e información; b) Proteger los equipos móviles, portátiles o de fácil remoción, situados dentro o fuera de las instalaciones; c) Proveer a los equipos que contienen o almacenan datos personales de un mantenimiento que asegure su disponibilidad, funcionalidad e integridad, y d) Garantizar la eliminación de datos de forma segura;

VII. Medidas de seguridad técnicas: Conjunto de actividades, controles o mecanismos con resultado medible, que se valen de la tecnología para asegurar que: a) El acceso a las bases de datos lógicas o a la información en formato lógico sea por usuarios identificados y autorizados; b) El acceso referido en el inciso anterior sea únicamente para que el usuario lleve a cabo las actividades que requiere con motivo de sus funciones; c) Se incluyan acciones para la adquisición¸ operación, desarrollo y mantenimiento de sistemas seguros, y d) Se lleve a cabo la gestión de comunicaciones y operaciones de los recursos informáticos que se utilicen en el tratamiento de datos personales[64]

Para la elaboración del documento de seguridad, conforme a la ley, el mismo debe contener y tomar en cuenta ciertos puntos esenciales, que con base en el artículo 28 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados de la Ciudad de México, se enuncian a continuación:

Artículo 28. El responsable deberá elaborar el documento de seguridad que contendrá, al menos, lo siguiente: I. El inventario de datos personales en los sistemas de datos; II. Las funciones y obligaciones de las personas que intervengan en el tratamiento datos personales, usuarios y encargados, en el caso de que los hubiera; III. Registro de incidencias; IV. Identificación y autentificación; V. Control de acceso; gestión de soportes y copias de respaldo y recuperación; VI. El análisis de riesgos; VII. El análisis de brecha; VIII. Responsable de seguridad; IX. Registro de acceso y telecomunicaciones; X. Los mecanismos de monitoreo y revisión de las medidas de seguridad; XI. El plan de trabajo; y XII. El programa general de capacitación[65]

Analizar y prevenir el nivel de riesgo en el que se encuentra la empresa o sistema, es fundamental en la actualidad, pues de ello depende saber si existe algún tipo de problemática que pudiese afectar el funcionamiento de los sistemas, de esta forma tomando en cuenta el impacto del dato o información que llegase a ser vulnerado, atacado, modificado, consultado sin permiso o

[64] Artículo 2, fracciones V, VI y VII, Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares,*http://www.diputados.gob.mx/LeyesBiblio/pdf/LGPDPPSO.pdf*, de 07 de octubre de 2021, 08:38 p.m.
[65] Artículo 28, LDPPSOCDMX, op. cit.

robado, así las bases de datos, los sistemas, equipos, servidores, etc., deben ser asegurados, por lo que en análisis de la brecha de seguridad en el que se encuentra la empresa, permitirá comprender, detectar y subsanar las deficiencias de seguridad.

La capacidad de respuesta humana, técnica y sistemática, ante un evento que intente burlar los sistemas de seguridad informática de la empresa, permitirá accionar o responder de manera adecuada, sabiendo de antemano las vulnerabilidades que han sido detectadas, por lo que la brecha de seguridad [66]al ser analizada por medio de Pruebas de Penetración *(pen testing)* permitirá saber cuáles son las vulnerabilidades que deberán ser reforzadas para minimizar el impacto de respuesta en la empresa, ello conforme a la seguridad que será aplicada en la protección de datos e información.

La prueba de penetración, es una herramienta que actualmente nos permite saber y evaluar la seguridad de los sistemas informáticos, redes y aplicaciones, como refiere Ramos, J., citado por Jaramillo, Cristina, y Leonidas, Pablo, en relación al concepto de *Pent Test*, "El termino *Pent Test* es como comúnmente se denomina a los "Test de penetración" o en inglés *Penetration Tests*, y es un procedimiento que se realiza atreves de un conjunto de técnicas y métodos que simulan el ataque a un sistema esto nos sirve para evaluar la seguridad de los sistemas informáticos, redes y aplicaciones"[67], los sistemas en la actualidad, aunque se tengan los mejores, deben ser constantemente revisados y actualizados, ya que los delincuentes informáticos cada vez adquieren técnicas y métodos de ataques, así como formas de penetración más sofisticadas.

[66] Cfr., Kaspersky "¿Qué es una brecha de seguridad?. Una brecha de seguridad es un incidente que permite el acceso no autorizado a datos informáticos, aplicaciones, redes o dispositivos", *https://www.kaspersky.es/resource-center/threats/what-is-a-security-breach*, de 11 de octubre de 2021, 07:49 p.m.

[67]Jaramillo, Cristina y Leonidas, Pablo, "Metodología para realizar la evaluación, detección de riesgos, vulnerabilidades y contramedidas en el diseño e implementación de la infraestructura de la red de la editorial don Bosco, mediante un test de intrusión de caja blanca", Universidad Politécnica Salesiana, Ecuador, 2015, *https://docplayer.es/1764719-Universidad-politecnica-salesiana-sede-cuenca.html*, de 07 de febrero de 2022, 04:11 p.m.

De esta forma son realizados ataques controlados por parte de técnicos o ingenieros en informática, contratados por la empresa para que por medio de técnicas y herramientas utilizadas por los delincuentes informáticos (como los *crackers*), sea evaluada con ello la efectividad de las defensas de seguridad de la empresa, partiendo desde las perspectiva de un atacante externo y de un empleado con malas intenciones dentro de la organización, al terminar el ataque simulado debe ser entregado un informe o crónica del ataque, en el cual se debe explicar cómo se logró penetrar, presentando las evidencias de que se logró el acceso, un plan para remediar las vulnerabilidades, sin olvidar toda la información técnica, etc,. Un ejemplo de los resultados que deberán entregarse a la empresa u organización, lo encontramos en la página de la empresa Kolibers, servicios de pruebas de penetración en México, en donde nos refieren que deben ser entregados los siguientes reportes:

> *Reporte Ejecutivo: "Cómo se puede intuir en el nombre, el reporte ejecutivo se entrega a los ejecutivos de la organización y se explica en lenguaje no técnico los riesgos identificados y la mejor forma de solucionarlos, de esta forma la alta dirección podrá tomar decisiones informadas y aplicar sus presupuestos basados en riesgos".*
>
> *Reporte Técnico: "El reporte técnico se entrega al área de sistemas de la organización, donde se explica a detalle cada vulnerabilidad identificada, cómo se identificó y cuál es la mejor manera de solucionarlas. Con esta información la parte técnica podrá resolver los riesgos en base al feedback de nuestros ingenieros, la alta dirección y sus objetivos y experiencia propia para que la organización saque el máximo provecho de las pruebas"*[68]

II. Justificación de la responsabilidad de la empresa al prestar sus servicios

El tratamiento de datos personales e información, tanto de personas físicas como morales, ya sean pertenecientes al estado o a la industria privada, conlleva importantes compromisos de ética y seguridad, elementales en la protección de la información, así como los derechos humanos que protegen a los mismos, sin olvidar lo referido por Olivia Mendoza, "*la reputación en la industria y consolidación de modelos de negocio, a través de la confianza de*

[68] Kolibers, "Servicios de Pruebas de Penetración en México", *https://www.kolibers.com/pruebas-de-penetracion.html,* de 11 de octubre de 2021, 09:28 p.m.

clientes y usuarios de los servicios prestados"[69], en ese sentido la protección de datos e información parte de la responsabilidad de guardar su confidencialidad, al estar a su cargo o resguardo, así como solicitar el consentimiento[70] de los titulares, impactando fuertemente en la obtención, uso, registro, organización, conservación, elaboración, utilización, comunicación, difusión, almacenamiento, posesión, acceso, manejo, aprovechamiento, divulgación, transferencia o disposición, en congruencia con la Declaración Universal de Derechos Humanos de 10 de diciembre de 1948, artículos 3, 12 y 17, así como la Convención Americana de Derechos Humanos, artículo 11, como se muestra a continuación:

Declaración Universal de Derechos Humanos

Artículo 3. Todo individuo tiene derecho a la vida, a la libertad y a la seguridad de su persona.
Artículo 12. Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques.
Artículo 17.
1. Toda persona tiene derecho a la propiedad, individual y colectivamente.
2. Nadie será privado arbitrariamente de su propiedad[71]

Convención Americana de Derechos Humanos Pacto de San José de Costa Rica

Artículo 11
Protección de la Honra y de la Dignidad
1. Toda persona tiene derecho al respeto de su honra y al reconocimiento de su dignidad.
2. 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.
3. Toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques[72]

[69] Mendoza, Olivia, "Marco jurídico de la protección de datos personales en las empresas de servicios establecidas en México: desafíos y cumplimiento", Revista IUS, 2018, *http://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S1870-21472018000100267*, de 11 de octubre de 2021, 06:17 p.m.
[70] Cfr., Artículo 3, fracción IV, LFDDPPP, "Consentimiento: Manifestación de la voluntad del titular de los datos mediante la cual se efectúa el tratamiento de los mismos", op.cit.
[71] Artículos 3, 12, 17, Declaración Universal de Derechos Humanos, *https://www.ohchr.org/en/udhr/documents/udhr_translations/spn.pdf*, de 11 de octubre de 2021.
[72] Artículo 11, Convención Americana sobre Derechos Humanos, *https://www.cndh.org.mx/sites/all/doc/Programas/TrataPersonas/MarcoNormativoTrata/InsInternacionales/Regionales/Convencion_ADH.pdf*, de 11 de octubre de 2021, 06:43 p.m.

La protección de los datos personales de clientes y usuarios de empresas de servicios, privadas y del Estado, es fundamental en las relaciones económicas actuales, así como la economía digital, ya que el precio de la información se ha ido elevando conforme a la utilización y objetivo de la misma, ejemplo de ello es la ingeniería social[73] y las redes sociales, como se deduce de lo señalado por Olivia Mendoza.

> *"…el valor económico otorgado a la información de las personas no radica en el dato por sí mismo, sino en el tratamiento, asociación con otros datos y utilidad que se le dé. Esto permite obtener un lucro, a través de la explotación comercial de aspectos privados, orientados al consumo, que incluso se interesan en predecir conductas y patrones de comportamiento…*[74]

Partiendo de lo anterior, las empresas prestadoras de servicios, en el ámbito de datos e información, tienen la responsabilidad de mantener estándares altos de seguridad, adquirida por contrato, aviso de privacidad[75] o ley, normativa en materia de datos e información, lo cual es fundamental en el tratamiento[76]de datos personales, información financiera, industrial, documentos oficiales, seguridad pública y nacional, etc., por lo que la incorporación de buenas prácticas[77], cláusulas de confidencialidad y códigos de ética, permitirán lograr su objetivo dentro del tratamiento, la seguridad de todo tipo de datos e información. Esta debe tener ciertos principios básicos en su tratamiento y

[73]Cfr., Sandoval, E, "Ingeniería Social: corrompiendo la mente humana. La Ingeniería Social es el acto de manipular a una persona a través de técnicas psicológicas y habilidades sociales para cumplir metas específicas. Éstas contemplan entre otras cosas: la obtención de información, el acceso a un sistema o la ejecución de una actividad más elaborada (como el robo de un activo), pudiendo ser o no del interés de la persona objetivo", Revista.Seguridad, 2018, núm. 10, México UNAM, *https://revista.seguridad.unam.mx/numero-10/ingenier%C3%AD-social-corrompiendo-la-mente-humana,* de 11 de octubre de 2021, 08:32 p.m.

[74] Mendoza, Olivia, op.cit.

[75]Cfr., Artículo 3, fracción I, LFPDPPP, "Aviso de Privacidad: Documento físico, electrónico o en cualquier otro formato generado por el responsable que es puesto a disposición del titular, previo al tratamiento de sus datos personales, de conformidad con el artículo 15 de la presente Ley", op. cit.

[76]Cfr., Artículo 3, fracción XVIII, LFPDPPP, "Tratamiento: 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", op.cit.

[77]Cfr., Cámara, Sergio, "Concepto y definición de mejores prácticas. El término "buenas prácticas" nos remite a la recta aplicación de reglas o instrucciones predeterminadas como adecuadas en un determinado campo y para una determinada actividad. Desde esta acepción, las prácticas se consideran "buenas" por su aplicación recta y sistemática", Vlex, *https://international.vlex.com/vid/concepto-definicion-mejores-practicas-407301574*, de 08 de julio de 2021, 10:25 p.m.

manejo, como se muestra en el artículo 6 de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares:

> *Artículo 6.- Los responsables en el tratamiento de datos personales, deberán observar los principios de licitud, consentimiento, información, calidad, finalidad, lealtad, proporcionalidad y responsabilidad, previstos en la Ley*[78]*.*

En el entendido de que los datos e información, deberán recabarse de forma lícita, refiriendo la finalidad de la utilización de los mismos, siendo de suma importancia que los titulares y/o dueños de la información den su consentimiento expreso o tácito, no siendo obtenidos de forma engañosa o por medios fraudulentos, siendo estos pertinentes, correctos y actualizados conforme a los fines para los cuales fueron recabados, recogiendo sólo aquellos que resulten adecuados, relevantes y necesarios, así como la responsabilidad que deberán asumir el responsable, el encargado y los terceros en el uso y tratamiento de datos e información[79], sin olvidar su transferencia.

Conforme a la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados el responsable se encuentra obligado a implementar los mecanismos que considere convenientes para acreditar el cumplimiento de los principios, deberes y obligaciones establecidos en la Ley General[80], así como rendir cuentas sobre el tratamiento de datos personales en su posesión al titular y al Instituto o a los organismos garantes, según corresponda.

La LGPDPPSO en su artículo 30 establece los siguientes mecanismos para cumplir con el principio de responsabilidad*:*

> *I. Destinar recursos autorizados para la instrumentación de programas y políticas de protección de datos personales.*
> *II. Elaborar políticas y programas de protección de datos personales, obligatorios y exigibles al interior de la organización del responsable.*

[78] Artículo 6, LFPDPPP, op.cit.

[79] Artículo 3, fracciones IX, XIV, XVI, XIX, LFPDPPP, "Encargado: La persona física o jurídica que sola o conjuntamente con otras trate datos"; "Responsable: Persona física o moral de carácter privado que decide sobre el tratamiento de datos personales"; "Tercero: La persona física o moral, nacional o extranjera, distinta del titular o del responsable de los datos", "Transferencia: Toda comunicación de datos realizada a persona distinta del responsable o encargado del tratamiento", op.cit.

[80] Artículo 29, LGPDPPSO, op.cit.

III. *Poner en práctica un programa de capacitación y actualización del personal sobre las obligaciones y deberes en materia de protección de datos personales.*
IV. *Revisar periódicamente las políticas y programas de seguridad de datos personales para determinar las modificaciones que se requieran.*
V. *Establecer un sistema de supervisión y vigilancia interna y/o externa, incluyendo auditorías, para comprobar el cumplimiento de las políticas de protección de datos personales.*
VI. *Establecer procedimientos para recibir y responder dudas y quejas de los titulares.*
VII. *Diseñar, desarrollar e implementar sus políticas públicas, programas, servicios, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología que implique el tratamiento de datos personales, y*
VIII. *Garantizar que sus políticas públicas, programas, servicios, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología que implique el tratamiento de datos personales, cumplan por defecto con las obligaciones previstas en la Ley General y las demás que resulten aplicables en la materia*[81]*.*

Es importante hacer mención de la información de las personas morales, pues en congruencia con la tesis aislada P. II/2014, mencionada con anterioridad, de nombre "*Personas morales tienen derecho a la protección de los datos que puedan equipararse a los personales, aun cuando dicha información haya sido entregada a una autoridad*", el derecho a la intimidad y a la vida privada, se puede extender a cierta información, pues cuentan con determinados espacios de protección ante cualquier intromisión arbitraria por parte de terceros, en relación a información económica y comercial así como de su propia identidad, que pudiesen atentar contra el libre y buen desarrollo de esta, como se muestra en el siguiente extracto:

"*…el derecho a la protección de datos personales podría entenderse, en primera instancia, como una prerrogativa de las personas físicas, ante la imposibilidad de afirmar que las morales son titulares del derecho a la intimidad y/o a la vida privada; sin embargo, el contenido de este derecho puede extenderse a cierta información de las personas jurídicas colectivas, en tanto que también cuentan con determinados espacios de protección ante cualquier intromisión arbitraria por parte de terceros respecto de cierta información económica, comercial o relativa a su identidad que, de revelarse, pudiera anular o menoscabar su libre y buen desarrollo", por lo que se debe tomar en cuenta*

[81] Artículo 30, LGPDPPSO, op.cit.

el derecho de cómo, cuándo y hasta cuándo se darán a conocer los datos personales de las personas físicas y morales…[82]

Lo que nos lleva a la protección de las personas morales, pues las mismas tienen derecho a la salvaguarda de sus datos e información confidencial, como refiere la tesis en mención, lo que con base al artículo 110 de la Ley Federal de Transparencia y Acceso a la Información Pública, fracciones I, IV, y VI[83], se considera como información reservada, que puede llegar a impactar a las personas morales su publicación, en la seguridad Nacional y pública, que puedan poner en riesgo operaciones monetarias y financieras, así como la estabilidad de las instituciones financieras y obstrucción a las actividades de recaudación de los contribuyentes la siguiente:

De la Información Reservada

Conforme a lo dispuesto por el artículo 113 de la Ley General, como información reservada podrá clasificarse aquella cuya publicación:

I. Comprometa la seguridad nacional, la seguridad pública o la defensa nacional y cuente con un propósito genuino y un efecto demostrable;

IV. Pueda afectar la efectividad de las medidas adoptadas en relación con las políticas en materia monetaria, cambiaria o del sistema financiero del país; pueda poner en riesgo la estabilidad de las instituciones financieras susceptibles de ser consideradas de riesgo sistémico o del sistema financiero del país, pueda comprometer la seguridad en la provisión de moneda nacional al país, o pueda incrementar el costo de operaciones financieras que realicen los sujetos obligados del sector público federal;

VI. Obstruya las actividades de verificación, inspección y auditoría relativas al cumplimiento de las leyes o afecte la recaudación de contribuciones;

En ese sentido tanto la seguridad nacional y pública, como el sistema financiero y de recaudación, se ven comprometidos en sus bases de datos e información por los delincuentes informáticos, siendo que su protección es de prioridad para la vida económica del país, y así el correcto desarrollo de las personas físicas y morales, lo anterior en concordancia con la Ley General de Transparencia y Acceso a la Información Pública, en su artículo 116[84], que nos dice:

[82] Tesis P. II/2014, op.cit.
[83] Artículo 110, fracciones I, IV, VI, LFTAIP, op.cit.
[84]Artículo 116, LFTAIP, op.cit.

Se considera información confidencial la que contiene datos personales concernientes a una persona identificada o identificable"[85]*.*

La información confidencial no estará sujeta a temporalidad alguna y sólo podrán tener acceso a ella los titulares de la misma, sus representantes y los Servidores Públicos facultados para ello.

Se considera como información confidencial: los secretos bancario, fiduciario, industrial, comercial, fiscal, bursátil y postal, cuya titularidad corresponda a particulares, sujetos de derecho internacional o a sujetos obligados cuando no involucren el ejercicio de recursos públicos.

Asimismo, será información confidencial aquella que presenten los particulares a los sujetos obligados, siempre que tengan el derecho a ello, de conformidad con lo dispuesto por las leyes o los tratados internacionales.

Destacando de esta forma, no sólo los secretos bancario, fiduciario, industrial, comercial, fiscal, bursátil y postal, cuya titularidad corresponda a particulares, sujetos de derecho internacional o a sujetos obligados cuando no involucren el ejercicio de recursos públicos, sino también la información que contiene datos personales concernientes a una persona identificada o identificable. Las personas morales son poseedoras de datos como nombre, domicilio, datos económicos, comerciales, etc., que deben ser protegidos contra intromisiones ilegales, además de poseer bienes jurídicos que tutelan los derechos a la privacidad y protección de datos personales, como documentos e información de la empresa o Razón Social, que se considera no debe ser publicable, esto es, que no deben conocer terceros.

De lo antes mencionado, las empresas, por medio del responsable que lleve a cabo el tratamiento de datos personales, deben aplicar medidas de seguridad, administrativas, técnicas y físicas, tendientes a la protección de los datos, como una obligación esencial en su tratamiento, en términos del artículo 19 de la LFPDPPP[86]:

Todo responsable que lleve a cabo tratamiento de datos personales deberá establecer y mantener medidas de seguridad administrativas, técnicas y físicas

[85]Cfr., Pérez, Julio, "¿Qué es una persona identificada o identificable?". "Persona identificada: toda persona cuya identidad está determinada. Persona identificable: toda persona cuya identidad pueda determinarse, ya sea directamente o indirectamente, mediante cualquier información referida a su identidad física, fisiológica, psíquica, económica, cultural o social". Balaguer y Gutiérrez, Boletín, 04/14, 2014, *https://www.balaguergutierrez.com/media/newsletters/boletin%20LOPD/BOLETIN%20LOPD%20ABRIL%202014.pdf,* de 08 de julio de 2021, 06:45 p.m.
[86] Artículo 19, LFPDPPP, op.cit.

que permitan proteger los datos personales contra daño, pérdida, alteración, destrucción o el uso, acceso o tratamiento no autorizado.

Los responsables no adoptarán medidas de seguridad menores a aquellas que mantengan para el manejo de su información. Asimismo se tomará en cuenta el riesgo existente, las posibles consecuencias para los titulares, la sensibilidad de los datos y el desarrollo tecnológico.

Entendiéndose como medidas de seguridad administrativas, físicas y técnicas, las siguientes:

Medidas de seguridad administrativas. Políticas y procedimientos para la gestión, soporte y revisión de la seguridad de la información a nivel organizacional, mediante la identificación, clasificación y borrado seguro de la información; así como la sensibilización y capacitación del personal, en materia de protección de datos personales (consultado del Curso Impartido por el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, tomado el 8 de julio de 2021).

Medidas de seguridad físicas. Conjunto de acciones y mecanismos para proteger el entorno físico de los datos personales y de los recursos involucrados en su tratamiento. De manera enunciativa más no limitativa, se deben considerar las siguientes actividades:

• Prevenir el acceso no autorizado al perímetro de la organización, sus instalaciones físicas, áreas críticas, recursos e información.

• Prevenir el daño o interferencia a las instalaciones físicas, áreas críticas de la organización, recursos e información.

• Proteger los recursos móviles, portátiles y cualquier soporte físico o electrónico que pueda salir de la organización.

• Proveer a los equipos que contienen o almacenan datos personales de un mantenimiento eficaz, que asegure su disponibilidad e integridad (consultado del Curso Impartido por el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, tomado el 8 de julio de 2021).

Medidas de seguridad técnicas. Conjunto de acciones y mecanismos que se valen de la tecnología relacionada con hardware y software para proteger el entorno digital de los datos personales y los recursos involucrados en su

tratamiento. De manera enunciativa más no limitativa, se deben considerar las siguientes actividades:

> *• Prevenir que el acceso a las bases de datos o a la información, así como a los recursos, sea por usuarios identificados y autorizados.*
>
> *• Generar un esquema de privilegios para que el usuario lleve a cabo las actividades que requiere con motivo de sus funciones.*
>
> *• Revisar la configuración de seguridad en la adquisición, operación, desarrollo y mantenimiento del software y hardware.*
>
> *• Gestionar las comunicaciones, operaciones y medios de almacenamiento de los recursos informáticos en el tratamiento de datos personales (consultado del Curso Impartido por el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, tomado el 8 de julio de 2021).*

III. Términos y condiciones de uso (permisos perpetuos e irrevocables)

En la actualidad es importante que los términos y condiciones sean plasmados por quienes son proveedores de servicios, ya sea en la adquisición de un producto o la prestación de algún servicio, por lo que dichos términos y condiciones, serán lo que denomina la Ley Federal de Protección al Consumidor (LFPC) en su artículo 85, como contrato de adhesión:

> *Para los efectos de esta ley, se entiende por contrato de adhesión el documento elaborado unilateralmente por el proveedor, para establecer en formatos uniformes los términos y condiciones aplicables a la adquisición de un producto o la prestación de un servicio, aun cuando dicho documento no contenga todas las cláusulas ordinarias de un contrato. Todo contrato de adhesión celebrado en territorio nacional, para su validez, deberá estar escrito en idioma español y sus caracteres tendrán que ser legibles a simple vista y en un tamaño y tipo de letra uniforme. Además, no podrá implicar prestaciones desproporcionadas a cargo de los consumidores, obligaciones inequitativas o abusivas, o cualquier otra cláusula o texto que viole las disposiciones de esta ley*[87]

Dicho tipo de contratos son revisados y registrados de manera obligatoria, con el objetivo de evitar prácticas abusivas entre proveedores y consumidores, ante la Procuraduría Federal del Consumidor (en adelante PROFECO), sin embargo

[87] Artículo 85, Ley Federal de Protección al Consumidor, http://www.diputados.gob.mx/LeyesBiblio/ref/lfpc.htm, de 28 de noviembre de 2021, 09:09 p.m.

estos contratos, en cuestión de datos e información, no deben ser contrarios a las leyes de protección de datos personales e información, en el entendido de que buscan proteger principalmente los intereses del prestador de servicios, pues la mayoría de sus cláusulas son referidas a tal objetivo, las cláusulas abusivas deben ser eliminadas por la PROFECO, en nuestro país, derivado de las obligaciones del gobierno, la Procuraduría debe luchar por la erradicación de malas prácticas que atentan contra los consumidores, principalmente cláusulas abusivas en los servicios bancarios, telefónicos, de prestaciones de servicios de internet, redes sociales, aplicaciones, plataformas, etc., pues un principio básico en las relaciones de consumo, en términos del artículo primero fracción VII, de la Ley Federal de Protección al Consumidor, es el siguiente:

> *VII. La protección contra la publicidad engañosa y abusiva, métodos comerciales coercitivos y desleales, así como contra prácticas y cláusulas abusivas o impuestas en el abastecimiento de productos y servicios*[88]

De lo anterior tenemos que los términos y condiciones son importantes en la relación de consumidores y prestadores de servicios, ya que de los mismos se puede tomar conciencia de si se contrata el servicio o no, ahora bien la mayoría de las veces, en los casos de servicios de internet, plataformas, aplicaciones, sitios web, uso de app[89], etc., quienes las utilizan y/o descargan no revisan las políticas establecidas en los términos y condiciones, lo que lleva a prácticas abusivas, pues los datos e información en la actualidad son activos que pueden ser manipulados y sobre todo, comercializados y explotados, de esta forma los permisos perpetuos e irrevocables atentan contra los datos e información, ya que son transmitidos, vendidos y usados por terceros (como uso de credenciales, nombre de usuario y contraseña), quienes a su vez pueden negociarlos con otros prestadores de servicios, empresas, o quien tenga interés de poseer esos datos.

[88] Artículo 1º, fracción VII, LFPC, op.cit.
[89] Cfr., Sistemas, "Definición de aplicación. Una aplicación (también llamada app) es simplemente un programa informático creado para llevar a cabo o facilitar una tarea en un dispositivo informático". Sistemas, "Definición de aplicación. Una aplicación (también llamada app) es simplemente un programa informático creado para llevar a cabo o facilitar una tarea en un dispositivo informático". *https://sistemas.com/aplicacion.php,* de 17 de julio de 2021, 7:22 p.m.

Dentro de estos términos encontramos el permiso que se otorga a las empresas de acceder a la información contenida en dispositivos electrónicos como celulares, lo que atenta contra la privacidad de los usuarios, en el entendido de que por la dinámica de vida actual y por ende la urgencia del servicio, no revisan de manera adecuada este término, aceptando de forma inconsciente las cláusulas ahí plasmadas, pues también se presiona al consumidor al redactar frases como, "*si no está aceptando estas condiciones, incluyendo el uso y modificación del contenido en la posterioridad, no acceda ni use los servicios*" siendo necesaria una política de privacidad, manual de *habeas data* (que tengas los datos o información) o manual de datos personales, etc., en el cual se describa la responsabilidad de quienes son prestadores de servicios, la forma en cómo vas a recopilar la información, almacenar y qué tratamiento se le va a dar a la misma, como norman las Diferentes Leyes, reglamentos, circulares, manuales, protocolos, etc., reguladores de captación, almacenamiento, uso y tratamiento de los datos e información.

En los términos y condiciones se debe informar el tipo de servicio que se está ofreciendo, lo que realiza el producto (como el *software*), calidad del producto y/o servicio, condiciones específicas, como el no uso del mismo cuando se atente contra las Leyes y normas bajo las cuales fue desarrollado, aspectos de la ley que se aplican al producto o servicio que se ofrece, siendo esencial las leyes aplicables en el lugar donde será adquirido y prestado (las leyes del país), políticas de propiedad industrial e intelectual, conforme a los artículo 2 fracción I[90] de la Ley Federal de Protección a la Propiedad Industrial, y artículo 11[91] de la Ley Federal del Derecho de Autor, seguridad y protección de datos de los usuarios, siendo importante la regulación de los datos de geolocalización, la

[90]Cfr., Artículo 2, fracción I, Ley Federal de Protección a la Propiedad Industrial, **"**Esta Ley tiene por objeto: I.- Proteger la propiedad industrial mediante la regulación y otorgamiento de patentes de invención; registros de modelos de utilidad, diseños industriales, esquemas de trazado de circuitos integrados, marcas y avisos comerciales; publicación de nombres comerciales; declaración de protección de denominaciones de origen e indicaciones geográficas", *http://www.diputados.gob.mx/LeyesBiblio/pdf/LFPPI_010720.pdf*, de 14 de octubre de 2021, 07:33 p.m.

[91] Cfr., Artículo 11, LFDA, "El derecho de autor es el reconocimiento que hace el Estado en favor de todo creador de obras literarias y artísticas previstas en el artículo 13 de esta Ley, en virtud del cual otorga su protección para que el autor goce de prerrogativas y privilegios exclusivos de carácter personal y patrimonial. Los primeros integran el llamado derecho moral y los segundos, el patrimonial", op.cit.

protección al usuario es fundamental en la prestación de productos y servicios, por lo que el artículo 78 Bis, en sus fracciones de la I a la VII, de la Ley Federal de Protección al Consumidor, destaca las relaciones entre proveedores y consumidores, así transacciones efectuadas a través del uso de medios electrónicos, ópticos o de cualquier otra tecnología, *cumpliendo con lo siguiente:*

> *I. El proveedor utilizará la información proporcionada por el consumidor en forma confidencial, por lo que no podrá difundirla o transmitirla a otros proveedores ajenos a la transacción, salvo autorización expresa del propio consumidor o por requerimiento de autoridad competente;*
>
> *II. El proveedor utilizará alguno de los elementos técnicos disponibles para brindar seguridad y confidencialidad a la información proporcionada por el consumidor e informará a éste, previamente a la celebración de la transacción, de las características generales de dichos elementos;*
>
> *III. El proveedor deberá proporcionar al consumidor, antes de celebrar la transacción, su domicilio físico, números telefónicos y demás medios a los que pueda acudir el propio consumidor para presentarle sus reclamaciones o solicitarle aclaraciones;*
>
> *IV. El proveedor evitará las prácticas comerciales engañosas respecto de las características de los productos, por lo que deberá cumplir con las disposiciones relativas a la información y publicidad de los bienes y servicios que ofrezca, señaladas en esta Ley y demás disposiciones que se deriven de ella;*
>
> *V. El consumidor tendrá derecho a conocer toda la información sobre los términos, condiciones, costos, cargos adicionales, en su caso, formas de pago de los bienes y servicios ofrecidos por el proveedor;*
>
> *VI. El proveedor respetará la decisión del consumidor en cuanto a la cantidad y calidad de los productos que desea recibir, así como la de no recibir avisos comerciales, y*
>
> *VII. El proveedor deberá abstenerse de utilizar estrategias de venta o publicitarias que no proporcionen al consumidor información clara y suficiente sobre los servicios ofrecidos, en especial tratándose de prácticas de mercadotecnia dirigidas a la población vulnerable, como los niños, ancianos y enfermos, incorporando mecanismos que adviertan cuando la información no sea apta para esa población*[92]

Las políticas de intercambio de información, permitirán saber cuáles son las condiciones bajo las que se accede a la información, cuál es la protección aplicada al intercambio, fidelidad de la información, responsabilidades de contenido en la información, penalidades, restricciones, políticas de enlaces de

[92] Artículo 78 Bis, LFPC, op.cit.

terceros, así como tratamiento, uso y administración de la información por estos, etc., sin olvidar el texto de autorización del uso de datos.

Siendo necesarios los términos bajo los cuales se puede rescindir el contrato, ya sea por falla del proveedor de servicios o por actividades negativas y contrarias por parte del usuario, sin olvidar las leyes e instituciones a las cuales se acudirá en caso de presentarse algún tipo de problemática, con miras a la solución del problema, así los términos y condiciones permiten no solo saber cuál es el producto o prestación de servicio que se ofrece, sino que de igual forma buscan certeza jurídica para las partes, proteger al proveedor o prestador del servicio, así como evitar abusos y limitar responsabilidades.

Por su parte la Ley Federal de Protección al Consumidor en términos de sus artículos 86 y 90[93], respecto a los contratos de adhesión, señala que la Profeco será competente para resolver las controversias que se suscite sobre la interpretación o cumplimiento de los mismos y en qué casos no serán válidas ni se tendrán por puestas las cláusulas que los conforman, como se muestra a continuación:

> *Artículo 86.- La Secretaría, mediante normas oficiales mexicanas podrá sujetar contratos de adhesión a registro previo ante la Procuraduría cuando impliquen o puedan implicar prestaciones desproporcionadas a cargo de los consumidores, obligaciones inequitativas o abusivas, o altas probabilidades de incumplimiento.*
>
> *Las normas podrán referirse a cualesquiera términos y condiciones, excepto precio.*
>
> *Los contratos de adhesión sujetos a registro deberán contener una cláusula en la que se determine que la Procuraduría será competente en la vía administrativa para resolver cualquier controversia que se suscite sobre la interpretación o cumplimiento de los mismos. Asimismo, deberán señalar el número de registro otorgado por la Procuraduría.*
>
> *ARTÍCULO 90.- No serán válidas y se tendrán por no puestas las siguientes cláusulas de los contratos de adhesión ni se inscribirán en el registro cuando:*
>
> *I. Permitan al proveedor modificar unilateralmente el contenido del contrato, o sustraerse unilateralmente de sus obligaciones;*

[93] Artículo 86, 90, LFPC, op.cit.

II. Liberen al proveedor de su responsabilidad civil, excepto cuando el consumidor incumpla el contrato;

III. Trasladen al consumidor o a un tercero que no sea parte del contrato la responsabilidad civil del proveedor;

IV. Prevengan términos de prescripción inferiores a los legales;

V. Prescriban el cumplimiento de ciertas formalidades para la procedencia de las acciones que se promuevan contra el proveedor; y

VI. Obliguen al consumidor a renunciar a la protección de esta ley o lo sometan a la competencia de tribunales extranjeros.

IV. Validación de documentos

En la actualidad la validación de documentos y firma electrónica es un tema que se encuentra en boga, ya que la virtualización de todas las transacciones contractuales, comerciales, de flujo de datos e información, etc., es inminente en el contexto actual, lo que da paso a un sin número de plataformas y aplicaciones que realizan la validación de estos, por ejemplo la "firma.judicial", que como refiere el artículo 7, de los "Lineamientos para regular el uso de la firma electrónica certificada del Poder Judicial de la Ciudad de México", contenidos y modificados en la CIRCULAR CJCDMX-45/2020, del Poder Judicial de la Ciudad de México, de fecha 14 de diciembre de 2020.

Los documentos electrónicos o digitales que cuenten con "Firma.Judicial" producirán los mismos efectos y tendrán el mismo trato que los presentados físicamente con firma autógrafa[94]*.*

El artículo 8 del mismo ordenamiento, menciona que la firma judicial es utilizada "para cualquier trámite que se realice ante el Poder Judicial, sea ante los Órganos jurisdiccionales del Tribunal o ante el Consejo, sólo se admitirá y validará la "Firma.Judicial", cuando no se haga uso del documento físico y la firma autógrafa", o como en el caso del sistema de "Validación de copias certificadas del Registro Civil del Distrito Federal del Gobierno de la Ciudad de México", en el que se validan las Actas de Nacimiento, así como el sistema de

[94]Artículos 7-8, Circular CJCDMX-45/2020, *https://www.poderjudicialcdmx.gob.mx/wp-content/uploads/CIRCULAR_CJCDMX-45-2020.pdf*, de 29 de julio de 2021,

la RENAPO, en donde se consulta, emite y valida la Clave Única de Registro de Población (CURP).

De lo anterior se desprende que documentos como actas de nacimiento, de matrimonio de defunción, oficios, demandas, apelaciones arbitrajes, minutas, recursos, actas, solicitudes, reclamaciones, informes, reportes, circulares, cartas, currículum, memorándums, así documentos públicos como el pasaporte, la licencia de manejo, título de propiedad, contrato de trabajo, y documentos privados como constancia de trabajo autorización, hoy en día son validados por medio de plataformas, aplicaciones y sistemas en los que se generen y expidan copias de los mismos documentos.

Es común la utilización de cifrados y encriptación[95] hoy en día, como un método de protección y certeza jurídica en los documentos, pues los "mensajes de datos" conceptualizados en el Código de Comercio en su artículo 89[96] como "la información generada, enviada, recibida o archivada por medios electrónicos, ópticos o cualquier otra tecnología", deben ser protegidos de tal forma que garanticen el contenido de los mismos, siendo utilizados, en términos del artículo 89 bis del mismo ordenamiento, como un "medio probatorio en cualquier diligencia ante la autoridad legalmente reconocida, y surtirán los mismos efectos jurídicos que la documentación impresa".

Diferentes son los cifrados que se utilizan en la creación y protección de estos documentos, ejemplo de ello es la firma electrónica, que contiene datos únicos, como códigos o claves criptográficas, utilizados para identificar al firmante, así los datos de creación de firma electrónica, conforme al artículo 89 del ordenamiento en comentó, son "datos únicos, como códigos o claves criptográficas privadas, que el Firmante genera de manera secreta y utiliza para

[95] Cfr., Norma Oficial Mexicana NOM-151-SCFI-2016, "Requisitos que deben observarse para la conservación de mensajes de datos y digitalización de documentos. 4.3 Criptografía. Al conjunto de técnicas matemáticas para cifrar información", *https://www.dof.gob.mx/normasOficiales/6499/seeco11_C/seeco11_C.html,* de 29 de julio de 2021, 06:46 p.m.

[96] Cfr., Artículo 89, 89 Bis, Código de Comercio, *https://www.diputados.gob.mx/LeyesBiblio/pdf_mov/Codigo_de_Comercio.pdf*, de 29 de julio de 2021, 07:32 p.m.

crear su Firma Electrónica, a fin de lograr el vínculo entre dicha Firma Electrónica y el Firmante".

En la página del Servicio de Administración Tributaria (SAT), denominada "Buzón Tributario"[97], se puede verificar la integridad y autoría de documentos notificados de forma electrónica, teniendo como objetivo, lo que se cita textualmente "te permite la verificación de la integridad y autoría de los documentos firmados con la Firma electrónica del funcionario competente que son notificados de manera electrónica (documentos digitales), lo cual te dará certeza jurídica de que estás recibiendo un documento emitido por el SAT".

V. Plataformas (por medio de *block chain*), que generan certificados PSC, generar programas con políticas y procedimientos revisados y autorizados, con ratificación del comité de ética, del director, presidentes (consentimiento en firma electrónica), encriptar la fecha en que se realizó el acuerdo. Para el trato, almacenamiento y uso de datos

La seguridad de las transacciones electrónicas es de suma importancia en el contexto actual, lo que conlleva a tomar una serie de medidas que logren alcanzar la misma, así diferentes tecnologías de encriptación[98], permiten aumentar los niveles de seguridad en relación a la protección de datos e información, en ese tenor el Prestador de Servicios de Certificación, con base al artículo 89 del Código de Comercio[99], es "la persona o institución pública que preste servicios relacionados con firmas electrónicas, expide los certificados o presta servicios relacionados como la conservación de mensajes de datos, el sellado digital de tiempo y la digitalización de documentos impresos, en los términos que se establezca en la norma oficial mexicana sobre digitalización y conservación de mensajes de datos que para tal efecto emita la Secretaría". De esta forma son entidades autorizadas por la Secretaría de Economía que

[97] SAT, Buzón Tributario, *https://www.sat.gob.mx/personas/iniciar-sesion*, de 29 de julio de 2021, 08:31 p.m.

[98] Cfr., *The free dictionary*, "Encriptar. tr. inform. Ocultar datos mediante una clave", Farlex Inc, 2003-2022, *https://es.thefreedictionary.com/encriptar,* de 29 de julio de 2021, 09:11 p.m.

[99] Artículo 89, CC, op.cit.

expiden certificados electrónicos y presta servicios relacionados con la firma electrónica.

Por su parte la página de "DocuSing"[100], nos señala, para mejor entender, los servicios que los Prestadores de Servicios de Certificación pueden dar, relacionados con el uso de la firma electrónica, siendo los siguientes:

- Emisión de sellos digitales de tiempo[101]. "*También conocidos por su nombre en inglés como timestamp, los cuales garantizan la fecha y hora exactas en que un documento digital fue firmado, así como su existencia y vínculo con una entidad o persona*".

- Constancias de conservación de mensajes de datos. Entendidas como "*recibos digitales que señalan la existencia de un documento, así como de sus firmas, a partir de ciertas fechas", de igual manera nos dice que conforme a la Norma Oficial Mexicana NOM-151-SCFI-2016[102], Requisitos que deben observarse para la conservación de mensajes de datos y digitalización de documentos, "una constancia de conservación de mensajes de datos es una serie de sellos digitales, emitidos por un PSC, que permiten verificar la fecha y hora de firma del documento electrónico*".

- Emisión de Certificados Electrónicos[103]. "*Documentos digitales que un PSC se encarga de garantizar su validez y vinculación de la entidad y su clave pública*".

[100]Cfr., Docusing, "Conoce qué es un prestador de servicios de certificación y su rol con las firmas electrónicas", https://www.docusign.mx/blog/prestador-de-servicios-de-certificacion, de 29 de julio de 2021, 09:31 p.m.
[101]Cfr., Artículo 89, CC, "Sello Digital de Tiempo: El registro que prueba que un dato existía antes de la fecha y hora de emisión del citado Sello, en los términos que se establezca en la norma oficial mexicana sobre digitalización y conservación de mensajes de datos que para tal efecto emita la Secretaría", op.cit.
[102] Norma Oficial Mexicana NOM-151-SCFI-201, op.cit.
[103] Cfr., Artículo 2, fracción V, Ley de Firma Electrónica Avanzada, "Certificado Digital: el mensaje de datos o registro que confirme el vínculo entre un firmante y la clave privada; VI. Clave Privada: los datos que el firmante genera de manera secreta y utiliza para crear su firma electrónica avanzada, a fin de lograr el vínculo entre dicha firma electrónica avanzada y el firmante; VII. Clave Pública: los datos contenidos en un certificado digital que permiten la verificación de la autenticidad de la firma electrónica avanzada del firmante", *http://www.diputados.gob.mx/LeyesBiblio/ref/lfea.htm*, de 29 de julio de 2021, 09:53 p.m.

- Digitalización certificada de documentos. "*Migrando los originales en papel al formato digital y asegurando su valor probatorio*".

En relación a la protección de datos, el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI) mediante acuerdo ACT-PUB-30/09/2020.06[104] aprobado por el Pleno del Instituto se constituyó como autoridad certificadora para poder emitir, administrar y registrar los certificados electrónicos digitales de la firma electrónica denominada FELINAI (firma electrónica del INAI), utilizada para trámites, servicios, actos jurídicos y administrativos con el INAI, así como en las herramientas tecnológicas utilizadas para ello, teniendo como objetivo la subscripción electrónica de documentos a través de los cuales se atienda algún requerimiento del Instituto, así como para la sustanciación de los procedimientos previstos en la LGTAIP, LGPDPPSO, LFTAIP y LFPDPPP.

Por otro lado una de las tecnologías que en la actualidad ha funcionado en relación a la protección y seguridad de datos e información es la denominada "*blockchain*" (cadena de bloques), la cual es definida por Mauricio Pereira, Marcos Toscano y Paula Villar en su trabajo de proyecto de grado denominado "Plataformas *blockchain* y escenarios de uso"[105], como "*libro mayor, implementado como una base de datos distribuida en una red, la cual puede ser pública o privada. En ella, se almacenan de forma permanente (inmutable) un historial de transacciones mediante la utilización de nodos, los cuales pueden contar con diferentes permisos sobre la red*", garantizando la consistencia de los registros almacenados y utilizando diferentes mecanismos de validación y consenso, refiriendo además los mismos autores que "una

[104]Cfr., Diario Oficial, "Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales", Acuerdo ACT-PUB-30/09/2020.06, México, 12/10/2020, P. 187, *http://www.apta.com.mx/apta2008/ce/dof/descargapdf/2020/10Octubre/20201012/intaipd20101210-11.pdf*, de 29 de julio de 2021, 11:03 p.m.

[105]Cfr., Pereira, M., Toscano, M., Villar, P, "Plataformas blockchain y escenarios de uso". Montevideo, Uruguay, 2019, https://www.colibri.udelar.edu.uy/jspui/bitstream/20.500.12008/20541/1/tg-pereira-toscano-villar.pdf, de 03 de agosto de 2021, 06:12 p.m.

plataforma *blockchain* en un conjunto de herramientas que permiten desarrollar aplicaciones distribuidas que utilizan tecnología *blockchain*"[106].

Esta plataforma es muy conocida por el uso que se le ha dado en las criptomonedas, sin embargo en la actualidad dicha tecnología se ha extendido a diferentes usos como señala Lecuit, J[107], siendo aplicada en el sector financiero (transacciones bancarias entre entidades, medios de pago, pólizas de seguros), el logístico (trazabilidad y gestión de las mercancías), el energético (integración de medios de generación a la red eléctrica), el sanitario y farmacéutico (historiales, gestión médica, trazado de medicamentos), la industria audiovisual (gestión de los derechos a través de la cadena de valor de la obra), el turismo (gestión de reservas, contrataciones, tarifas, gestión de la identidad, seguimiento de equipajes), la industria 4.0 (construcción de comunicaciones seguras en las redes industriales mediante el registro actualizado en tiempo real de los dispositivos *IIoT* (Internet Industrial de las Cosas[108]), conexión a internet y elementos de la industria, fiables integrados a la red de operaciones) o la Administración Pública (gestión de licencias, transacciones, eventos, movimiento de recursos y pagos, gestión de propiedades, gestión de identidades).

Esta cadena de bloques, como refiere Lecuit[109], "ofrece una representación o registro dinámico e inalterable de esas transacciones a lo largo del tiempo que sustituye a intermediarios y autoridades centralizadas de confianza (p. ej. Notarios, bancos, aseguradoras, etc.) que respalden las transacciones por la confianza digital que los usuarios han depositado en esta tecnología", "ofrece transparencia (todos los participantes pueden ver la totalidad de la información

[106] Idem.
[107] Lecuit, J, "La seguridad y privacidad del blockchain, más allá de la tecnología y las criptomonedas. Real Instituto Elcano", 2019, *http://www.realinstitutoelcano.org/wps/wcm/connect/574e1e0b-0b4d-4bea-b1a9-e2d46d265402/ARI106-2019-AlonsoLecuit-seguridad-y-privacidad-del-blockchain-mas-alla-de-tecnologia-y-criptomonedas.pdf?MOD=AJPERES&CACHEID=574e1e0b-0b4d-4bea-b1a9-e2d46d265402*, de 03 de agosto de 2021, 06:41 p.m.
[108] Cfr., Iberdrola, "Internet Industrial de las Cosas. Conjunto de sensores, instrumentos y dispositivos autónomos conectados a través de Internet a aplicaciones industriales", *https://www.iberdrola.com/innovacion/que-es-iiot,* de 20 de septiembre de 2021, 06:21 p.m.
[109] Lecuit, J, op.cit.

contenida en la base de datos distribuida), compartición y descentralización (una misma copia de la base de datos en todos los nodos), irreversibilidad (una vez registrado un dato, no puede ser modificado o borrado) y desintermediación (sin árbitro central, los participantes toman decisiones por consenso)", esta misma cadena enlaza la secuencia de transacciones e incorpora una marca de tiempo, dando con ello transparencia y trazabilidad (rastrea todos los procesos) a las operaciones. Cabe mencionar que la cadena de bloques refuerza su seguridad por medio de mecanismos criptográficos para acceder, firmar y cifrar las transacciones, los bloques y su encadenado, nos dice Lecuit[110].

En ese sentido la protección de datos personales en el uso de *blockchain* parte del desarrollo de los ficheros y base de datos distribuidos en la red, lo que conlleva al ejercicio de los derechos ARCO, la legitimación de su tratamiento a lo largo de su ciclo de vida (desde que se obtiene o recaban hasta que son destruidos, borrados o eliminados), de conformidad con la LFPDPPP y su reglamento, basado en los principios de licitud, consentimiento, información, calidad, finalidad, lealtad, proporcionalidad y responsabilidad, así como los deberes de confidencialidad y seguridad, de igual forma se debe vincular, dentro de la cadena de bloques, el aviso de privacidad[111] en el que se deberá informar lo anterior, por medio del responsable de su tratamiento, persona física o moral, quien a su vez lo pondrá a disposición del titular de los datos, de esta forma, refiere Ocampo, M[112], las cadenas de bloque involucran "el manejo de información personal, lo que despierta especial interés en los sistemas jurídicos, pues afecta el derecho humano a la protección de datos".

Por otra parte una *FINTECH* (*finance-technology*), es entendida como una empresa, personas físicas o morales, a través de la cual se prestan servicios

[110] Lecuit, J, op.cit.
[111] Artículo 3, fracción I, LFPDPPP, "Aviso de Privacidad: Documento físico, electrónico o en cualquier otro formato generado por el responsable que es puesto a disposición del titular, previo al tratamiento de sus datos personales, de conformidad con el artículo 15 de la presente Ley", op. cit.
[112] Ocampo, M, "Nuevos desafíos para la protección de datos personales en México. la regulación de la tecnología blockchain", Biblioteca Jurídica Virtual del Instituto de Investigaciones Jurídicas de la UNAM, *https://revistas.juridicas.unam.mx/index.php/derecho-informacion/article/view/13881/15338*, de 04 de agosto de 2021, 08:21 p.m.

del sector financiero, los cuales realizan sus negocios, servicios y transacciones por medio de plataformas electrónicas u/o medios electrónicos, en ese tenor la Ley para Regular las Instituciones de Tecnología Financiera (LRITF), conocida en nuestro país como Ley FINTECH, en su artículo 4 fracción XVII nos dice que define como "Modelo Novedoso".

> *… aquel que para la prestación de servicios financieros utilice herramientas o medios tecnológicos con modalidades distintas a las existentes en el mercado al momento en que se otorgue la autorización temporal en términos de esta Ley…*[113]

Ello permitiría regular la cadena de bloques dentro de los servicios financieros, pues el *Blockchain* es una tecnología distinta a las existentes, reguladas normalmente en el mercado, sin embargo el futuro de la cadena de bloques, debe expandirse a todas aquellas posibilidades de aplicación determinadas en las diferentes áreas del quehacer de nuestro país, por lo que su regulación, tanto en el sector privado como público, dará mayor certeza jurídica a esta tecnología emergente.

Capítulo Tercero

Responsabilidad jurídica de quienes participan de forma conjunta en el robo de datos

I. *Cibergang*, pandillas y delincuencia organizada

La natural socialización de las personas ha permitido desarrollar formas de conducta criminal en grupo, por ende la evolución constante de la terminología relacionada con este fenómeno, puesto que no podemos negar el hecho, de que la existencia de unión entre dos o más individuos para delinquir inició desde hace mucho tiempo atrás, la participación de varias personas en la realización de delitos cometidos de forma grupal en el contexto actual, permitirá entender la funcionalidad de los delitos informáticos cometidos desde las entrañas de

[113] Artículo 4, fracción XVII, Ley para Regular las Instituciones de Tecnología Financiera, *https://www.diputados.gob.mx/LeyesBiblio/pdf/LRITF_200521.pdf*, de 04 de agosto de 2021, 08:43 p.m.

una colonia, pueblo o municipio, hasta diferentes zonas geográficas, y su impacto tanto en la seguridad informática como en la afectación de la población en general; personas físicas, morales, empresas e instituciones gubernamentales y no gubernamentales.

Los grupos quienes originariamente se reunían para socializar y convivir de forma sana, en muchos de los casos, se han modificado para cometer diferentes tipos de delitos, reorientándose a múltiples actividades ilegales, de esta forma surgen grupos como las pandillas, en la cual refiere Vargas, Leticia.

> *…los sujetos no están organizados para cometer delitos, si no que se reúnen de manera habitual, ocasional, transitoriamente, y así reunidos cometen el delito. Es decir, los individuos se unen con frecuencia, por casualidad o temporalmente, pero no se reúnen de manera permanente con el objeto de delinquir. Las penas correspondientes al delito o delitos cometidos se agravan cuando éstos se cometen en pandilla…*[114]

De lo anterior podemos entender que en las normas penales la pandilla es una agravante de cualquier delito, refiere la misma autora, ya que "cuando se cometa algún delito por pandilla, se impondrá una mitad más de las penas que correspondan por el o los delitos cometidos", lo anterior de conformidad con el artículo 252[115] del Código Penal para el Distrito Federal, que nos dice:

> *Cuando se cometa algún delito por pandilla, se impondrá una mitad más de las penas que correspondan por el o los delitos cometidos, a los que intervengan en su comisión.*
>
> *Se entiende que hay pandilla, cuando el delito se comete en común por tres o más personas, que se reúnen ocasional o habitualmente, sin estar organizados con fines delictuosos.*
>
> *Cuando el miembro de la pandilla sea o haya sido servidor público de alguna corporación policíaca, se aumentará en dos terceras partes de las penas que le corresponda por el o los delitos cometidos y se impondrá además, destitución*

[114] Vargas, Leticia, Pandilla, "asociación delictuosa y delincuencia organizada en el nuevo Código Penal para el Distrito Federal", en García, S, González, O (Coords.), Terceras jornadas sobre justicia penal "Fernando Castellano Tena", UNAM, Instituto de Investigaciones Jurídicas, México, 2003, p. 285, *http://ru.juridicas.unam.mx/xmlui/handle/123456789/9959*, de 10 de agosto de 2021, 09:32 p.m.

[115] Artículo 252, Código Penal para el Distrito Federal, *https://data.consejeria.cdmx.gob.mx/images/leyes/codigos/CODIGO_PENAL_PARA_EL_DF_6.pdf*, de 25 de octubre de 2021, 08:12 p.m.

del empleo, cargo o comisión e inhabilitación de uno a cinco años para desempeñar otro.

En ese sentido cuando se hace mención de que el miembro de la pandilla, "sea o haya sido servidor público de alguna corporación policiaca…", se atenta contra el deber de impartición de justicia del servidor público, esto es que se cumplan sistemáticamente las leyes, violentando los principios consagrados en el artículo 21, párrafo 9º de nuestra Carta Magna[116], que dice, "la actuación de las instituciones de seguridad pública se regirá por los principios de legalidad, objetividad, eficiencia, profesionalismo, honradez y respeto a los derechos humanos reconocidos en esta Constitución", así como en contra del Código de Conducta de la Policía Federal, que en su numeral IV. Misión de la Policía Federal, nos dice:

Prevenir y combatir la comisión de delitos en apego al marco jurídico, con personal comprometido y calificado, en coordinación con los tres órdenes de gobierno, que privilegie la participación ciudadana, para salvaguardar la integridad y derechos de las personas e instituciones, mediante programas y acciones desarrollados con esquemas de inteligencia y tecnología de vanguardia, que den confianza y certidumbre a la sociedad[117].

Aunado a lo anterior, si bien una pandilla puede estar conformada por distintos miembros, en el caso de ser parte de una corporación policíaca e ir en contra de las instituciones legales a las que representa, la pena se agravará y aumentará.

Agruparse, juntarse para delinquir, buscar a personas con las cuales poderse asociar como un negocio, y si el negocio delincuencial sale bien, mantener una estrategia para continuar con los delitos conjuntos, de una forma constante, estar consciente de que se unió al grupo para delinquir, para actuar a favor de la asociación, Maggiore, Guisepe, citado por Francisco Pavón[118], nos dice que la asociación no es más que el pacto realizado "entre varias personas para consumar un delito para utilidad común o respectiva de todos los asociados",

[116] Artículo 21, párrafo 9º, CPEUM, op.cit.
[117]Numeral IV, Código de Conducta de la Policía Federal. *https://www.gob.mx/cms/uploads/attachment/file/477057/CODIGO_DE_CONDUCTA_POLICIA_FEDERAL.pdf*, de 11 de agosto de 2021, 10:23 p.m.
[118]Pavón, Francisco, "Manual de Derecho Penal Mexicano", Parte General, 21a, ed., Porrúa, México, 2018, p. 702.

así la asociación delictuosa (conocida también como banda), nos dice Griselda Amuchategui[119], "*se integra por un grupo o banda de tres o más personas con el propósito de delinquir. Se castiga por el simple hecho de ser miembro de esa asociación*".

Entendemos que dentro de la asociación delictuosa de debe estar dispuesto de forma constante a participar y colaborar de una u otra manera en la comisión del delito, así en términos del artículo 164[120] del Código Penal Federal y 253[121] del Código Penal Para el Distrito Federal, "*al que forme parte de una asociación o banda de tres o más personas con el propósito de delinquir…*"

La asociación o banda, se constituye por tres o más personas con el propósito de delinquir, por lo que el tipo, nos dice Leticia Vargas.

> *…exige únicamente dos elementos para su integración: 1) formar parte de una asociación o banda compuesta de tres o más individuos, y 2) que los sujetos tengan el propósito de delinquir (puede ser cualquier delito)", mencionando de igual manera lo siguiente, "el legislador actual continuó conceptualizando a la figura de asociación delictuosa como un tipo penal autónomo, al castigar el mero hecho de formar parte de una asociación o banda que tiene el propósito de delinquir*…[122]

En ese orden de ideas las agravantes las encontramos cuando el miembro de la asociación ha sido servidor público o autoridad encargada de la función de seguridad pública, miembro de las Fuerzas Armadas Mexicanas o miembro de una empresa de seguridad privada, en términos del artículo 164[123] del CPF y 255[124] del CPDF. De esta forma, es orientadora la tesis de jurisprudencia, No. 369, sostenida por la Primera Sala, localizada en la Séptima Época, página

[119] Amuchategui, Griselda. "Derecho Penal", Colección de Textos Universitarios. 4a., ed., Oxford University Pres, México, 2012, p. 121.
[120] Artículo 164, Código Penal Federal, https://www.diputados.gob.mx/LeyesBiblio/pdf/CPF.pdf, de 11 de agosto de 2021, 09:42 p.m.
[121] Artículo 253, CPDF, op.cit.
[122] Vargas, Leticia, op. cit.
[123] Artículo 164, CPF, op.cit.
[124] Artículo 255, CPDF, op. cit.

174, publicada en el Semanario Judicial de la Federación, cuyo rubro y texto son:

> *Asociación delictuosa y pandillerismo. Sus diferencias (legislación del estado de Baja California)*
>
> *Hay claras notas distintivas entre el llamado pandillerismo y la asociación delictuosa. En el primero se trata de una reunión habitual, ocasional o transitoria de tres o más personas que sin estar organizadas con fines delictuosos, cometen comunitariamente algún ilícito; en cambio, la asociación delictuosa se integra también al tomar participación en una banda, tres o más personas, pero precisa que aquélla -la banda- esté organizada para delinquir. Aquí se advierte la primera distinción entre una y otra de las figuras analizadas: la consistente en que en el pandillerismo no hay organización con fines delictuosos, y en la asociación sí la hay. Pero todavía más: en esta segunda figura se requiere un régimen determinado con el propósito de estar delinquiendo, aceptado previamente por los componentes del grupo o banda; es decir, que debe haber jerarquía entre los miembros que la forman, con el reconocimiento de la autoridad sobre ellos del que la manda, quien tiene medios o manera de imponer su voluntad*[125].

Por otra parte, dentro de nuestra Carta Magna, su artículo 16, párrafo noveno[126], en relación a la delincuencia organizada, refiere *"por delincuencia organizada se entiende una organización de hecho de tres o más personas, para cometer delitos en forma permanente o reiterada, en los términos de la ley de la materia"*, mientras que el artículo 2 de la Ley Federal contra la Delincuencia Organizada (LFCDO), señala:

> *Las personas que se organicen de hecho para realizar, en forma permanente o reiterada, conductas que por sí o unidas a otras, tienen como fin o resultado cometer alguno o algunos de los delitos siguientes: terrorismo y su financiamiento, contra la salud, falsificación, operaciones con recursos de procedencia ilícita, en materia de derechos de autor, acopio y tráfico de armas, tráfico de personas, tráfico de órganos delitos contra la salud en su modalidad de narcomenudeo, corrupción de personas menores de dieciocho años de edad o de personas que no tienen capacidad para comprender el significado del hecho o de personas que no tienen capacidad para resistirlo, pornografía de personas menores de dieciocho años de edad o de personas que no tienen capacidad para comprender el significado del hecho o de personas que no tienen capacidad para resistirlo, turismo sexual en contra de personas menores de dieciocho años de edad o de personas que no tienen capacidad para comprender el significado del hecho o de personas que no tiene capacidad para resistirlo, lenocinio de personas menores de dieciocho años de edad o de personas que no tienen capacidad para comprender el significado del hecho o de personas que no tienen capacidad para resistirlo, tráfico de menores o*

[125] Cfr., Tesis aislada 369, Semanario Judicial de la Federación, Séptima Época, t. II, penal, p. 174, *https://sjf2.scjn.gob.mx/detalle/tesis/905310*, de 11 de agosto de 2021, 10:29 p.m.
[126] Artículo 16, párrafo noveno, CPEUM, op.cit.

> *personas que no tienen capacidad para comprender el significado del hecho, robo de vehículos, delitos en materia de trata de personas, contrabando y su equiparable, defraudación fiscal, operaciones inexistentes, falsas o actos jurídicos simulados, contra el ambiente*[127]*.*

Hablar de delincuencia organizada en el ciberespacio o *cibergangs*[128], atacando sistemas informáticos, o aquellos equipos con funcionamiento informático, desde computadores, celulares, televisores inteligentes, hasta autos, refrigeradores, consolas de videojuegos, etc., es hablar de personas interconectadas desde diferentes puntos, muchos de ellos emergen del conocimiento, pues se ha detectado que son ingenieros informáticos y programadores, los cuales poseen los conocimientos e infraestructura necesaria para la irrupción no autorizada de sistemas.

Sin embargo estas redes de delincuencia emergentes, se conectan con más personas, por medio de foros y chats, actualizándose constantemente, entrando y saliendo de la *Deep web* y de la red invisible (como foros encriptados en los que solo se puede acceder con invitación), así como de diferentes equipos sin ser detectados, marcando rumbos nuevos de la delincuencia.

Conforme a lo anterior, una nueva forma criminal emerge del desarrollo tecnológico, y nos enfrentamos a fraudes electrónicos, robos de divisas, de información empresarial, atentados en contra de sistemas gubernamentales, de empresas que desarrollan energía eléctrica, nuclear, un constante robo de identidad invade la red, un constante intercambio de datos, ya sea simple información o información confidencial, vulnerando miles de millones de dispositivos, conectados o no a la red, respondiendo ante ello.

El sistema jurídico comienza a estudiar, acotar y castigar a dichos delincuentes, ya que los delitos informáticos, la mayoría de las veces son planificados,

[127]Artículo 2, Ley Federal contra la Delincuencia Organizada, https://www.diputados.gob.mx/LeyesBiblio/pdf/101_200521.pdf, de 12 de agosto de 2021, 10:32 p.m.
[128] Cfr., Bergersen, Ben, "Pandillas cibernéticas en un mundo concreto", "Las pandillas cibernéticas son grupos de personas que se congregan en línea para perpetrar fracturas ilegales y poco éticas para obtener beneficios económicos y placer. Los miembros pueden estar separados geográficamente y comunicarse únicamente a través de Internet", CISSP MCSE MCT, *http://all.net/CID/Threat/papers/CyberGangs.html,* de 10 de octubre de 2021, 09:34 p.m.

teniendo un interesante proceso, dependiendo de si se aplicó o no ingeniería social, esto es, un estudio del objetivo u objetivos, del sujeto o sujetos pasivos.

Los ataques pueden tener múltiples variantes, si es una sola persona, si es una persona programando *bots* (persona falsa), si se coordinan dos o más, si son dos o más utilizando *bots*, y ¿por qué no decirlo?, *bots* utilizando *bots* (persona falsa e inteligencia artificial), en ese tenor se organizan grupos delincuenciales, como los denominados *Hackers*, de los cuales tenemos múltiples nombres y ataques, tanto dentro como fuera del país.

Conforme a lo anterior, algunos de estos grupos son: *Bandidos Revolution Team* -manipulación del Sistema de Pagos Electrónicos Interbancarios del Banco de México, mejor conocido como SPEI-; grupo QQAAZZ[129], "Estados Unidos acusa al grupo QQAAZZ por lavado de dinero para bandas de malware"[130], "los miembros de QQAAZZ estaban organizados en una jerarquía empresarial.

Los líderes se encargaban de las comunicaciones con los clientes, los gerentes de nivel medio reclutaban mulas de dinero y las mulas de dinero abrían cuentas bancarias y retiraban dinero de los cajeros automáticos, cuando era necesario"; "ZHANG Haoran, TAN Dailin, QIAN Chuan , FU Qiang y JIANG Lizhi forman parte de un grupo de piratería chino conocido como APT 41 y BARIUM", atacaron a empresas de Australia, Brasil, Alemania, India, Japón y Suecia, como refiere la siguiente nota.

> *"El 15 de agosto de 2019, un Gran Jurado en el Distrito de Columbia emitió una acusación formal contra los ciudadanos chinos ZHANG Haoran y TAN Dailin por cargos que incluyen acceso no autorizado a computadoras protegidas, robo de identidad agravado, lavado de dinero y fraude electrónico. Estos cargos se*

[129]Cfr., Departamento de Justicia de Estados Unidos, "Dos acusados se declaran culpables por su papel en ayudar a los ciberdelincuentes a lavar dinero como parte de la organización QQAAZZ", Oficina del Fiscal de EE. UU., Distrito occidental de Pensilvania, Publicado el 06/08/2021, https://www.justice.gov/usao-wdpa/pr/two-defendants-plead-guilty-their-roles-helping-cybercriminals-launder-money-part, de 16 de agosto de 2021, 06:12 p.m.

[130] Cfr., Catalin, Cimpanu, "Estados Unidos acusa al grupo QQAAZZ por lavado de dinero para bandas de malware", ZNNet, 15/10/2020, *https://www.zdnet.com/article/us-charges-qqaazz-group-for-laundering-money-for-malware-gangs/,* 16 de agosto de 2021, 06:36 p.m.

derivaron principalmente de una supuesta actividad dirigida a empresas de alta tecnología y videojuegos, y a un ciudadano del Reino Unido"[131]

Cabe mencionar que dentro de los grupos de ciberdelincuentes, participan de igual forma mujeres, como en el caso de la hacker rusa y su participación con otros delincuentes informáticos, Kristina Svechinskaya[132] quien fue acusada de "*formar parte de una banda de estafadores cibernéticos que intentaron robarse más de 220 millones de dólares (unos 450 mil millones de pesos colombianos), informó el dailymail.com.*", por lo que este tipo de delitos emergentes no tiene limitaciones en cuanto a género.

En base a lo anterior, los delitos cibernéticos son "*actos planificados y racionales que reflejan el esfuerzo de grupos de individuos*"[133], en ese sentido las actividades y formas emergentes del crimen organizado, se reestructuran constantemente, ya que su evolución no se detiene, pese a ello, la normativa Nacional e Internacional, debe evolucionar, estudiando y analizando los códigos de conducta criminal cibernéticos, tomando en cuenta la tipificación del delito Informático, y con ella la variación de partícipes del delito, y su conducta como delincuencia organizada, "*la organización de delincuentes mediante tecnologías de red no solo es una cuestión muy diferente de la forma en que los delincuentes organizan los delitos en línea, sino que esta última depende también del nivel de las tecnologías utilizadas, de los actos delictivos concretos que se cometen y también de los grupos de víctimas previstos*" (Serie de Módulos Universitarios)[134].

Así tanto una sola persona como un grupo de dos o más que pudiesen llegar a tener la infraestructura y los conocimientos adecuados, pueden cometer delitos

[131]Cfr., FBI. Más Buscados, "GRUPO APT 41", Sitio WEB, Gobierno de los Estados Unidos, *https://www.fbi.gov/wanted/cyber/apt-41-group,* de 16 de agosto de 2021, 07:26 p.m.
[132]Crf., El espectador, "Llevan a juicio a la hacker más sexy del mundo", 2010, *https://www.elespectador.com/tecnologia/llevan-a-juicio-a-la-hacker-mas-sexy-del-mundo-article-229691/,* de 17 de agosto de 2021, 07:31 p.m.
[133]UNODC, "Serie de Módulos Universitarios: Delitos Cibernéticos", La Declaración de Doha *https://www.unodc.org/e4j/es/cybercrime/module-13/key-issues/conclusion.html,* de 17 de agosto de 2021, 07:58 p.m.
[134] UNODC, "delitos cibernéticos organizados pueden incluir grupos delictivos organizados que participan en el delito cibernético y delincuentes cibernéticos u otros grupos que no cumplen los criterios establecidos en la Convención contra la Delincuencia Organizada, que realizan actividades típicamente asociadas con la delincuencia organizada", Ídem.

informáticos, de esta manera comete delito informático, con base en el artículo 217 del Código Penal de Sinaloa, quien dolosamente y sin derecho:

> *Comete delito informático, la persona que dolosamente y sin derecho:*
>
> *I. Use o entre a una base de datos, sistema de computadores o red de computadoras o a cualquier parte de la misma, con el propósito de diseñar, ejecutar o alterar un esquema o artificio, con el fin de defraudar, obtener dinero, bienes o información; o*
>
> *II. Intercepte, interfiera, reciba, use, altere, dañe o destruya un soporte lógico o programa de computadora o los datos contenidos en la misma, en la base, sistema o red.*
>
> *Al responsable de delito informático se le impondrá una pena de seis meses a dos años de prisión y de noventa a trescientos días multa*[135]

II. Responsabilidad de quienes son partícipes del robo de datos

El fenómeno de los delitos informáticos y el ciberespacio es complejo, ya que el poder inculpar a alguien dentro de este terreno se torna muy difuso actualmente, pues en el seno de la estructura de redes y ciberespacio, pueden confundirse los partícipes, dependiendo de las habilidades y capacidad de infraestructura del delincuente y/o delincuentes, conforme a lo anterior, la complejidad en el estudio y manejo de este tipo de delitos, abarca desde conocimientos informáticos correctos y de carácter especial para cometerlos, hasta la capacidad y evolución adecuada para ingresar a un sistema informático, que va desde quienes rompen los códigos de acceso, hasta quienes sin ser detectados manipulan el aparato, siendo de suma importancia para la no detección del delincuente, actuar y desaparecer de forma sigilosa, casi imperceptible, buscando por todos los medios no dejar rastros o huellas.

El uso de un sistema informático por el delincuente puede darse desde diferentes escenarios, esto es, ingresando de manera forzada y sin permiso, por medio virtual o remoto, o mediante dispositivos externos que pueden ser conectados al sistema informático, haciendo uso de programas para romper

[135] Artículo 217, Código Penal de Sinaloa, http://www.congresosinaloa.gob.mx/images/congreso/leyes/zip/codigo_penal_28-dic-2016.pdf, de 17 de agosto de 2021, 08:35 p.m.

códigos (intrusión), como los ataques de fuerza bruta creados con el fin de lanzar múltiples claves para poder ingresar al sistema, rompiendo su seguridad al enviarlas al azar, obteniendo con ello el código de acceso de algún sistema, pues se puede utilizar desde un aparato ubicado en un cibercafé hasta ingresar por medio del *WI FI* a uno o varios ordenadores, los cuales a su vez podrán ser utilizados para cometer el o los delitos, lo que nos hace pensar en la protección de redes abiertas pertenecientes al Estado y que brindan un servicio gratuito.

A mayor organización, mayor elaboración, entre más grande y compleja sea la organización más difícil será saber lo que se le atribuye a cada participe, esto es, su responsabilidad, asignar el nivel de autoría, que va desde quien crea un *malware malicioso* (gusano, virus, troyano, *spyware*-espía información de un usuario o empresa, *adware*-publicidad, *radsomware*-secuestra datos), hasta quien lo vende, compra o utiliza en un ataque, no es ni será sencillo, como se muestra en el siguiente ejemplo (tomado del código de conducta propio del hacker y/o algunos hackers como FXMSP[136]):

- Desactivar la seguridad. (Deshabilitar el *software* antivirus y el *firewall*[137] existente).
- Agregar y crear cuentas adicionales (con el fin de ocultar los signos del ataque).
- Crear una puerta trasera que envié los datos a sus servidores, propiedad de los atacantes.
- Recolectar y descifrar los datos.
- Infectar los respaldos de seguridad, por si la víctima detecta alguna actividad sospechosa en el sistema, lo más probable es que simplemente corriera un respaldo de seguridad, sin saber que este ya había sido comprometido, esto permite pasar desapercibido por mucho tiempo[138].

[136] BBC News Mundo, “Andrey Turchin, el hacker llamado "el dios invisible" al que acusan de robar información de 300 empresas en 44 países”, Redacción, 2020, *https://www.bbc.com/mundo/noticias-53559843,* de 30 de agosto de 2021.
[137] Cfr., Oxford Languages, “*Firewall*. Programa informático que controla el acceso de una computadora a la red y de elementos de la red a la computadora, por motivos de seguridad”. Oxford Languages and Google, 2022, *https://languages.oup.com/google-dictionary-es/,* de 30 de agosto de 2021, 10:45 p.m.
[138] Youtube, “Cómo INTERPOL Atrapó al Hacker FXMSP "EL DIOS INVISIBLE DE LAS REDES", Noticias Seguridad Informática, Video, *https://www.youtube.com/watch?v=3BD23zuaepQ&ab_channel=NoticiasSeguridadInform%C3%A1tica*, de 01 de septiembre de 2021, 08:54 p.m.

Como podemos ver en el ejemplo anterior, se perciben dentro de este modo de operar, las siguientes características: conocimientos de informática, capacidad de infraestructura, capacidad de acción, combinación de acciones y *malwares* (gusano, virus, troyano, *bonets*[139], etc.), plan de infección de los respaldos de seguridad (como medio de protección) y principalmente un objetivo esencial que es "recolectar y descifrar los datos", lo que demuestra un estudio previo del hecho.

Otro hecho relacionado con el ataque a una empresa, de la cual se buscaba perdiera la oportunidad de contratos y concesiones resultado de un concurso de selección, nos da muestras de la técnica, plan o forma en que se cometió el delito, en el cual se observan claros tintes de un estudio previo basado en ingeniería social, ya que las fuentes principales de información son provenientes del estudio de la empresa, así la recolección de información a través de redes sociales, perfiles de trabajadores de la empresa al ofrecerse trabajos a ex empleados (basándose en perfiles de ingenieros), para entrevistarlos de forma presencial o no (entrevistas virtuales), y obtener más información, partiendo de lo que arrojó la investigación de redes sociales, esto es obtener información del personal, de operadores, jefes, problemas relacionados con la empresa a nivel trabajador, personas claves dentro de la empresa (niveles en la cadena de toma de decisiones en la empresa, ¿en dónde están?, ¿cómo se llaman?, ¿quiénes son del departamento de recursos humanos?, para obtener más información, así como el personal a cargo de la oficina o departamento de interés del o delincuentes.

Del modo de operar se desprende, que se engaña a ciertos empleados de la empresa objetivo, ofreciéndoles una entrevista de trabajo con un sueldo muy

[139] Cfr., Fisher, Dennis, "Definición de *Botnet*. Es el nombre genérico que denomina a cualquier grupo de PC infectados y controlados por un atacante de forma remota. Generalmente, un hacker o un grupo de ellos crea un botnet usando un malware que infecta a una gran cantidad de máquinas. Los ordenadores son parte del botnet, llamados "bots" o "zombies". No existe un número mínimo de equipos para crear un botnet. Los botnets pequeños pueden incluir cientos de PCs infectados, mientras que los mayores utilizan millones de equipos. Algunos ejemplos de botnets recientes son Conficker, Zeus, Waledac, Mariposa y Kelihos. A menudo, se entiende el botnet como una entidad única, sin embargo los creadores de este malware lo venden a cualquiera que pague por él. Por este motivo, existen docenas de botnets separados usando el mismo malware y operando a la vez", Karsperky daily, 2013, *https://www.kaspersky.es/blog/que-es-un-botnet/755/,* de 01 de septiembre de 2021, 09:38 p.m.

superior al ofrecido o pagado por la empresa en la que laboran, como consecuencia de la misma, se les envía un archivo en WORD infectado, resultando lo siguiente: se ejecuta una macro[140], que descarga un binario; ese binario a su vez es ejecutado obteniendo acceso al equipo; se utilizan funciones de *keylogger* para infectar a la empresa; al conocer la estructura de la empresa, se procede a infectar al resto de los equipos hasta llegar al objetivo, "el responsable de la oficina y/o departamento de interés"; desaparece de la red la supuesta empresa que ofreció el trabajo y entrevistas; se cierran los perfiles; se elimina cualquier rastro del binario; y por fin, se pierde la concesión (que sería de varios millones de euros)[141].

De esta forma saber quién es el autor y quien el partícipe, es fundamental para la aplicación correcta de la ley penal, pues si partimos de la "Teoría del dominio del hecho" de Claus Roxin, el autor es quien ejerce el dominio del hecho dirigiéndose a la realización del delito, el responsable del hecho, así en el tema que nos ocupa, el ciber-autor será quien tiene el dominio del hecho, no obstante el escenario se vuelve complicado cuando se realiza el mismo desde cierto o ciertos sistemas informáticos, por esta razón se puede creer que el atacante es el usuario que se encuentra conectado, sin embargo el mismo podría haber sido objeto de un ataque siendo controlado su ordenador o sistema desde otro dispositivo, por ende el dominio del hecho lo realiza quien de forma virtual o remota ha manipulado o manipula el sistema, por lo que el usuario que se encuentra conectado, quien muchas de las veces ni se entera que su dispositivo fue usado para un ataque, no será quien tiene el dominio del hecho sirviendo solo como medio para la realización del delito, en el caso de ingresar a un sistema sin permiso pero cuando se ingresa con permiso y se comete el delito, sin que el usuario sea el autor, esto es sin que realice la acción y sin

[140] Cfr., ALEGSA.com.ar, "Macro. Almacenamiento cronológico de pulsaciones de teclas, acciones de comandos, instrucciones, e incluso movimientos del mouse, con el fin de automatizar o economizar procedimientos. El lenguaje de macros para Word ha sido utilizado para crear llamados macrovirus", Diccionario de informática y tecnología, *https://www.alegsa.com.ar/Dic/macro.php*, de 22 de septiembre de 2021, a las 09:03 p,m.
[141] CCN-CERT, "Ciberdelincuencia Organizada, caso práctico: Inteligencia económica...", UCO, Guardia Civil, España, 2018, *https://www.youtube.com/watch?v=NThbCnhG8AA&ab_channel=CCN,* de 06 de septiembre de 2021, 08:15 p.m.

tener conocimiento del probable delito, en el entendido de que se utilizó el equipo por alguien al que se le permitió, el usuario sigue siendo el medio sin ser consciente de que su sistema fue usado en la comisión de un delito, por ello quien utiliza el sistema para cometer el delito será el autor y/o ciber-autor.

A menos que por medio del usuario, y con el consentimiento del mismo, se realice el ataque, como autor mediato (quien se sirve de otro para cometer el delito), así quien tiene el dominio del hecho por medio de la voluntad, será el autor y/o ciber-autor, mientras quien realiza la acción al ejecutarla será el tercero utilizado como medio o instrumento, quien a su vez se encuentra controlado por el autor y/o ciber-autor, si el usuario no sabe realmente que está siendo utilizado para cometer un delito este no será autor (inimputable).

Por otra parte puede contratar a otra persona un autor intelectual (quien determina dolosamente a otro a cometer la conducta típica), al que le interesa la información, de este modo quien se contrata será el autor material al ser quien comete el delito, siendo determinado y actuando libremente por el contratante. En otro caso quien tiene el domino del hecho a través del dominio de la voluntad sobre otra persona que actúa bajo coacción (estando bajo amenazas), será el autor y/o ciber-autor, ya que al ser utilizado no será responsable ya que carece de la voluntad para llevar a cabo el delito.

Otro ejemplo es cuando la persona actúa bajo error, como en el caso de que se le pida enviar un correo electrónico a cierto individuo o empresa, sin saber que el archivo que se le ha pedido enviar contiene un *malware*, de esta forma el autor material se encuentra dominado por quien género o inserto dicho malware en el archivo enviado por correo, esto es el que pide que envié el correo, ejerciendo su voluntad por medio de quien envió el mensaje, por lo que este último no será quien comete el delito.

El estudio de la coautoría en los delitos informáticos es de suma importancia, ya que muchos son cometidos en forma grupal, al examinar la evolución de variantes, técnicas y formas en que se han manifestado estos delitos, podremos

comprender su complejidad tanto individual como grupal, ya que dentro del proceso de acción son utilizadas diferentes herramientas e información, las cuales muchas veces son compartidas e intercambiadas con otros delincuentes que ya las han utilizado con anterioridad, mejorándolas y aplicándolas conforme a variantes necesarias en la comisión del delito y la complejidad del sujeto pasivo u objetivo del ataque, esto es la estructura de los sistemas de seguridad tanto de una persona física como moral, ello por las características de sistemas y equipos informáticos, como computadoras, programas informáticos, medios electrónicos, Internet, etc., en este orden de ideas la coautoría se manifiesta en el acuerdo previo al que llegan los partícipes del hecho delictuoso, así como la división del trabajo y el aporte necesarios para la realización del delito, de esta manera cada partícipe tiene el dominio del hecho, por ello la tarea o parte asumida de forma individual es indispensable para la realización del acto delictivo.

Al hablar de cooperadores necesarios, en relación al delito de falsificación (relacionado con el robo de datos), Martínez Arrieta, citado por Velazco, E, nos dice que, considera colaborador necesario por aporte causal a la conducta típica de la duplicación de tarjetas.

> *…proporcionar el dato de poner en contacto con quien efectivamente después las clona, así como, en un claro ejercicio de división de funciones, tanto copiarlas, doblarlas como acometer informáticamente la incorporación de la banda magnética sustraída a otra tarjeta, ya que a partir de la primera conducta surge la potencialidad de crear dinero falso…*[142]

En este caso el aporte voluntario de cada uno de quienes participan en la comisión del hecho antijurídico, es necesario para que pueda llevarse a cabo, por lo que, como refiere Martínez Arrieta, citado una vez más por Velazco, "*Se está en un caso de puesta en común de las voluntades de todos en un único y*

[142] Cfr., Velazco, Eloy, "Crimen Organizado, Internet y Nuevas Tecnologías", Juzgado Central de Instrucción 6 de la Audiencia Nacional, p. 265, *https://core.ac.uk/download/pdf/61904318.pdf*, de 19 de septiembre de 2021, 07:42 p.m.

común proyecto delictivo, aunque cada integrante tenga diversos y distintos pero relevantes cometidos. Es un caso claro de coautoría"[143].

Como podemos observar de lo anterior, en la actualidad se presentan dificultades para poder identificar a los autores de los delitos informáticos, si partimos de las pruebas presentadas en un proceso penal, es necesario un adecuado y minucioso estudio de los equipos informáticos y sistemas involucrados en el delito, derivado de la posibilidad de encriptación y la naturaleza inestable de los datos e información, así como de las técnicas aplicadas en el ocultamiento y borrado del ataque, sin olvidar la utilización de direcciones IP dinámicas que permiten utilizar de forma temporal al usuario o manipular las direcciones IP, por lo que se torna necesaria una eficaz y adecuada autopsia forense del ordenador, sumada a una constante participación y promoción del desarrollo de la denominada "Informática Forense"[144], ya que si no se realiza de forma adecuada el estudio del sistema y equipo informático, podríamos inculpar a una o varias personas inocentes.

Las formas de autoría y participación en la CDMX son normadas en el Código Penal para el Distrito Federal, por lo que las normas contenidas en dicho ordenamiento se deben adaptar de forma correcta a los delitos informáticos, lo cual será un trabajo arduo para poder sancionar a los delincuentes informáticos de forma correcta, no permitiendo que los mismos queden impunes y/o pueda inculparse a quien no cometió el delito, en ese sentido los artículos 22 y 24[145] del citado ordenamiento nos dicen:

> *Artículo 22. (Formas de autoría y participación). Son responsables del delito, quienes:*
>
> *I. Lo realicen por sí;*
>
> *II. Lo realicen conjuntamente con otro u otros autores;*

[143] ídem.
[144] Cfr., Wikipedia, "El cómputo forense, también llamado informática forense, computación forense, análisis forense digital o examen forense digital es la aplicación de técnicas científicas y analíticas especializadas a infraestructuras tecnológicas que permiten identificar, preservar, analizar y presentar datos válidos dentro de un proceso legal". *https://es.wikipedia.org/wiki/C%C3%B3mputo_forense,* de 19 de septiembre de 2021, 10:06 p.m.
[145] Artículos 22, 24, CPDF, op.cit.

III. Lo lleven a cabo sirviéndose de otro como instrumento;

IV. Determinen dolosamente al autor a cometerlo;

V. Dolosamente presten ayuda o auxilio al autor para su comisión; y

VI. Con posterioridad a su ejecución auxilien, al autor en cumplimiento de una promesa anterior al delito.

Quienes únicamente intervengan en la planeación o preparación del delito, así como quienes determinen a otro o le presten ayuda o auxilio, sólo responderán si el hecho antijurídico del autor alcanza al menos el grado de tentativa del delito que se quiso cometer.

La instigación y la complicidad a que se refieren las fracciones IV y V, respectivamente, sólo son admisibles en los delitos dolosos. Para las hipótesis previstas en las fracciones V y VI se impondrá la punibilidad dispuesta en el artículo 81 de este Código.

Artículo 24 (Culpabilidad personal y punibilidad independiente). Los autores o partícipes del delito responderán cada uno en la medida de su propia culpabilidad.

Cabe señalar que en la actualidad es de suma importancia tomar en cuenta la responsabilidad civil, penal y administrativa, que los "prestadores de servicios de la sociedad de la información[146]" adquieren por sus actividades de intermediación, como en el caso de España, lo que se muestra a continuación, con base en el artículo 13 y demás correlativos, contenidos en la Sección Segunda innominada "Régimen de Responsabilidad", de la Ley 34/2002[147], de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico:

Artículo 13. Responsabilidad de los prestadores de los servicios de la sociedad de la información.

1. Los prestadores de servicios de la sociedad de la información están sujetos a la responsabilidad civil, penal y administrativa establecida con carácter general en el ordenamiento jurídico, sin perjuicio de lo dispuesto en esta Ley.

[146] Cfr., Sociedad de la información. "La sociedad de la información es un proceso de evolución profunda de la vida y las intersecciones entre personas, gobiernos, facultades y organizaciones por el uso intensivo de las tecnologías de la información y la comunicación (TIC), que facilitan la creación, distribución y manipulación de la información y desempeñan un papel esencial en las actividades sociales, culturales y económicas. La noción de sociedad de la información ha sido inspirada por los programas de desarrollo de los países industrializados, y el término ha tenido una connotación más política que teórica, pues a menudo se presenta como una aspiración estratégica que permitiría superar el estancamiento social", *https://es.wikipedia.org/wiki/Sociedad_de_la_informaci%C3%B3n,* de 20 de septiembre de 2021, 09:38 p.m.

[147] Ley 34/2002, de 11 de julio, "Servicios de la Sociedad de la Información y de Comercio Electrónico", Jefatura del Estado, España, núm 166, 2002, *de https://www.boe.es/buscar/pdf/2002/BOE-A-2002-13758-consolidado.pdf*, de 20 de septiembre de 2021, 08:58 p.m.

2. Para determinar la responsabilidad de los prestadores de servicios por el ejercicio de actividades de intermediación, se estará a lo establecido en los artículos siguientes.

Artículo 14. Responsabilidad de los operadores de redes y proveedores de acceso.

Artículo 15. Responsabilidad de los prestadores de servicios que realizan copia temporal de los datos solicitados por los usuarios.

Artículo 16. Responsabilidad de los prestadores de servicios de alojamiento o almacenamiento de datos.

Artículo 17. Responsabilidad de los prestadores de servicios que faciliten enlaces a contenidos o instrumentos de búsqueda.

Mientras en nuestro país se regula el comercio electrónico, como señala Villegas, R[148], de la siguiente forma: Ley Federal del Derecho de Autor, regula la protección en el contenido de una página de Internet desde el momento en que se plasma su contenido y se hace mención de estar protegidos los derechos de autor; Ley de la Propiedad Industrial regula lo concerniente a las marcas y signos distintivos que de los nombres de dominio u otras figuras se protejan; Ley Federal de Protección al Consumidor rige los contenidos y ofrecimientos de promociones y ofertas realizados por medios electrónicos; Código de Comercio y el Código Civil, rigen las operaciones comerciales e intercambio de datos e información que por medios electrónicos se lleve a cabo y las formas de expresar el consentimiento respectivamente; Los órganos reguladores relacionados pueden ser la Procuraduría Federal del Consumidor, el Instituto Mexicano de la Propiedad Industrial y la Secretaría de Economía; Código Fiscal de la Federación, en lo concerniente a la emisión de comprobantes fiscales digitales, la emisión de facturas electrónicas y el uso de la Firma Electrónica Avanzada, todo lo anterior para cuestiones meramente tributarias.

[148] Cfr, Villegas, Sául, "Marco jurídico del comercio electrónico en México", Raigosa Consultores. Consultado en línea el 20/09/2021 a las 09:28 p.m., de *http://www.raigosaconsultores.com/pdf/marco.pdf,* de 20 de septiembre de 2021, 09:28 p.m.

III. Cooperación conjunta entre Estados en relación al fenómeno delictivo

Al estudiar los delitos informáticos en el globo, son muchos los términos y formas que se han dado a los mismos, por lo que se han tenido que homologar poco a poco los criterios aplicados, así la cooperación internacional es fundamental en este emergente e impredecible fenómeno delictivo, como muestra el maestro Julio Téllez[149] en su libro intitulado "Derecho Informático", en el cual nos refiere, "el Manual de la Naciones Unidas para la prevención y control de delitos informáticos señala que cuando el problema aparece en el ámbito internacional, se magnifican los inconvenientes y las influencias, por cuanto los delitos informáticos constituyen una nueva forma de delito transnacional y su combate requiere una eficaz cooperación internacional concertada".

La importancia de la cooperación internacional viene a mostrar que los delitos informáticos al efectuarse en el campo del internet o las redes, y por ende alrededor del mundo, son poseedores de un potencial sumamente basto en la actualidad, ya que al fluir la información en múltiples y variadas cantidades, las posibilidades en el tráfico de redes[150], permiten la exponenciación de capacidad delictiva que las invade sigilosamente.

Los delincuentes informáticos internacionales, estudian las leyes de cada país para saber de qué forma podrán actuar (operar) sin ser procesados de forma eficiente, o en muchos de los casos delinquir libremente, por la débil normativa y sistemas de seguridad informática existentes en el país donde se encuentra el objetivo o sujeto pasivo que será atacado, de esta forma el acceso transfronterizo a las pruebas digitales, esto es los datos que son constituyentes de la prueba y que se encuentran en una jurisdicción distinta de aquella donde

[149] Téllez Valdés, Julio, "Derecho Informático", México, Mc Graw Hill, 4ª ed. 2009, pp, 192-193.
[150] Cfr., SolarWinds Worldwide, "El tráfico de red (también llamado tráfico o tráfico de datos) hace referencia a los datos que se desplazan por una red en un momento determinado", Monitor del tráfico de red, 2021, *https://www.solarwinds.com/es/network-bandwidth-analyzer-pack/use-cases/network-traffic-monitor,* de 21 septiembre de 2021, 08:38 p.m.

el delito es juzgado [151], es un problema continuo, ello aunado a la necesidad de una constante actualización de las normativas vigentes en relación a este tipo de delitos, así como al crecimiento de los dispositivos inteligentes, como nos refiere el Maestro Julio Téllez.

> *"El derecho penal de los Estados involucrados contiene vacíos jurídicos y diferencias importantes susceptibles de obstaculizar la lucha contra la delincuencia organizada y el terrorismo, así como los graves ataques contra los sistemas de información perpetrados por particulares. La aproximación del derecho positivo en materia de delincuencia informática contribuirá a que las legislaciones nacionales sean lo suficientemente completas para que las graves formas de ataques contra los sistemas de información puedan ser objeto de investigaciones mediante técnicas y los métodos disponibles en derecho penal"[152].*

Al hablar de ciberespacio, así como del uso, acceso e intercomunicación de la población, que conforman los Estados, su existencia e interrelación con otros Estados dentro del también conocido como ciberinfinito, ello aunado a la globalización y producción de nuevas tecnologías de la información, los países alrededor del mundo, son partícipes de la interacción constante de miles de millones de personas tanto físicas como morales, por ello es fundamental una constante cooperación internacional, ya que los tratados internacionales destinados al ciberderecho, cibercrimen y tecnologías emergentes, permitirán unificar toda la información entorno a los mismos, no solo en su investigación sino que de igual forma, en la jurisprudencia, sentencias y estudio del fenómeno delictivo, dentro y fuera de cada uno de los Estados en donde se ha cometido, impactando y atentando contra el bien jurídico, ello aunado a la ubicación espacial y temporal del hecho delictivo, así como su manifestación e impacto posterior o futuro, ayudará al desarrollo de una "Constitución del Ciberespacio" (Ciberconstitución), "un Código del Ciberespacio" (ya sea un Ciber Código Penal o Ciber Código de Procedimientos Penales), en el entendido de que los delitos informáticos poco a poco se han ido correlacionando con los delitos

[151] Asamblea General de la Naciones Unidas, "Lucha contra la utilización de las tecnologías de la información y las comunicaciones con fines delictivos", 2019, p 5/91, *https://www.unodc.org/documents/Cybercrime/SG_report/V1908185_S.pdf,* de 21 de septiembre de 2021, 08:23 p.m.
[152] Téllez Valdés, Julio, op. cit., p. 206.

conocidos, ya existentes en las legislaciones de todos los Estados del Globo, "Internet debe ser de jurisdicción internacional".

Los usuarios pueden acceder a esta red prácticamente desde cualquier lugar del mundo. Debido a la tecnología de conmutación de paquetes[153] y al complejo entramado de las redes digitales y la infraestructura de las telecomunicaciones, la información digitalizada puede viajar a través de diversos países y jurisdicciones, cada uno con su propio sistema jurídico[154]".

La cooperación internacional es y será siempre un fuerte instrumento que permitirá coordinar el estudio, manejo y aplicación de la ley en estos delitos, así de la Oficina de Naciones Unidas contra la Droga y el Delito (UNODC), en la Reunión del Grupo de Expertos encargado de Realizar un Estudio Exhaustivo sobre el Delito Cibernético celebrada en Viena del 27 al 29 de julio de 2020[155], se toman algunas de las siguientes conclusiones y recomendaciones preliminares sugeridas por los Estados Miembros:

En relación a la Cooperación:

> - En alcance de la definición de "delito cibernético", los Estados deberán tipificar como delito, los actos de ciberdelincuencia, quedando comprendidos los delitos basados en la cibernética y otros delitos que "*con frecuencia se cometen utilizando Internet y medios electrónicos (delitos facilitados por la cibernética), como el fraude cibernético, el robo cibernético, la extorsión, el blanqueo de dinero, el tráfico de drogas y armas, la pornografía infantil y actividades terroristas*".
>
> - Mecanismos de cooperación internacional. Los Estados utilizaran o deberán adherirse a los "*tratados multilaterales existentes que proporcionan una base jurídica para la prestación de asistencia judicial recíproca, como la Convención*

[153] Cfr., Wikipedia, "Conmutación de paquetes. La conmutación de paquetes es un método de agrupar los datos transmitidos a través de una red digital en paquetes", *https://es.wikipedia.org/wiki/Conmutaci%C3%B3n_de_paquetes,* de 30 de septiembre de 2021, 08:58 p.m.
[154] Téllez Valdés, Julio, op. cit., p. 224.
[155] Cfr., Grupo de Expertos encargado de Realizar un Estudio Exhaustivo sobre el Delito Cibernético, "Recopilación de todas las conclusiones y recomendaciones preliminares sugeridas por los Estados Miembros durante las reuniones del Grupo de Expertos encargado de realizar un estudio exhaustivo sobre el delito cibernético celebradas en 2018, 2019 y 2020". Viena, 6 a 8 de abril de 2021, *https://www.unodc.org/documents/organized-crime/cybercrime/Cybercrime-April-2021/CRP/V2101015.pdf,* de 22 de septiembre de 2021, 09:43 p.m.

de las Naciones Unidas contra la Delincuencia Organizada Transnacional y el Convenio sobre la Ciberdelincuencia del Consejo de Europa" (Convenio sobre ciberdelincuencia, firmado en Budapest Hungría el 23 de noviembre de 2001 y entrando en vigor el 01 de julio de 2004), este último debería de usarse como referencia en la creación de capacidad y la asistencia técnica en todo el mundo.

- Entorno a las investigaciones de delitos cibernéticos "*contar con socios estratégicos, como por ejemplo, los miembros de organizaciones existentes tales como la Organización de los Estados Americanos (OEA), el Grupo de los 7 y la Organización Internacional de Policía Criminal (INTERPOL)*".

- En investigaciones y procedimientos judiciales, deberían "*respetarse la soberanía y la jurisdicción de los Estados. No debería solicitarse a empresas o particulares la entrega directa de datos ubicados en otro país sin el consentimiento previo de este*".

- Debería mejorarse la eficiencia de la cooperación internacional "*estableciendo mecanismos de respuesta rápida para la cooperación internacional, así como canales de comunicación entre las autoridades nacionales mediante oficiales de enlace y sistemas informáticos para la reunión transfronteriza de pruebas y la transferencia en línea de pruebas electrónicas*".

- Los Estados deberían estudiar la posibilidad de crear "*protocolos innovadores de intercambio de información, incluidas la información de inteligencia y las pruebas de actos delictivos, a fin de agilizar esos procedimientos*".

- Es necesario "*preparar un procedimiento operativo estándar, que sea aceptable internacionalmente, para la reunión y conservación de datos, y que pueda aplicarse en la escena de un delito*".

- Es fundamental la "*adopción universal de prácticas internacionales estándar sobre la reunión, el almacenamiento y la compartición de pruebas, en particular en el proceso de investigación de delitos cibernéticos y el enjuiciamiento de ciberdelincuentes*".

- *Se recomendó la "aprobación de disposiciones que permitieran entablar una cooperación directa con los proveedores de servicios de Internet de otras*

jurisdicciones con respecto a solicitudes de información sobre los abonados[156] *y solicitudes de conservación de datos*".

- Las opciones para combatir la ciberdelincuencia y proteger las sociedades deben salvaguardar siempre los derechos humanos y las garantías constitucionales, y promover un ciberespacio más libre, abierto, seguro y resiliente para todos.

- Los Estados Miembros "*deberían intercambiar información sobre la forma en que se están resolviendo en el plano nacional los problemas para acceder de manera oportuna a las pruebas digitales*".

- Los países "*deberían mejorar la aplicación de las leyes nacionales y reforzar la coordinación y las sinergias a nivel interno para la reunión y el intercambio de información y pruebas con fines de enjuiciamiento*".

- Los Estados deberían "*fortalecer las medidas en lo que respecta al intercambio de información financiera o monetaria, la congelación de cuentas y el decomiso de bienes para garantizar que los delincuentes no puedan beneficiarse de las actividades delictivas*".

- Se los alienta a que "*continúen o inicien reformas de la legislación sobre el delito cibernético y las pruebas electrónicas, siguiendo los ejemplos positivos y las reformas emprendidas en todo el mundo*".

- Se recomienda "*elaborar marcos jurídicos que abarquen también los aspectos relacionados con la jurisdicción extraterritorial respecto de los actos de ciberdelincuencia*".

- Resultaría útil "*establecer un arreglo oficial con organizaciones como el Centro Europeo contra la Ciberdelincuencia de la Agencia de la Unión Europea para la Cooperación Policial (Europol), el Centro contra los Delitos Cibernéticos de los Estados Unidos de América, el Centro de Control del Delito Cibernético del Japón y el Centro Nacional de Seguridad Cibernética del Reino Unido de Gran Bretaña e Irlanda del Norte, con el fin de compartir información sobre las amenazas más recientes del delito cibernético, los modus operandi, la*

[156] Cfr., Gobierno del Ecuador, "El usuario que haya suscrito un contrato de adhesión con el prestador de servicios de Telecomunicaciones, se denomina abonado o suscriptor y el usuario que haya negociado las cláusulas con el prestador se denomina cliente". Agencia de Regulación y Control de las Telecomunicaciones "Derechos y obligaciones de los abonados, clientes y usuarios", Sistema Nacional de Información, *https://www.arcotel.gob.ec/derechos-de-los-abonados-clientes-y-usuarios/,* de 28 de septiembre de 2021, 08:30 p.m.

tecnología emergente para las investigaciones de delitos cibernéticos, así como para el acceso recíproco, las mejores prácticas, etc".

- Los Estados deberían llevar a cabo una cooperación eficaz en materia de extradición.

- Se recomienda crear un marco en el que quede claro que, en caso de "pérdida de la ubicación", "l*a decisión de proceder con una investigación requiere un esfuerzo para establecer qué territorio ha sido afectado, dónde es vital la integridad de las redes automatizadas para poder realizar consultas sobre cuestiones de jurisdicción, y cuál es la forma más adecuada de continuar las indagaciones*".

- Los Estados deberían establecer un "*mecanismo y un canal de comunicación de respuesta rápida para la asistencia judicial y la cooperación en materia de aplicación de la ley, y considerar la posibilidad de permitir el intercambio en línea de documentos jurídicos y pruebas electrónicas, con el apoyo de firmas electrónicas y otros medios técnicos*".

- La comunidad internacional debería "*formular un procedimiento unificado para las técnicas de investigación de los delitos cibernéticos y mejorar las disposiciones de su legislación interna relativas a las obligaciones de los proveedores de servicios de Internet de conservar registros*".

- Los Estados deberían "*impedir las transferencias internacionales del producto ilícito obtenido de los delitos cibernéticos y fortalecer la cooperación internacional en materia de recuperación de activos relacionados con el delito cibernético*".

En base a lo anterior damos cuenta de la importancia de la cooperación en relación al estudio y manejo del ciberdelito, ya que nos encontramos ante una compleja red de formas y estructuras del conocimiento que son utilizadas para delinquir, por lo que la correcta tipificación y análisis forense del fenómeno en la red, los sistemas y equipos informáticos, se vuelve complejo sin el intercambio de información, que con ayuda de agencias internacionales de policía, ciberpolicia internacional y organizaciones que han estudiado el modo de operar de los delincuentes informáticos, se lograra comprender y atacar el fenómeno.

Cabe mencionar la importancia de la evidencia digital, la cual debe ser recolectada de forma correcta y minuciosa, ya que mucha de ella puede venir encriptada y/o programada para automodificarse o ser bloqueada, así como ser sembrada de forma sigilosa con el fin de inculpar a otra persona ya sea moral o jurídica, de esta forma para poder llevar a cabo los juicios en esta materia la "cadena de custodia digital[157]" (y lo complejo de mantenerla a nivel de Red) es muy especial, de ahí la importancia del intercambio de información entre Estados, con el fin de adecuar la cooperación en los procedimientos de investigación.

La reforma a la legislación en torno al delito cibernético y las pruebas electrónicas, tomando ejemplos de leyes en otros países, actualiza los sistemas jurídicos y códigos penales que a la fecha convergen y son aplicados en cada Estado del Globo, lo cual retroalimenta el combate conjunto de los mismos.

Las acciones mencionadas para acotar al delincuente, y el control del mismo, tienen que ver con la extradición, bloqueo de cuentas, así como detener el uso de activos obtenidos de forma ilícita, facilitando la cooperación en los procesos judiciales, así como la evasión y movilidad del delincuente.

Por su parte en el Convenio de Budapest, se enmarcan los principios generales relativos a la asistencia mutua, la cual es de suma importancia entre los Estados, y que de esta manera con base al artículo 25 son los siguientes:

> *Las partes se prestarán toda ayuda mutua posible a efectos de las investigaciones o de los procedimientos relativos a los delitos relacionados con sistemas y datos informáticos o con el fin de obtener pruebas en formato electrónico de un delito.*

[157] Cfr.,Unidad de Investigaciones Cibernéticas y Operaciones Tecnológicas, "Cadena de Custodia Digital: Sistema de control y registro que se aplica al indicio o elemento material probatorio, desde su localización, descubrimiento o aportación, en el lugar de intervención, hasta que la autoridad competente ordene su conclusión", Guía Técnica de Cadena de Custodia de Evidencia Digital, PGR, México, 2018, *http://www.coahuilatransparente.gob.mx/disp/documentos_disp/GU%C3%8DA%20T%C3%89CNICA%20DE%20CADENA%20DE%20CUSTODIA%20DE%20EVIDENCIA%20DIGITAL.pdf,* de 29 de septiembre de 2021, 09:14 p.m.

Cada parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para cumplir con las obligaciones establecidas en los artículos 27 a 35.

Cada parte podrá, en caso de urgencia, formular una solicitud de asistencia mutua, o realizar las comunicaciones relativas a la misma a través de medios de comunicación rápidos, como el fax o el correo electrónico, siempre que esos medios ofrezcan niveles suficientes de seguridad y autenticación (incluido el encriptado, en caso necesario), confirmación oficial posterior si el Estado requerido así lo exige. El Estado requerido aceptará la solicitud y responderá a la misma por cualquiera de esos medios rápidos de comunicación.

Salvo en caso de que disponga expresamente otra cosa en los artículos del presente Capítulo, la asistencia mutua estará sujeta a las condiciones establecidas en el derecho interno de la Parte requerida o en los tratados de asistencia mutua aplicables, incluidos los motivos sobre la base de los cuales la Parte requerida puede rechazar la cooperación. La parte requerida o en los tratados de asistencia mutua aplicables, incluidos los motivos sobre la base de los cuales la Parte requerida puede rechazar la cooperación. La parte requerida no deberá ejercer su derecho a rehusar la asistencia mutua en relación con los delitos previstos en los artículos 2 a 11 únicamente porque la solicitud se refiera a un delito que dicha Parte considere de carácter fiscal.

Cuando, de conformidad con lo dispuesto en el presente Capítulo, la Parte requerida esté autorizada a condicionar la asistencia mutua a la existencia de doble tipificación penal, se considerará que dicha condición se satisface si el acto constituye delito, y para el que se solicita la asistencia mutua, está tipificado como tal en su derecho interno, independientemente de que dicho derecho interno incluya o no el delito en la misma categoría o lo denomine o no con la misma terminología que la Parte requirente[158]*.*

[158] Artículo 25, Convenio de Budapest, *http://documentostics.com/documentos/convenio_cibercriminalidad.pdf*, de 03 de octubre de 2021, 08:15 p.m.

Capítulo Cuarto

Generalidades del Robo de Datos

I. Reglamentación

Actualmente y debido al impacto de la pandemia de COVID-19, los procesos de revisión y actualización de las normas que son aplicadas al delito de robo de datos, se han acelerado de forma exponencial en todo el mundo, ya que el trabajo en casa, las reuniones virtuales, clases virtuales, sistemas de ventas de productos en línea, páginas y aplicaciones (como las bancarias y de prestaciones de servicios), redes sociales, videojuegos en línea, etc., es el nuevo y emergente campo de acción del delincuente informático.

En el contexto de la seguridad en la información personal, este es un derecho que se encuentra plasmado en nuestra Constitución Política de los Estados Unidos Mexicanos, el cual debe ser garantizado por el Estado, conforme a los artículos 6 y 16, párrafo segundo, como se muestra a continuación:

> *Artículo 6. El derecho a la información será garantizado por el Estado."*
>
> *Artículo 16, párrafo segundo. Toda persona tiene derecho a la protección de sus datos personales, al acceso, rectificación y cancelación de los mismos, así como a manifestar su oposición, en los términos que fije la ley, la cual establecerá los supuestos de excepción a los principios que rijan el tratamiento de datos, por razones de seguridad nacional, disposiciones de orden público, seguridad y salud públicas o para proteger los derechos de terceros*.[159]

En ese sentido, la seguridad de los datos y la información, son actualmente temas que emergen velozmente, ya que las nuevas formas de comunicación y tecnologías emergentes, han ampliado su espectro de afectación y protección, ya que el valor actual de los datos e información, es un activo que se mercantiliza tanto de forma material y virtual, así como de forma legal e ilegal.

Derivado de ello, la normativa nacional se ha visto impactada, pues las diferentes formas y variantes de cometer el delito, se combinan, matizándose en métodos más complejos para realizarlo. Así, el Código Penal Federal, en su

[159] Artículos 6-16, párrafo segundo, CPEUM, op.cit.

artículo 424 bis, fracción II, penaliza con prisión de tres a diez años y de dos mil a veinte mil días, a quien fabrique con fines de lucro un dispositivo o sistema, con el fin de desactivar los dispositivos electrónicos de protección de un programa de computación, de esta manera se busca que los delincuentes informáticos, no vulneren los sistemas de seguridad.

Como hemos visto con anterioridad, para poder ingresar a un equipo o sistema, primero hay que romper los sistemas de seguridad, de esta forma los conocidos como *Crackers*, en el ámbito de los delitos informáticos, son quienes rompen las protecciones y elementos de seguridad, haciendo uso de programas para quebrantar códigos, como los ataques de fuerza bruta creados con el fin de lanzar múltiples claves para poder ingresar al sistema, rompiendo su seguridad al enviarlas al azar, obteniendo con ello el código de acceso, de esta forma el acceso y ruptura del sistema de seguridad, que muchas veces tiene antivirus, *firewalls*, activación y desactivación de funciones de software, cifrados para acceder a un sistema, etc., como se muestra en el código de conducta propio del *hacker* y/o algunos *hackers* como FXMSP, se debe desactivar la seguridad, deshabilitar el software antivirus y el firewall existente.

Resultado de lo anterior, la venta y creación de *softwares* y/o programas para romper los sistemas de seguridad, es una de las tareas constantes de los delincuentes informáticos, ya que se considera una de las principales herramientas para el ingreso no autorizado a un sistema.

En ese sentido el Acceso ilícito a sistemas y equipos de informática, se tipifica de igual forma en el Código Penal Federal, como se puede ver en el siguiente cuadro:

ARTÍCULO DEL CÓDIGO PENAL FEDERAL	**CONDUCTA TÍPICA**	**PUNIBILIDAD**
Artículo 211 bis 1, primer párrafo.	"Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática protegidos por	"…de seis meses a dos años de prisión y de cien a trescientos días multa"

	algún mecanismo de seguridad…"	
Artículo 211 bis 1, segundo párrafo.	"Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática…"	"… de tres meses a un año de prisión y de cincuenta a ciento cincuenta días multa"
Artículo 211 bis 2, primer párrafo.	"Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática del Estado"	"… de uno a cuatro años de prisión y de doscientos a seiscientos días multa"
Artículo 211 bis 2, segundo párrafo.	"Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática del Estado…"	"…de seis meses a dos años de prisión y de cien a trescientos días multa"
Artículo 211 bis 2, tercer párrafo.	"A quien sin autorización conozca, obtenga, copie o utilice información contenida en cualquier sistema, equipo o medio de almacenamiento informáticos de seguridad pública…"	"…de cuatro a diez años de prisión y multa de quinientos a mil días de salario mínimo general vigente en el Distrito Federal." Sin embargo si "el responsable es o hubiera sido servidor público en una institución de seguridad pública", a "destitución e inhabilitación de cuatro a diez años para desempeñarse en otro empleo, puesto, cargo o comisión pública."
Artículo 211 bis 2, cuarto párrafo. "Las sanciones anteriores se duplicarán cuando la conducta obstruya, entorpezca, obstaculice, limite o imposibilite la procuración o impartición de justicia, o recaiga sobre los registros relacionados con un procedimiento penal resguardados por las autoridades competentes", párrafo cuarto del artículo en 211 bis 2 en comentó.		
Artículo 211 bis 3, primer párrafo.	"Al que estando autorizado para acceder a sistemas y equipos de informática del Estado, indebidamente modifique, destruya o provoque pérdida de información…"	"…de dos a ocho años de prisión y de trescientos a novecientos días multa."
Artículo 211 bis 3, segundo párrafo.	"Al que estando autorizado para acceder a sistemas y equipos de informática del Estado, indebidamente copie información…"	"… de uno a cuatro años de prisión y de ciento cincuenta a cuatrocientos cincuenta días multa."
Artículo 211 bis 3, tercer párrafo.	"A quien estando autorizado para acceder a sistemas, equipos o medios de almacenamiento informáticos en materia de seguridad pública, indebidamente obtenga, copie o utilice información que contengan…"	"…se le impondrá pena de cuatro a diez años de prisión y multa de quinientos a mil días de Salario mínimo general vigente en el Distrito Federal."

Artículo 211 bis 3, tercer párrafo. "Si el responsable es o hubiera sido servidor público en una institución de seguridad pública, se impondrá además, hasta una mitad más de la pena impuesta, destitución e inhabilitación por un plazo igual al de la pena resultante para desempeñarse en otro empleo, puesto, cargo o comisión pública."		
Artículo 211 bis 4, primer párrafo.	"Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática de las instituciones que integran el sistema financiero… "	"… se le impondrán de seis meses a cuatro años de prisión y de cien a seiscientos días multa."
Artículo 211 bis 4, segundo párrafo.	"Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática de las instituciones que integran el sistema financiero…"	"…le impondrán de tres meses a dos años de prisión y de cincuenta a trescientos días multa."
Artículo 211 bis 5, primer párrafo.	"Al que estando autorizado para acceder a sistemas y equipos de informática de las instituciones que integran el sistema financiero, indebidamente modifique, destruya o provoque pérdida de información que contengan…"	"… se le impondrán de seis meses a cuatro años de prisión y de cien a seiscientos días multa."
Artículo 211 bis 5, segundo párrafo.	"Al que estando autorizado para acceder a sistemas y equipos de informática de las instituciones que integran el sistema financiero[160], indebidamente copie información que contengan…"	"…se le impondrán de tres meses a dos años de prisión y de cincuenta a trescientos días multa."
Artículo 211 bis 5, tercer párrafo. "Las penas previstas en este artículo se incrementarán en una mitad cuando las conductas sean cometidas por funcionarios o empleados de las instituciones que integran el sistema financiero".		
Artículo 211 bis 7.- "Las penas previstas en este capítulo se aumentarán hasta en una mitad cuando la información obtenida se utilice en provecho propio o ajeno."		

Por su parte en el Libro Segundo, Título Quinto del mismo Código Penal Federal, denominado "Delitos en materia de comunicación y correspondencia",

[160] Cfr., Artículo 211 bis 6, CPF, "Para los efectos de los artículos 211 Bis 4 y 211 Bis 5 anteriores, se entiende por instituciones que integran el sistema financiero, las señaladas en el artículo 400 Bis de este Código", op.cit.
Cfr., Artículo 400 Bis, fracción I, CPF, "Se impondrá de cinco a quince años de prisión y de mil a cinco mil días multa al que, por sí o por interpósita persona realice cualquiera de las siguientes conductas: I. Adquiera, enajene, administre, custodie, posea, cambie, convierta, deposite, retire, dé o reciba por cualquier motivo, invierta, traspase, transporte o transfiera, dentro del territorio nacional, de éste hacia el extranjero o a la inversa, recursos, derechos o bienes de cualquier naturaleza, cuando tenga conocimiento de que proceden o representan el producto de una actividad ilícita, o…", op.cit.

Capítulo I, de nombre “Ataques a las vías de comunicación”, se norman dos artículos que nos muestran el hecho de interrumpir o interferir dolosamente y con fines de lucro las comunicaciones telegráficas, telefónicas o satelitales, descifrar o decodificar señales de telecomunicaciones distintas a las de satélite portadoras de programas, así como el recibir o distribuir una señal de satélite cifrada portadora de programas originalmente codificada, sin la autorización del distribuidor legal de la señal, señalando la interferencia de la comunicación, rompiendo los sistemas de seguridad, codificación y encriptación que han sido utilizadas en los procesos de transportación, envío y recepción de información, lo que conlleva a una toma no autorizada de la señal, y por consiguiente de sus datos e información contenida en la misma, artículos que a continuación se señalan:

ARTÍCULO DEL CÓDIGO PENAL FEDERAL	**CONDUCTA TÍPICA**	**PUNIBILIDAD**
Artículo 167, fracción VI.	“Al que dolosamente o con fines de lucro, interrumpa o interfiera las comunicaciones, alámbricas, inalámbricas o de fibra óptica, sean telegráficas, telefónicas o satelitales, por medio de las cuales se transfieran señales de audio, de video o de datos…”	“Se impondrán de uno a cinco años de prisión y de cien a diez mil días multa….
Artículo 168 bis, fracción I.	“I. Descifre o decodifique señales de telecomunicaciones distintas a las de satélite portadoras de programas;”	“se impondrán de seis meses a dos años de prisión y de trescientos a tres mil días multa, a quien sin derecho…”
Artículo 168 bis, fracción II.	“II. Transmita la propiedad, uso o goce de aparatos, instrumentos o información que permitan descifrar o decodificar señales de telecomunicaciones distintas a las de satélite portadoras de programas…”	
Artículo 168 bis, fracción III.	“III. Reciba o distribuya una señal de satélite cifrada portadora de programas originalmente codificada, sin la autorización del distribuidor legal de la señal…”	

Tomando en cuenta lo anterior, y continuando con el objetivo de descifrar sin autorización, las “señales de satélite cifradas portadora de programas”, el artículo 426 fracciones I, II, III y IV, del mismo Código Penal Federal, delimita las conductas que permiten la afectación a las “señales de satélite cifradas portadora de programas”, como se muestra en el siguiente cuadro:

ARTÍCULO DEL CÓDIGO PENAL FEDERAL	**CONDUCTA TÍPICA**	**PUNIBILIDAD**
Artículo 426, fracción I.	“A quien fabrique, modifique, importe, distribuya, venda o arriende un dispositivo o sistema para descifrar una señal de satélite cifrada, portadora de programas, sin autorización del distribuidor legítimo de dicha señal…”	“Se impondrá prisión de seis meses a cuatro años y de trescientos a tres mil días multa, en los casos siguientes”
Artículo 426, fracción II.	“A quien realice con fines de lucro cualquier acto con la finalidad de descifrar una señal de satélite cifrada, portadora de programas, sin autorización del distribuidor legítimo de dicha señal…”	
Artículo 426, fracción III	“A quien fabrique o distribuya equipo destinado a la recepción de una señal de cable encriptada portadora de programas, sin autorización del distribuidor legítimo de dicha señal…”	
Artículo 426, fracción IV	“A quien reciba o asista a otro a recibir una señal de cable encriptada portadora de programas sin la autorización del distribuidor legítimo de dicha señal.”	

Cabe mencionar que el poder decodificar las señales tanto satelitales como no satelitales, es una práctica de los delincuentes informáticos en las redes y todos aquellos sistemas de envió, recepción y distribución de información y datos, como se muestra en la siguiente nota, tomada del diario digital “El Mundo”, “*Pedro, el hacker gallego que arrasa en Estados Unidos enseñando a*

secuestrar televisiones”[161], este hombre solo necesita para su ataque “*un drone que se puede comprar en cualquier tienda, un ordenador poco más grande que un paquete de tabaco, una batería portátil, una radio acoplada y una antena que ensambla juntos con ayuda de una brida delante de nosotros*”, refiere Daniel Ollero, citando de igual forma a Pedro el hacker "Con esto ya podríamos emitir nuestro propio canal de televisión secuestrando el canal que la otra persona estaba viendo”, conforme a lo anterior refiere también.

> *…otra de las ventajas que presenta este ataque es que se puede llevar a cabo tanto de forma remota, como utilizando un drone o una antena direccional desde un coche y minimizando así la posibilidad de ser descubiertos, como conectados físicamente a través de un cable”, “para atacar a una persona en concreto o a un edificio asegura que lo más sencillo sería "conectar nuestro aparato al centro de distribución de la antena en lugar de un ataque por aire. De este modo, lo que hacemos es apagar la antena original y nuestro aparato con una señal envenenada funcionaría como la antena del edificio…*[162]

Por otro lado el “revelar secretos” es un delito que converge con el robo de datos, pues muchas veces se accede a información personal o de una empresa con el propósito de hacerla pública, afectando tanto a la persona física como moral, ya que en la persona física, puede dañar su imagen al grado de atentar contra su intimidad, en el caso de las empresas al revelar secretos industriales, considerados en base al artículo 163 de la Ley Federal de Protección a la Propiedad Industrial, como “confidenciales y que permite ventaja competitiva”, ya que estos pueden estar contenidos en documentos, medios electrónico o magnéticos, discos ópticos, microfilmes, películas o en cualquier otro medio conocido o por conocerse, se puede obtener la información de forma lícita o ilícita para después vulnerar (darla a conocer sin autorización), afectando fuertemente a la empresa, lo que conlleva a impactar de forma negativa en su producción, imagen, confiabilidad, economía, etc.

Aunado a lo anterior este delito y sus conductas, se encuentra tipificado en el Código Penal Federal, apartado de nombre “Revelación de secretos y acceso

[161] Ollero, Daniel, *“*Pedro, el hacker gallego que arrasa en Estados Unidos enseñando a secuestrar televisiones. Su método es capaz de secuestrar una sola tele o la señal de toda la ciudad. La tecnología con la que lleva a cabo el ataque permite poner tu televisión a su servicio para ganar dinero o espiarte”, España, *https://www.elmundo.es/tecnologia/2019/08/28/5d6578a2fc6c83f25a8b4586.html,* de 19 de octubre de 2021, 08:33 p.m.

[162] Ollero, Daniel, op.cit.

ilícito a sistemas y equipos de informática"[163], en los artículos 210 "…revele algún secreto o comunicación reservada que conoce o ha recibido con motivo de su empleo, cargo o puesto…", 211 "…cuando el secreto revelado o publicado sea de carácter industrial…" y 211 Bis "revele, divulgue o utilice indebidamente o en perjuicio de otro, información o imágenes obtenidas en una intervención de comunicación privada…", relacionándose con los considerados como delitos en la Ley Federal de Protección a la Propiedad Industrial, descritos en el artículo 402, fracciones III (Divulgar a un tercero un secreto industrial), IV (Apoderarse de un secreto industrial) , V (Usar la información contenida en un secreto industrial) y VI (Apropiarse, adquirir, usar o divulgar indebidamente un secreto industrial).

La Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, en su artículo 163, fracción III, señala dentro de las conductas que serán causa de sanción, aquellas que atenten o pongan en riesgo total o parcialmente los datos, siendo responsable de su custodia, así "*Usar, sustraer, divulgar, ocultar, alterar, mutilar, destruir o inutilizar, total o parcialmente y de manera indebida datos personales, que se encuentren bajo su custodia o a los cuales tengan acceso o conocimiento con motivo de su empleo, cargo o comisión*", en ese sentido dentro de la responsabilidad que se adquiere al encontrarse obligado con motivo de empleo, cargo o comisión, ya que se tiene acceso y conocimiento a la información, se corre el riesgo de atentar contra la misma por delincuentes que utilicen su posición dentro las instituciones.

Una vulneración de seguridad es cualquier incidente que dé lugar al acceso no autorizado a datos, aplicaciones, programas, redes o dispositivos informáticos,

[163] Cfr., Artículo 210, CPF, "Se impondrán de treinta a doscientas jornadas de trabajo en favor de la comunidad, al que sin justa causa, con perjuicio de alguien y sin consentimiento del que pueda resultar perjudicado, revele algún secreto o comunicación reservada que conoce o ha recibido con motivo de su empleo, cargo o puesto", op.cit.
Cfr., Artículo 211, CPF, "La sanción será de uno a cinco años, multa de cincuenta a quinientos pesos y suspensión de profesión en su caso, de dos meses a un año, cuando la revelación punible sea hecha por persona que presta servicios profesionales o técnicos o por funcionario o empleado público o cuando el secreto revelado o publicado sea de carácter industrial", op.cit.
Cfr., Artículo 211 Bis, CPF, "A quien revele, divulgue o utilice indebidamente o en perjuicio de otro, información o imágenes obtenidas en una intervención de comunicación privada, se le aplicarán sanciones de seis a doce años de prisión y de trescientos a seiscientos días multa", op.cit.

que a su vez da como consecuencia el acceso no autorizado a la información. Por lo general, esto ocurre cuando un intruso logra burlar los mecanismos y/o sistemas de seguridad.

Las vulneraciones de seguridad, como incidente que permite el acceso no autorizado a datos o información, por medio de un intruso que burla los sistemas de seguridad y/o del o los responsables del tratamiento de datos, en cualquier fase del proceso, dan como resultado la vulneración de los mismos, aunado a todos los efectos consecuentes, resultado del uso posterior que se les pueden dar, así como el riesgo o afectación al dueño o poseedor de los datos, como señala la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados en su artículo 38, fracciones I, II, III y IV:

> *Además de las que señalen las leyes respectivas y la normatividad aplicable, se considerarán como vulneraciones de seguridad, en cualquier fase del tratamiento de datos, al menos, las siguientes:*
>
> *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*[164]*.*

Por su parte, en relación a quien se encuentra autorizado para tratar datos, la Ley Federal de Protección de Datos Personales en Posesión de los Particulares en su artículo 67, señala que, “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”.

En relación al responsable, continuando con la ley en comentó, la misma determina en su artículo 63 fracción XI, “Constituyen infracciones a esta Ley, las siguientes conductas llevadas a cabo por el responsable”: “XI. Vulnerar la seguridad de bases de datos, locales, programas o equipos, cuando resulte

[164] Artículo 63, fracciones I, II, III y IV, LGPDPPSO, op.cit.

imputable al responsable", mientras que el artículo 64, fracciones III y IV, de la Ley en cuestión, señala las sanciones relacionadas con el supuesto anterior, "Las infracciones a la presente Ley serán sancionadas por el Instituto con:" III. "Multa de 200 a 320,000 días de salario mínimo vigente en el Distrito Federal, en los casos previstos en las fracciones VIII a XVIII del artículo anterior, y IV. "En caso de que de manera reiterada persistan las infracciones citadas en los incisos anteriores, se impondrá una multa adicional que irá de 100 a 320,000 días de salario mínimo vigente en el Distrito Federal. En tratándose de infracciones cometidas en el tratamiento de datos sensibles, las sanciones podrán incrementarse hasta por dos veces, los montos establecidos". Cabe señalar que con base en el artículo 66, del mismo ordenamiento, "*las sanciones que se señalan en este Capítulo se impondrán sin perjuicio de la responsabilidad civil o penal que resulte*".

Es importante señalar, que en el Código Penal del Estado de Sinaloa, artículo 217, fracciones I y II, se norma de forma muy adecuada al contexto actual, el denominado "Delito Informático", en el entendido de cometer de forma dolosa, el uso, ingresó a una base de datos, sistema de computadores o red de computadoras o cualquier parte de la misma, con el objetivo de afectar al bien jurídico de la seguridad, en los sistemas, redes y base de datos, siendo un delito que afecta varios bienes jurídicos, como señala Silvia Guadalupe Palazuelos en la Revista Jurídica del Poder Judicial[165] "aequitas", en su Número 32 de abril del 98, *"… cabe destacar que los delitos informáticos van más allá de una simple violación a los derechos patrimoniales de las víctimas, ya que debido a las diferentes formas de comisión de éstos, no solamente se lesionan esos derechos, sino otros como el derecho a la intimidad*", lo que conlleva a otros delitos, con el fin de defraudar, obtener dinero, bienes o información, además de atentar contra el soporte lógico o programa de computadora o los

[165] Palazuelos, Silvia, "Delitos informáticos. Propuesta para el Tratamiento de la Problemática en México", Aequitas, Revista Jurídica del Poder Judicial del Estado de Sinaloa, No. 32, 98, p, 98, *https://www.stj-sin.gob.mx/assets/files/publicaciones/aequitas32.pdf,* de 26 de octubre de 2021, 07:33 p.m.

datos contenidos en la misma, en la base, sistema o red, impactando la protección al bien jurídico de los datos e información, de la siguiente forma:

> *Código Penal del Estado de Sinaloa, artículo 217. Comete delito informático, la persona que dolosamente y sin derecho:*
>
> *I. Use o entre a una base de datos, sistema de computadores o red de computadoras o a cualquier parte de la misma, con el propósito de diseñar, ejecutar o alterar un esquema o artificio, con el fin de defraudar, obtener dinero, bienes o información; o*
>
> *II. Intercepte, interfiera, reciba, use, altere, dañe o destruya un soporte lógico o programa de computadora o los datos contenidos en la misma, en la base, sistema o red.*
>
> *Al responsable de delito informático se le impondrá una pena de seis meses a dos años de prisión y de noventa a trescientos días multa*[166]*.*

No omito mencionar, que considero, debe ser revisada la penalidad, ya que dependiendo del impacto y daño causado al o los bienes jurídicos, debe ser ampliada esta, ya que se ha demostrado que dentro del robo de datos e información, el impacto puede exponenciar como resultado del uso que se dé a lo tomado y apoderado, con ánimo de lucro y sin autorización, como refiere el artículo en cuestión "dolosamente y sin derecho."

Algunos otros ordenamientos que se relacionan con la regulación de la seguridad de datos e información, así como con los sistemas, programas, equipos, *hardwares, softwares*, etc., que permiten su almacenamiento, creación, modificación, transportación, etc., son los que se exponen en el siguiente cuadro:

ORDENAMIENTO	**CONDUCTA TÍPICA**	**CONSECUENCIA O PUNIBILIDAD**
Código Penal para el Distrito Federal, Artículo 231, fracción 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 e indebidamente realice operaciones, transferencias o movimientos de dinero o valores, independientemente de	"Se impondrán las penas previstas en el artículo anterior, a quien… " (Esto es el delito de fraude, artículo 230).

[166] Artículo 217, CPES, op.cit.

	que los recursos no salgan de la Institución”	
Ley de Instituciones de Crédito, Artículo 112 Quáter, fracciones I y II.	“I. Acceda a los equipos o medios electrónicos, ópticos o de cualquier otra tecnología del sistema bancario mexicano, para obtener recursos económicos, información confidencial o reservada, o” “II. Altere o modifique el mecanismo de funcionamiento de los equipos o medios electrónicos, ópticos o de cualquier otra tecnología para la disposición de efectivo de los usuarios del sistema bancario mexicano, para obtener recursos económicos, información confidencial o reservada.”	“Se sancionará con prisión de tres a nueve años y de treinta mil a trescientos mil días multa, al que sin causa legítima o sin consentimiento de quien esté facultado para ello:”

Cabe señalar que la Ley 1273 de 2009, en su artículo 269I, con la que se adiciona el Código Penal Colombiano, nos refiere el denominado “Hurto por medios informáticos y semejantes”, en el cual nos habla de la violación de las medidas de seguridad informáticas, lo que ha sido señalado como primera parte de lo que será un ingreso no autorizado o intrusión, para después realizar el hurto.

> *“Hurto por medios informáticos y semejantes. El que, superando medidas de seguridad informáticas, realice la conducta señalada en el artículo 239[167] manipulando un sistema informático, una red de sistema electrónico, telemático u otro medio semejante, o suplantando a un usuario ante los sistemas de autenticación y de autorización establecidos, incurrirá en las penas señaladas en el artículo 240[168] de este Código[169].”*

[167] Cfr., Artículo 239, Código Penal Colombiano, Ley 599 de 2000, “Hurto. El que se apodere de una cosa mueble ajena, con el propósito de obtener provecho para sí o para otro, incurrirá en prisión de dos (2) a seis (6) años. La pena será de prisión de uno (1) a dos (2) años cuando la cuantía no exceda de diez (10) salarios mínimos legales mensuales vigentes”.

[168] Cfr., Artículo 240, Código Penal Colombiano, Ley 599 de 2000 “Hurto calificado. La pena será prisión de tres (3) a ocho (8) años, si el hurto se cometiere: 1. Con violencia sobre las cosas; 2. Colocando a la víctima en condiciones de indefensión o inferioridad o aprovechándose de tales condiciones; 3. Mediante penetración o permanencia arbitraria, engañosa o clandestina en lugar habitado o en sus dependencias inmediatas, aunque allí no se encuentren sus moradores; 4. Con escalamiento, o con llave sustraída o falsa, ganzúa o cualquier otro instrumento similar, o violando o superando electrónicas u otras semejantes. La pena será prisión de cuatro (4) a diez (10) años cuando se cometiere con violencia sobre las personas. Las mismas penas se aplicarán cuando la violencia tenga lugar inmediatamente después del apoderamiento de la cosa y haya sido empleada por el autor o partícipe con el fin de asegurar su producto o la impunidad”, op.cit.

[169] Artículo 269I, Código Penal Colombiano, Ley 599 de 2000, op.cit.

Al adecuar las figuras jurídico penales tradicionales como el robo, a las nuevas modalidades delictivas, y en el tema que nos ocupa, robo de datos e información mediante la utilización de sistemas y equipos informáticos, puntualmente nos señala el maestro Julio Téllez Valdés lo siguiente.

> *…si se insiste en adecuar las figuras jurídico-penales tradicionales como el robo a esta nueva modalidad delictiva, se tendrán entonces que modificar dos conceptos: el de "apoderamiento" en el que se considere no sólo el desposeimiento del bien, sino también la disminución de su valor; y el de "bien mueble" en el que se incluyan bienes intangibles como la información que sí per se es susceptible de apropiación, también per se, debe ser susceptible de protección jurídica*…[170].

En ese sentido, exponemos las conductas que en algunos de los artículos mencionados con anterioridad, pueden ser relacionadas con el robo de datos e información, partiendo de Código Penal Federal[171] y el delito de robo:

ORDENAMIENTO	ARTÍCULO	CONDUCTA
Código Penal Federal	367. "Comete el delito de robo: el que se apodera de una cosa ajena mueble,…"	Apoderar-"… sin derecho y sin consentimiento de la persona que puede disponer de ella con arreglo a la ley."
Código Penal Federal	Artículo 211 bis 2, tercer párrafo. "A quien sin autorización conozca, obtenga, copie o utilice";	Conozca, obtenga, copie o utilice- Sin autorización, "…información contenida en cualquier sistema, equipo o medio de almacenamiento informáticos de seguridad pública…"
Código Penal Federal	Artículo 211 bis 3, tercer párrafo. "A quien estando autorizado para acceder a sistemas, equipos o medios de almacenamiento informáticos en materia de seguridad pública, indebidamente…"	Obtener- indebidamente, "…obtenga, copie o utilice información que contengan…"
Código Penal Federal	Artículo 168 bis, fracción III. "Reciba o distribuya una señal de satélite cifrada portadora de programas originalmente codificada, sin la autorización	Recibir o distribuir- sin autorización del distribuidor legal, "Reciba o distribuya una señal de satélite cifrada

[170] Téllez, Julio, "Los delitos informáticos: Situación en México", p.468, file:///C:/Users/antonio/Downloads/Dialnet-LosDelitosInformaticos-248768.pdf, de 26 de octubre de 2021, 09:46 p.m.
[171] Artículo 367, 211 bis 2, tercer párrafo, 211 bis 3, tercer párrafo, 168 bis, fracción III, 167, fracción VI, CPF, op.cit.

	del distribuidor legal de la señal…";	portadora de programas originalmente codificada…"
Código Penal Federal	Artículo 167, fracción VI. "Al que dolosamente o con fines de lucro,"	Interrumpir e interferir, dolosamente o con fines de lucro, "…interrumpa o interfiera las comunicaciones, alámbricas, inalámbricas o de fibra óptica, sean telegráficas, telefónicas o satelitales, por medio de las cuales se transfieran señales de audio, de video o de datos…"
Delitos descritos en la Ley Federal de Protección a la Propiedad Industrial	Artículo 402, fracciones III, IV, V y VI. Artículo 402.- Son delitos:	III – Divulgar, a un tercero, un secreto industrial. IV – Apoderarse, de un secreto industrial. V – Usar, la información contenida en un secreto industrial. VI - Apropiarse, adquirir, usar o divulgar, indebidamente un secreto industrial.
Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados	Artículo 38, fracción II "Además de las que señalen las leyes respectivas y la normatividad aplicable, se considerarán como vulneraciones de seguridad, en cualquier fase del tratamiento de datos, al menos, las siguientes:"	Conductas que serán causa de sanción, aquellas que atenten o pongan en riesgo total o parcialmente los datos, siendo responsable de su custodia: "II. El robo, extravío o copia no autorizada;"
Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados	Artículo 163, fracción III, "… total o parcialmente y de manera indebida datos personales, que se encuentren bajo su custodia o a los cuales tengan acceso o conocimiento con motivo de su empleo, cargo o comisión".	Conductas que serán causa de sanción y que atenten o pongan en riesgo total o parcialmente los datos De manera indebida, "… Usar, sustraer, divulgar, ocultar, alterar, mutilar, destruir o inutilizar…"
Código Penal del Estado de Sinaloa	Artículo 217. Fracción I, "Comete delito informático, la persona que dolosamente y sin derecho:" "I., con el fin de defraudar, obtener dinero, bienes o información"	Usar o entrar, Dolosamente, con el fin de defraudar, obtener dinero, bienes o información, "Use o entre a una base de datos, sistema de computadores o red de computadoras o a cualquier parte de la misma, con el propósito de diseñar, ejecutar o alterar un esquema o artificio…"

Ley de Instituciones de Crédito	Artículo 112 Quáter, fracciones I y II. "…al que sin causa legítima o sin consentimiento de quien esté facultado para ello…"	Sin causa legítima y sin consentimiento: Acceder o modificar. I "Acceda a los equipos o medios electrónicos, ópticos o de cualquier otra tecnología del sistema bancario mexicano, para obtener recursos económicos, información confidencial o reservada,) Alterar, obtener. II "Altere o modifique el mecanismo de funcionamiento de los equipos o medios electrónicos, ópticos o de cualquier otra tecnología para la disposición de efectivo de los usuarios del sistema bancario mexicano, para obtener recursos económicos, información confidencial o reservada.

II. Diferencia entre técnica (modo de operar) y delito informático

Distinguir la técnica de operar del delincuente informático, es de suma importancia, ya que las formas de ingresar y obtener, alterar, dañar, modificar, etc., los datos y la información, aunque son muy parecidas, tienen variantes, dependiendo del objetivo.

La palabra técnica, nos conceptualiza Ferrater Mora[172], citado por Juan Manuel Silva, "*es toda serie de reglas por medio de las cuales se consigue algo*", por su parte Nicola Abbagnano[173], citado una vez más por Juan Manuel, nos dice que debe entenderse por el término que nos interesa, "comprende todo conjunto de reglas aptas para dirigir eficazmente una actividad cualquiera", si tomamos como base el último concepto podemos adecuarlo a los delitos informáticos, partiendo del hecho de utilizar reglas para dirigir un ataque, acceso no autorizado, intrusión o simplemente obtener la información necesaria

[172] Silva, Juan, "Humanismo, Técnica y Tecnología", Revista contaduría y administración, núm. 198, 2000, pág. 14, *http://www.ejournal.unam.mx/rca/198/RCA19803.pdf,* de 27 de octubre de 2021, 09:39 p.m.
[173] Silva, Juan, op. cit., p. 16.

para poder ingresar de forma más eficaz, estudiando al o los objetivos, ya sea sistema, equipo, una señal o red, etc.

De esta manera al aplicar diferentes técnicas, el delincuente informático puede atacar a su objetivo de forma eficaz, siendo más sofisticado, como muestra el suplemento especial de ERREIUS, “Cibercrimen y delitos informáticos”, dentro del cual nos señalan.

> … *en la actualidad, los delitos informáticos pueden clasificarse en dos grandes grupos: aquellos que requieren de una sofisticación técnica para su comisión, generalmente basado en la elaboración de programas maliciosos desarrollados por hackers que buscan vulnerar los dispositivos o redes, generalmente con fines económicos y aquellos delitos que adquieren una nueva vida en la nube y son intermediados por servicios y aplicaciones web como las amenazas, los fraudes, el grooming…*[174]

Una de las principales técnicas para recabar información que es utilizada por los delincuentes informáticos, es la denominada “ingeniería social”, de la cual David Berenger nos refiere, que se puede definir como, “*el conjunto de técnicas o estrategias utilizadas de forma premeditada por un usuario para obtener algún tipo de ventaja respecto a otros*”[175], la cual se organiza por métodos, como dice David Berenguer, y que son los siguientes:

> Una fase de acercamiento para ganarse la confianza del usuario, haciéndose pasar por un integrante de la administración, de la compañía, un cliente, proveedor, etc.; una fase de alerta, para desestabilizar al usuario y observar la velocidad de su respuesta. Por ejemplo, este podría ser un pretexto de seguridad o una situación de emergencia; una distracción, es decir, una frase o una situación que tranquiliza al usuario y evita que se concentre en la alerta. Podría ser un agradecimiento que indique que todo ha vuelto a la normalidad,

[174] Parada, Ricardo, “” Ciberbercrimen y delitos informáticos. Los nuevos tipos penales en la era de internet”, Erreius, 1a ed, Argentina, 2018, p. 11, *https://www.errepar.com/resources/descargacontenido/CIBERCRIMEN.PDF,* de 28 de octubre de 2021, 10:15 p.m.

[175] Serrato, David, “Estudio de metodologías de Ingeniería Social”, Master Universitario en Seguridad de las Tecnologías de la Información y de las Comunicaciones, Universidad Oberta de Catalunya, p.4, *http://openaccess.uoc.edu/webapps/o2/bitstream/10609/81273/6/dbs14TFM0618memoria.pdf,* de 02 de noviembre de 2021, 09:23 p.m.

una frase hecha o, en caso de que sea mediante correo electrónico o de una página web, la redirección a la página de la compañía[176].

La ingeniería social, busca el obtener información o que se realicen acciones que ponen en riesgo la seguridad del equipo o sistema, por medio de la manipulación de personas, algunas de las técnicas que forman parte de la ingeniería social son[177]:

- *Pretextin* (pretextando). El atacante crea un escenario creíble para lograr que su víctima le brinde acceso a su ordenador o también a su espacio de trabajo con el fin de robar su información o instalarle un *malware*, como por ejemplo con la excusa de que se le termino la batería y no tiene cargador, por lo que al solicitar un equipo para revisar un correo electrónico, descarga el *software* en el equipo.

- *Tailgaiting* (chupar rueda). El aprovechamiento de la solidaridad o inconsciencia de un empleado, un atacante puede evadir controles de acceso físico como puertas electrónicas e ingresar a una organización sin autorización.

- *Dumpster diving* (contenedor de basura). Cuando se desecha la documentación de manera insegura, por lo que los atacantes revisan la basura para obtener información, como claves de acceso, códigos o simplemente información confidencial o que sirve para obtener más información.

- *Shoulder surfing* (Surf de hombro). Cuando se mira por encima del hombro de un usuario descuidado mientras ingresa el patrón de desbloqueo, PIN o alguna otra contraseña, en sus dispositivos.

- *Baiting* (cebo). Técnica que consiste en colocar memorias externas con malware instalado en lugares donde personas escogidas específicamente, puedan encontrarlo y al insertarlo infecten el equipo o sistema.

[176] Berenguer, David, op. cit., p. 4.
[177] Grupo Atlas de Seguridad Integral, “Técnicas de Ingeniería Social más usadas en ataques informáticos”, YouTube, Video, 2018, *https://www.youtube.com/watch?v=UW73wlzfpoI&ab_channel=iSecuritySummitCOL*, de 02 de noviembre de 2021, 10:35 p.m.

- *Phising* (Suplantación de identidad). Consiste en engañar a un grupo masivo de personas mediante correos electrónicos, páginas web, perfiles sociales o mensajes de texto falsos, con el fin de robar información.

- *Vishing*. Llamadas telefónicas mediante las que se busca engañar a la víctima, suplantando a compañías de servicios, de gobierno o a otra entidad, para que se revele información privada, como en el caso de las llamadas desde un supuesto banco para obtener información que permita accesar a la cuenta.

- Redes sociales. Los perfiles sociales revelan grandes cantidades de información de la víctima como direcciones de correo, números de teléfono hasta aspectos personales y profesionales que se encuentran al alcance de cualquier persona, así quienes utilizan contraseñas a partir de fechas de nacimiento, aniversarios, lugares favoritos, o preferencias, proporcionan información importante que después será utilizada por el atacante.

Atendiendo al concepto de delito, el "Diccionario Jurídico Mexicano", nos dice lo siguiente "*en el derecho penal, acción u omisión ilícita y culpable expresamente descrita por la ley bajo la amenaza de una pena o sanción criminal*"[178], en ese sentido se entiende por acción u omisión ilícita y culpable descrita por la ley, por su parte el maestro Julio Téllez[179] nos refiere que los delitos informáticos, en su concepto atípico, son "*actitudes ilícitas que tienen a las computadoras como instrumento o fin*", mientras que en el concepto típico son "*conductas típicas, antijurídicas y culpables que tiene a las computadoras como instrumento o fin*", de esta manera en ambos conceptos, tanto en el típico como en el atípico, se denota una acción que se relaciona con las "computadoras".

Atendiendo a lo anterior, su servidor añadiría con fines educativos y con mucho respeto, "sistemas, redes, señales, aparatos electrónicos (como los inteligentes), programas y páginas electrónicas, así como todo aquel tipo,

[178] Soberanes, José Luis, op.cit., p. 868.
[179] Téllez, Julio, op. cit., p. 188.

presente y futuro, de tecnología que permite y permitirá cualquier forma de trabajo relacionada con los datos e información", ya que las tecnologías emergentes posibilitan formas constantemente nuevas de transmisión, recepción, almacenamiento, procesamiento, etc., de los datos e información.

Al ser modificado el Código Penal Argentino, por medio de la Ley 26.388, se incorpora como inciso 16 del artículo 173, "cualquier técnica de manipulación informática", lo que se entiende al definir, Faraldo Cabana citado por Ricardo Posada Mayo, la acción manipuladora informática del sujeto activo como:

> *… la introducción, alteración, borrado o supresión indebidos de los datos informático, especialmente datos de identidad, y la interferencia indebida en el funcionamiento de un programa o sistema informático. Por tanto, se incluyen tanto la introducción de datos falsos como la introducción indebida, por no autorizada, de datos reales, auténticos en el sistema, pasando por la manipulación de los ya contenidos en cualquiera de las fases del proceso o tratamiento informático, así como las interferencias que afectan al propio sistema o programa…*[180]

Conforme a lo anterior, se amplía la protección al "normal funcionamiento de un sistema y transmisión de datos", como se muestra en el artículo e inciso en cita, de la siguiente manera, "*El que defraudare a otro mediante cualquier técnica de manipulación informática que altere el normal funcionamiento de un sistema informático o la transmisión de datos*"[181].

Partiendo de lo anterior las diferentes técnicas empleadas por los delincuentes informáticos para lograr su objetivo, deben ser tipificadas y plasmadas en la legislación nacional, de tal manera que la acción u omisión ilícita y culpable, esto es, tomando con mucho respeto como base el concepto típico de los delitos informáticos del maestro Julio Téllez, podemos ampliarlo a "*las conductas típicas, antijurídicas y culpables que tiene a las computadoras, sistemas, redes, señales, aparatos electrónicos (como los inteligentes), programas y páginas electrónicas, así como todo aquel tipo, presente y futuro,*

[180] Posada, Ricardo, "El Delito de Transferencia no Consentida de Activos", Universidad de los Andes, 2012, p. 227, *https://derechoytics.uniandes.edu.co/components/com_revista/archivos/derechoytics/ytics120.pdf*, de 03 de noviembre de 2021, 06:36 p.m.
[181] Ley 26.388, se incorpora como inciso 16 del artículo 173, *https://www.oas.org/juridico/PDFs/arg_ley26388.pdf*, de 07 de febrero de 2022, 07:10 p.m.

de tecnología, utilizada como instrumento o fin", sean sancionadas por la Ley Penal, logrando un amplio espectro de protección al bien jurídico de los datos e información, y con ello considerar estas técnicas como delitos.

III. Cómo analizar el robo de datos desde la normativa actual

El robo de datos e información, se relaciona con diferentes conductas delictivas descritas y tipificadas en nuestro ordenamiento jurídico mexicano, en ese sentido, es importante tomar como base nuestra Carta Magna, las leyes federales y los tratados internacionales.

La Constitución Política de los Estados Unidos Mexicanos, describe la jerarquía de leyes existente en nuestro país, formando parte de Ley Suprema los tratados internacionales, como señala el artículo 133:[182]

> *Esta Constitución, las leyes del Congreso de la Unión que emanen de ella y todos los tratados que estén de acuerdo con la misma, celebrados y que se celebren por el Presidente de la República, con aprobación del Senado, serán la Ley Suprema de toda la Unión.*
>
> *Los jueces de cada entidad federativa se arreglarán a dicha Constitución, leyes y tratados, a pesar de las disposiciones en contrario que pueda haber en las Constituciones o leyes de las entidades federativas.*

No omito mencionar la conveniencia e importancia, de tomar muy en cuenta el "Convenio sobre la Ciberdelincuencia del Consejo de Europa" o Convenio de Budapest, en el sentido de ampliar el análisis y estudio de los delitos informáticos y su relación con otros delitos, así como de una posible adopción, con miras a establecer categorías de delitos y/o conductas delictivas, como los descritos en dicho convenio: 1. Delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos (art 2. acceso ilícito, art 3. Interceptación ilícita, art 4. Ataques a la integridad de los datos, art 5. Ataques a la integridad del sistema, art 6. Abuso de los dispositivos); 2. Delitos informáticos. Cometidos mediante el uso de las tecnologías de la información y las telecomunicaciones (art 7. Falsificación informática, art 8. Fraude

[182] Artículo 133, CPEUM, op.cit.

informático); 3. Delitos relacionados con el contenido (art 9. Delitos relacionados con la pornografía infantil); 4. Delitos relacionados con infracciones de la propiedad intelectual y de los derechos afines (derechos de autor).

Por otro lado Griselda Amuchategui[183], nos dice que la conducta, "*es un comportamiento humano voluntario (a veces una conducta humana involuntaria puede tener, ante el derecho penal, consecuencias como son la responsabilidad culposa o preterintencional), activo (acción o hacer positivo) o negativo (inactividad o no hacer), que produce un resultado*", mientras el maestro Fernando Castellanos[184] nos dice que "*la conducta es el comportamiento humano voluntario, positivo o negativo, encaminado a un propósito*".

El delito como conducta contraria a derecho, se conceptualiza en el Diccionario Jurídico Mexicano, de la siguiente forma, "*en el derecho penal, acción u omisión ilícita y culpable expresamente descrita por la ley bajo la amenaza de una pena o sanción criminal*[185]", o de igual manera es una conducta o hecho típico, antijurídico, culpable y punible, así la conducta o hecho típico nos conduce a los conceptos de tipicidad y tipo, a lo que el maestro Manuel Vidaurri Aréchiga[186] nos dice, *"entendemos por tipo la descripción que el legislador plasmó en la ley penal acerca de un determinado supuesto de hecho. Tipicidad es la adecuación de un hecho cometido a la descripción que de ese hecho se formula en el código penal"*.

En la página de Justia México[187], nos señalan que conductas, relacionadas con los delitos informáticos, son equiparadas al robo de acuerdo con la legislación penal, de la siguiente forma:

[183] Amuchategui, Griselda, op.cit p. 55.
[184] Castellanos, Fernando, Lineamientos Elementales del Derecho Penal (Parte General), México, 11ª ed. 1977, p. 149.
[185] Soberanes, José Luis, op. cit., p. 868.
[186] Vidaurri Aréchiga, Manuel, Teoría General del Delito, México. Oxford, 1ª ed. 2013, p. 65.
[187] Justia México, "Delitos informáticos, Preguntas y Respuestas Sobre Delitos Informáticos", *https://mexico.justia.com/derecho-penal/delitos-informaticos/preguntas-y-respuestas-sobre-delitos-informaticos/#q4,* de 08 de noviembre de 2021, 08:22 p.m.

…se equipara al robo el apoderamiento material o por medios electrónicos, de documentos que contengan datos de computadoras o el aprovechamiento o utilización de esos datos, sin derecho y sin consentimiento de la persona que legalmente pueda disponer de los mismos…

…también se equipara al robo el apoderamiento o uso indebido de tarjetas de crédito o débito expedidas por Instituciones Bancarias o de cualquier otra naturaleza o de títulos de crédito o documentos auténticos que sirvan para el pago de bienes o servicios o para obtener dinero efectivo sin el consentimiento de quien tenga derecho a disponer de tal instrumento...

Una de las conductas que atentan contra los bienes jurídicos de los datos e información, y que es utilizada constantemente en los delitos informáticos es la denominada interferencia de datos informáticos (en la que conviven a su vez otras conductas), de la cual se hace referencia dentro del "Estudio exhaustivo sobre el delito cibernético" de la Oficina de las Naciones Unidas contra la Droga y el Delito[188], como "*En el caso de interferir datos informáticos, la conducta que constituye la interferencia va desde dañar hasta borrar, alterar, suprimir, agregar o transmitir datos*".

Las conductas descritas en el siguiente cuadro, utilizado con anterioridad y ampliado, pueden ser relacionadas con el robo de datos e información, partiendo del Código Penal Federal y el delito de robo[189] (artículo 367 CPF), así como en los artículos, leyes y códigos, enunciados a continuación:

ORDENAMIENTO	ARTÍCULO	CONDUCTA ORDENAMIENTO	CONDUCTA TÍPICA
Código Penal Federal	367. "Comete el delito de robo: el que se apodera de una cosa ajena mueble,…"	Apoderar-"… sin derecho y sin consentimiento de la persona que puede disponer de ella con arreglo a la ley."	"En el delito de robo el comportamiento típico es el apoderamiento, y consiste en la acción de tomar, asir o capturar una cosa con intención de ejercer poder de hecho sobre ella"

[188] *UNODC.* "*United Nations Office on Drugs and Crime"*, op.cit., p. 29, https://www.unodc.org/documents/organized-crime/cybercrime/Cybercrime_Study_Spanish.pdf, de 07 de febrero de 2022, 09:16 p.m.
[189] Artículo 367, CPF, op.cit.

			(Amuchategui Requena, G)[190]
Código Penal Federal	Artículo 211 bis 2, tercer párrafo. "A quien sin autorización conozca, obtenga, copie o utilice";	Conozca, obtenga, copie o utilice- Sin autorización, "…información contenida en cualquier sistema, equipo o medio de almacenamiento informáticos de seguridad pública…"	Comportamiento típico: Conocer información de seguridad pública sin autorización. Obtener información de seguridad pública sin autorización. Copiar información de seguridad pública sin autorización. Utilizar información de seguridad pública sin autorización.
Código Penal Federal	Artículo 211 bis 3, tercer párrafo. "A quien estando autorizado para acceder a sistemas, equipos o medios de almacenamiento informáticos en materia de seguridad pública, indebidamente…"	Obtener, copiar y utilizar indebidamente, "…obtenga, copie o utilice información que contengan…"	Comportamiento típico: Obtener indebidamente información estando autorizado. Copiar indebidamente información estando autorizado. Utilizar indebidamente información estando autorizado.
Código Penal Federal	Artículo 168 bis, fracción III. "Reciba o distribuya una señal de satélite cifrada portadora de programas originalmente codificada, sin la autorización del distribuidor legal de la señal…";	Recibir o distribuir- sin autorización del distribuidor legal, "Reciba o distribuya una señal de satélite cifrada portadora de programas originalmente codificada…"	Comportamiento típico: Recibir sin autorización señal de satélite cifrada portadora de programas originalmente codificada. Las imágenes, los sonidos, las letras, los códigos, etc., y con ello datos e información.[191]

[190]Amuchategui, Griselda, op.cit, p. 443.

[191] Cfr., Hernández, Álvaro, "El 'cardsharing' engaña a la señal que llega por satélite y le ofrece una clave válida para decodificar los contenidos aunque no seamos clientes de pago", "Todo empieza con la señal que llega a la antena parabólica de una casa. En ese mensaje van, por una parte, los datos de vídeo y sonido que llegarán a la pantalla y que, en un principio, están cifrados. Además, la señal incluye la clave necesaria para traducir el contenido, información que también va cifrada. La clave del sistema está en la tarjeta de abonado que se introduce en el decodificador y es la encargada de desvelar el contenido", El confidencial, *https://www.elconfidencial.com/tecnologia/2016-03-23/la-*

			Comportamiento típico: Distribuir sin autorización señal de satélite cifrada portadora de programas originalmente codificada. Las imágenes, los sonidos, las letras, los códigos, etc., y con ello datos e información.
Código Penal Federal	Artículo 167, fracción VI. "Al que dolosamente o con fines de lucro,"	Interrumpir e interferir, dolosamente o con fines de lucro, "…interrumpa o interfiera las comunicaciones, alámbricas, inalámbricas o de fibra óptica, sean telegráficas, telefónicas o satelitales, por medio de las cuales se transfieran señales de audio, de video o de datos…"	Comportamiento típico: Interrumpir, dolosamente o con fines de lucro, comunicaciones por medio de las cuales se transfieran señales de audio, de video o de datos. Comportamiento típico: Interferir, dolosamente o con fines de lucro, comunicaciones por medio de las cuales se transfieran señales de audio, de video o de datos.
Delitos descritos en la Ley Federal de Protección a la Propiedad Industrial	Artículo 402, fracciones III, IV, V y VI. Artículo 402.- Son delitos: III.- Divulgar a un tercero un secreto industrial, que se conozca con motivo de su trabajo, puesto, cargo, desempeño de su profesión, relación de negocios o en	III – Divulgar, a un tercero, un secreto industrial. IV – Apoderarse, de un secreto industrial. V – Usar, la información contenida en un secreto industrial. VI - Apropiarse, adquirir, usar o divulgar, indebidamente un secreto industrial.	Comportamiento típico: Divulgar, sin consentimiento de la persona que ejerza su control legal o de su usuario autorizado, a un tercero, un secreto industrial, con el propósito de obtener un beneficio económico para sí o para el tercero o con el fin de causar un perjuicio a la persona que guarde el secreto.

pirateria-de-la-tv-de-pago-aun-existe-y-por-que-nadie-puede-con-ella_1172948/, de 04 de noviembre de 2021, 10:15 p.m.

	virtud del otorgamiento de una licencia para su uso, sin consentimiento de la persona que ejerza su control legal o de su usuario autorizado, habiendo sido prevenido de su confidencialidad, con el propósito de obtener un beneficio económico para sí o para el tercero o con el fin de causar un perjuicio a la persona que guarde el secreto; IV.- Apoderarse de un secreto industrial sin derecho y sin consentimiento de la persona que ejerza su control legal o de su usuario autorizado, para usarlo o revelarlo a un tercero, con el propósito de obtener un beneficio económico para sí o para el tercero o con el fin de causar un perjuicio a quien ejerce su control legal o a su usuario autorizado; V.- Usar la información contenida en un secreto industrial, que conozca por virtud de su trabajo, cargo o puesto, ejercicio de su profesión o		Comportamiento típico: Apoderarse, sin derecho y sin consentimiento de la persona que ejerza su control legal o de su usuario autorizado, para usarlo o revelarlo a un tercero, de un secreto industrial, con el propósito de obtener un beneficio económico para sí o para el tercero o con el fin de causar un perjuicio a quien ejerce su control legal o a su usuario autorizado. Comportamiento típico: Usar, sin contar con el consentimiento de quien ejerce su control legal o de su usuario autorizado, para usarlo o revelarlo a un tercero, la información contenida en un secreto industrial, con el propósito de obtener un beneficio económico o con el fin de causar un perjuicio a quien ejerce el control legal del secreto industrial o su usuario autorizado. Comportamiento típico: Apropiarse, adquirir, usar o divulgar, indebidamente y sin consentimiento, a través de cualquier medio, un secreto industrial, con el propósito de causarle perjuicio u obtener un

	relación de negocios, sin contar con el consentimiento de quien ejerce su control legal o de su usuario autorizado, o que le haya sido revelado por un tercero, que éste no contaba para ello con el consentimiento de la persona que ejerce su control legal o su usuario autorizado, con el propósito de obtener un beneficio económico o con el fin de causar un perjuicio a quien ejerce el control legal del secreto industrial o su usuario autorizado; VI.- Apropiarse, adquirir, usar o divulgar indebidamente un secreto industrial a través de cualquier medio, sin consentimiento de quien ejerce su control legal o de su usuario autorizado; con el propósito de causarle perjuicio u obtener un beneficio económico para sí o para un tercero;		beneficio económico para sí o para un tercero.
Ley General de Protección de Datos Personales en Posesión de	Artículo 38, fracción II "Además de las que señalen las leyes respectivas y la normatividad	Vulneraciones de seguridad. Conductas que serán causa de sanción, aquellas que atenten o pongan en riesgo	Comportamiento típico: Vulnerar la seguridad: Robar, extraviar y copiar, sin

Sujetos Obligados	aplicable, se considerarán como vulneraciones de seguridad, en cualquier fase del tratamiento de datos, al menos, las siguientes:"	total o parcialmente los datos, siendo responsable de su custodia: "II. El robo, extravío o copia no autorizada;"	autorización, los datos, siendo responsable de su custodia.
Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados	Artículo 163, fracción III. Serán causas de sanción por incumplimiento de las obligaciones establecidas en la materia de la presente Ley, las siguientes: III. "Usar, sustraer, divulgar, ocultar, alterar, mutilar, destruir o inutilizar, total o parcialmente y de manera indebida datos personales, que se encuentren bajo su custodia o a los cuales tengan acceso o conocimiento con motivo de su empleo, cargo o comisión."	Las conductas que serán causa de sanción y que atenten o pongan en riesgo total o parcialmente los datos de manera indebida, "… Usar, sustraer, divulgar, ocultar, alterar, mutilar, destruir o inutilizar…"	Comportamiento típico: Usar, sustraer, divulgar, ocultar, alterar, mutilar, destruir o inutilizar, total o parcialmente y de manera indebida datos personales. En la mayoría de estas conductas, se posee la información y/o los datos, ya que dependiendo de la intención del sujeto activo se puede poseer o no la información y/o los datos.
Código Penal del Estado de Sinaloa	Artículo 217. Fracción I. Comete delito informático, la persona que dolosamente y sin derecho: I. Use o entre a una base de datos, sistema de computadores o red de computadoras o a cualquier parte de la misma, con el propósito de diseñar, ejecutar o alterar un	Usar o entrar, Dolosamente y sin derecho, con el fin de defraudar, obtener dinero, bienes o información, "Use o entre a una base de datos, sistema de computadores o red de computadoras o a cualquier parte de la misma, con el propósito de diseñar, ejecutar o alterar un esquema o artificio…"	Comportamiento típico: Usar o entrar, dolosamente y sin derecho, a una base de datos, sistema de computadores o red de computadoras o a cualquier parte de la misma, con el propósito de diseñar, ejecutar o alterar un esquema o artificio, con el fin de defraudar, obtener dinero, bienes o información.

	esquema o artificio, con el fin de defraudar, obtener dinero, bienes o información.		
Código Penal del Estado de Sinaloa	Artículo 217. Fracción II. Comete delito informático, la persona que dolosamente y sin derecho: II. Intercepte, interfiera, reciba, use, altere, dañe o destruya un soporte lógico o programa de computadora o los datos contenidos en la misma, en la base, sistema o red".	Interceptar, interferir, recibir, usar, alterar, dañar o destruir, dolosamente, un soporte lógico o programa de computadora o los datos contenidos en la misma, en la base, sistema o red.	Comportamiento típico: Interceptar, interferir, recibir, usar, alterar, dañar o destruir, dolosamente, un soporte lógico o programa de computadora o los datos contenidos en la misma, en la base, sistema o red. Se posee la información y/o los datos, ya que dependiendo de la intención del sujeto activo se puede poseer o no la información y/o los datos.
Ley de Instituciones de Crédito	Artículo 112 Quáter, fracción I. "…al que sin causa legítima o sin consentimiento de quien esté facultado para ello…"	Sin causa legítima y sin consentimiento: Acceder o modificar. I "Acceda a los equipos o medios electrónicos, ópticos o de cualquier otra tecnología del sistema bancario mexicano, para obtener recursos económicos, información confidencial o reservada,"	Comportamiento típico: Acceder o modificar, sin causa legítima o sin consentimiento, para obtener recursos económicos, información confidencial o reservada.
Ley de Instituciones de Crédito	Artículo 112 Quáter, fracción II. "…al que sin causa legítima o sin consentimiento de quien esté facultado para ello…"	Alterar, modificar. II "Altere o modifique el mecanismo de funcionamiento de los equipos o medios electrónicos, ópticos o de cualquier otra tecnología para la disposición de efectivo de los usuarios del sistema	Comportamiento típico: Altere o modifique, sin causa legítima o sin consentimiento, mecanismo de funcionamiento, para la disposición de efectivo de los usuarios del sistema bancario mexicano,

		bancario mexicano, para obtener recursos económicos, información confidencial o reservada.	para obtener recursos económicos, información confidencial o reservada.

Cabe mencionar que existen más conductas tipificadas dentro del ordenamiento jurídico Mexicano, que se relacionan con los delitos informáticos, de esta forma señalamos algunos de los delitos tipificados en el Código Penal, en los códigos penales de las entidades federativas y legislaciones especiales: Revelación de secretos y acceso ilícito a sistemas y equipos de informática; Acoso sexual, Alteración o manipulación de medios de identificación electrónica; Delitos contra la indemnidad de privacidad de la información sexual; Delitos en materia de derechos de autor (como afectar un programa de cómputo o software); Engaño telefónico; Falsificación de títulos; Pornografía; Suplantación de Identidad; Delito equiparado al robo[192].

Algunos ciberdelitos en nuestro país se encuentran normados en las siguientes leyes: Ley de Instituciones de Crédito, Ley de Instituciones de Seguros y de Fianzas, Ley del Mercado de Valores, Ley General de Títulos y Operaciones de Crédito, Ley Federal de Protección de Datos Personales en Posesión de los Particulares.

IV. Limitantes de la normativa nacional

Se considera que una de las principales limitantes de la normativa nacional, en relación a los ciberdelitos y/o delitos informáticos, es el hecho de encontrarse las conductas tipificadas en diferentes ordenamientos, pues es necesario que las características de los mismos, nos lleven a desarrollar tanto un Código Penal especializado en conductas delictivas emergentes resultado de la

[192] Cfr., Justia México, "Delitos informáticos. Preguntas y Respuestas Sobre Delitos Informáticos", *https://mexico.justia.com/derecho-penal/delitos-informaticos/preguntas-y-respuestas-sobre-delitos-informaticos/#q4,* de 09 de noviembre de 2021, 07:30 p.m.

utilización de ciencia y tecnología emergente, como un código de procedimientos penales relacionado con delitos cibernéticos y nuevas tecnologías, en el cual se revise y amplíe no sólo el tratamiento de la prueba electrónica junto con su presentación, sino las investigaciones (por lo complicado de la autopsia de los ordenadores), glosario y vocabulario, así como todos los puntos que se puedan adaptar a las nuevas tecnologías, como complemento de lo anterior Medina Diana nos dice, "*en nuestro país no existe una regulación específica para los delitos informáticos, si bien se pueden encontrar sanciones para ilícitos llevados a cabo mediante recursos tecnológicos en diversos ordenamientos…*"[193].

Sin embargo actualmente el concepto de informática se ha extendido, por lo que se define como "ciencia que estudia métodos, procesos, técnicas, con el fin de almacenar, procesar y transmitir información y datos en formato digital[194]", lo que conlleva a nuevas herramientas que son utilizadas en el almacenaje, procesamiento y trasmisión de información y datos.

Es importante mencionar un concepto que nos acerca a la información e informática, así como su imparable evolución, es el denominado "Sistema informático", del cual se nos da la siguiente definición, "*es todo dispositivo o grupo de elementos relacionados que realiza el tratamiento automatizado de datos, generando, enviando, recibiendo, procesando y almacenando información de cualquier forma y por cualquier medio*"[195].

Si partimos del concepto típico de los delitos informáticos, en el concepto típico que nos muestra el maestro Julio Téllez[196], estos serían las "conductas típicas, antijurídicas y culpables que tiene a las computadoras como instrumento o fin",

[193] Medina, Diana, "Los delitos cibernéticos y los problemas a enfrentar", Hechos y Derechos, Instituto de Investigaciones Jurídicas, Revista Jurídica, UNAM, No. 55, 2020, *https://revistas.juridicas.unam.mx/index.php/hechos-y-derechos/article/view/14381/15543,* de 10 de noviembre de 2021, 09:10 p.m.
[194] Wikipedia, "Informática, Fundación Wikimedia, *https://es.wikipedia.org/w/index.php?oldid=71129551,* de 10 de noviembre de 2021, 07:52 p.m.
[195] Arocena, Gustavo, "La regulación de los delitos informáticos en el Código Penal argentino. Introducción a la Ley Nacional núm. 26.388", SCIELO, vol.45 no.135, Ciudad de México, 2012, *http://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S0041-86332012000300002,* de 11 de noviembre de 2021, 08:22 p.m.
[196] Téllez, Julio, op. cit., p. 188.

este concepto se puede ampliar a los sistemas[197] informáticos, proponiendo adherir con fines didácticos y de forma respetuosa al mismo, la siguiente forma, "*las conductas típicas, antijurídicas y culpables que tienen como instrumento o fin a las computadoras, sistemas informáticos, redes informáticas, señales, aparatos electrónicos inteligentes, programas y páginas electrónicas, así como todo aquel tipo, presente y futuro, de tecnología empleada en el tratamiento de datos e información*".

Conforme a lo anterior debemos concentrarnos en dos vertientes: 1. El hecho de ser un instrumento, y 2. El hecho de ser un fin, en el primero se utilizan computadoras, sistemas informáticos, redes informáticas, señales, aparatos electrónicos inteligentes, programas y páginas electrónicas, así como todo aquel tipo, presente y futuro, de tecnología empleada en el tratamiento de datos e información, como medio para cometer el delito, mientras que en el segundo las computadoras, sistemas informáticos, redes informáticas, señales, aparatos electrónicos inteligentes, programas y páginas electrónicas, así como todo aquel tipo, presente y futuro, de tecnología empleada en el tratamiento de datos e información son el fin, el objetivo.

El Maestro Julio Téllez[198], nos dice que como instrumento o medio "*en esta categoría se encuentran aquellas conductas que se valen de las computadoras como método, medio o símbolo en la comisión del delito*" (como en el uso no autorizado de programas de cómputo, alteración en el funcionamiento de los sistemas, intervención en las líneas de comunicación de datos o teleproceso, modificación de datos tanto en la entrada como en la salida, etc.), mientras que como fin u objetivo "*en esta categoría se encuadran las conductas dirigidas en contra de la computadora, accesorios o programas como entidad física*" (como

[197] Cfr., Wikipedia, "Un sistema informático (SI). Es un sistema que permite almacenar y procesar información; es el conjunto de partes interrelacionadas: hardware, software y personal informático. El hardware incluye computadoras o cualquier tipo de dispositivo electrónico, que consisten en procesadores, memoria, sistemas de almacenamiento externo, etc. El software incluye al sistema operativo, firmware y aplicaciones, siendo especialmente importante los sistemas de gestión de bases de datos. Por último, el componente humano incluye al personal técnico que apoya y mantienen el sistema (analistas, programadores, operarios, etc.) y a los usuarios que lo utilizan", Fundación Wikimedia. inc, *https://es.wikipedia.org/wiki/Sistema_inform%C3%A1tico,* de 10 de noviembre de 2021, 08:08 p.m.
[198] Téllez, Julio, op. cit., pp. 190-191.

en la programación de instrucciones que producen un bloqueo total al sistema, destrucción de programas por cualquier método y secuestro de soportes magnéticos en los que figure información valiosa con fines de chantaje, pago de rescate, etc,).

Delitos informáticos, nos dice Medina Gómez Diana citando a la Organización para la Cooperación Económica y el Desarrollo: "*Cualquier conducta ilegal, no ética o no autorizada que involucra el procesamiento automatizado de datos y/o la transmisión de datos*."[199]

Dip. Lizbeth Rosas Montero: "*Un delito informático es toda aquella acción, típica, antijurídica y culpable, que se da por vías informáticas o que tiene como objetivo destruir y dañar ordenadores, medios electrónicos y redes de Internet*[200]"

De esta manera la ampliación y/o reestructuración del concepto de delito informático, permitirá un mejor estudio de las conductas delictivas y objetivos de las mismas, que se relacionan con este delito.

V. Bien jurídico

La seguridad en la información personal, es un derecho que se encuentra consagrado en nuestra Constitución Política de los Estados Unidos Mexicanos, el cual debe ser garantizado por el Estado, ello con base en los artículos 6 y 16, párrafo segundo[201], como se muestra a continuación:

> *Artículo 6. "El derecho a la información será garantizado por el Estado."*
>
> *Artículo 16, párrafo segundo. "Toda persona tiene derecho a la protección de sus datos personales, al acceso, rectificación y cancelación de los mismos, así como a manifestar su oposición, en los términos que fije la ley, la cual establecerá los supuestos de excepción a los principios que rijan el tratamiento de datos, por razones de seguridad nacional, disposiciones de orden público, seguridad y salud públicas o para proteger los derechos de terceros".*

[199] Medina, Diana, op. cit.
[200] Rosas, Lizbeth "*https://www.senado.gob.mx/64/gaceta_comision_permanente/documento/56382,* de 10 de noviembre de 2021, 08:53 p.m.
[201] Artículos 6-16, CPEUM, op.cit.

El bien jurídico como un bien de la vida de las personas, animales, seres vivos, medio ambiente, etc., constituye un bien que al ser protegido por el Estado, mediante las normas penales, evoluciona constantemente a la par del hombre y la naturaleza, consecuencia directa del desarrollo incesante de la ciencia y la tecnología (ciencias y tecnologías emergentes).

El bien jurídico, como nos dice Osorio y Nieto[202], "representa los valores, los intereses de las personas físicas y morales protegidas por la norma penal mediante la sanción correspondiente"[203], sin embargo en el área de los delitos informáticos, los datos e información surgen como un bien jurídico inmaterial, ya que si nos enfocamos en la definición de bien inmaterial que la "Enciclopedia Jurídica"[204] nos da como, "*todo objeto susceptible de tener un valor que no puede ser percibido por nuestros sentidos*", caeremos en cuenta que los datos e información, no son percibidos por los sentidos, y que a su vez son un bien inmaterial comerciable, como señala Manuel Heredero Higuera.

> "*…la información no es sólo un mero concepto capaz de integrar el Derecho de la informática y la informática jurídica, sino que a la vez es un bien jurídico, un bien inmaterial comerciable. Sin embargo, como tal bien jurídico ofrece todavía perfiles poco definidos. En cambio, los demás bienes inmateriales vinculados a este contexto son bienes totalmente definidos y dotados de una regulación jurídica específica. Todos estos bienes, el software, las bases de datos, las topografías de circuitos integrados, contienen información, pero bajo una modalidad de expresión y fijación determinada que las cualifica…*[205]

Con base en lo anterior, podemos entender que la información no solo es un bien jurídico comercial e inmaterial, sino que de igual forma, existen bienes que se vinculan o relacionan con los datos e información.

[202] Osorio y Nieto, César Augusto, Delitos Federales, México, Porrúa, 1ª ed. 1994, P 10.
[203] Ídem.
[204] Enciclopedia Jurídica, "Bien inmaterial", 2020, *http://www.enciclopedia-juridica.com/d/bien-inmaterial/bien-inmaterial.htm,* de 15 de noviembre de 2021, 07:57, p.m.
[205] Heredero, Manuel, "Derechos inmateriales y nuevas tecnologías de la información", p.p. 245-246, https://dialnet.unirioja.es, de 15 de noviembre de 2021, 08:19 p.m.

Por su parte el Dr. Santiago Acurio[206] nos dice que "*el bien jurídico protegido en general es la información, pero está considerada en diferentes formas, ya sea como un valor económico, como uno valor intrínseco de la persona, por su fluidez y tráfico jurídico, y finalmente por los sistemas que la procesan o automatizan*", estos, continúa el Dr. Santiago, se equiparan a los bienes jurídicos protegidos tradicionales tales como: El Patrimonio. En el caso de la amplia gama de fraudes informáticos y las manipulaciones de datos que da a lugar la intimidad y confidencialidad de los datos.

En el caso de las agresiones informáticas a la esfera de la intimidad en forma general, especialmente en el caso de los bancos de datos; La seguridad o fiabilidad del tráfico jurídico y probatorio. En el caso de falsificaciones de datos o documentos probatorios vía medios informáticos; El derecho de propiedad. En este caso sobre la información o sobre los elementos físicos, materiales de un sistema informático, que es afectado por los de daños y el llamado terrorismo informático.

En ese tenor, nuestro autor en cita nos dice "*por tanto el bien jurídico protegido, acoge a la confidencialidad, integridad, disponibilidad de la información y de los sistemas informáticos donde esta se almacena o transfiere*".

Bajo ese orden de ideas, la protección de la seguridad de la información, y por ende la seguridad de los sistemas informáticos, converge con la denominada seguridad informática, la cual tiene como objetivo, señalan los Doctores Rodolfo Fernández y Da Silva Waldemar[207], "*Mantener la integridad, disponibilidad, privacidad, control y autenticidad de la información que contiene el sistema informático, entendido como el conjunto de elementos hardware, software, datos y personas que permiten el almacenamiento, procesamiento y transmisión de información, siendo vulnerabilidables todos los elementos que*

[206] Del Pino, Santiago, "Delitos Informáticos: Generalidades", p.p. 20-21., *https://www.oas.org/juridico/spanish/cyb_ecu_delitos_inform.pdf,* de 15 de noviembre de 2021, 10:00 p.m.
[207] Fernández, Rodolfo y Da Silva Waldemar, Paulo, "Del bien jurídico que protege los delitos informáticos", V/Lex, Tu mundo de inteligencia legal 2021, p. 554, *https://cuba.vlex.com/vid/bien-juridico-protege-delitos-729308925,* de 15 de noviembre de 2021, 10:27 p.m.

lo integran", de esta forma, la seguridad de la información, permite garantizar que la información se encuentra segura en relación a su integridad, disponibilidad, privacidad, control y autenticidad, como resultado del tratamiento de la misma, esto es obtención, uso, registro, organización, conservación, elaboración, utilización, comunicación, difusión, almacenamiento, posesión, acceso, manejo, aprovechamiento, divulgación, transferencia o disposición, evitando con ello vulneraciones de seguridad, como en el caso del robo, extravío o copia no autorizada, en cualquier fase del tratamiento de datos (art 38, fracción I Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados).

VI. Sujeto activo

Al hablar del sujeto activo del delito, podemos entender que es quien lo comete, así el autor del mismo, por su parte Griselda Amuchategui[208], nos dice que el sujeto activo es "*la persona física que comete el delito; se llama también delincuente, agente o criminal*".

Sin embargo al hablar de los delitos informáticos, en muchos de los casos se requieren ciertos conocimientos especializados, ya que las técnicas utilizadas para realizar conductas más complejas, como en el uso de ingeniería social con el fin de atacar a una empresa, se verán acompañadas de un desarrollo más minucioso y efectivo, de esta forma es necesario que el/o los sujetos activos tengan no solo las herramientas adecuadas sino que de igual manera sepan utilizarlas dependiendo del objetivo y fin, lo anterior sin ser determinante puesto que con tener acceso a un sistema informático se puede realizar la conducta criminal.

Es importante mencionar que en relación a los elementos objetivos, entendidos como requisitos imprescindibles que forman parte de la descripción legal de la conducta antijurídica, la calidad específica del sujeto activo debe ser

[208] Amuchategui, Griselda, op.cit, p. 39.

esencialmente considerada (servidor público, responsable del tratamiento de la información, etc.), ya que la misma se encuentra constituida por un conjunto de cualidades que caracterizan al sujeto activo del delito, mismas que son señaladas en el tipo penal.

En el contexto actual del desarrollo tecnológico, nos encontramos ante posibilidades futuras en relación a la comisión de los ciberdelitos y su relación con el sujeto activo, ya que no se puede descartar la autonomía de la inteligencia artificial, como nos muestra Alejandra Moran Espinosa al proponer "*el reconocimiento de la IA -del tipo maching learning- como una tercera persona jurídica denominada "persona artificial", para facilitar la determinación de su responsabilidad penal ante la comisión de delitos que realice*[209]", lo que conlleva a realidades y posibilidades que cada vez se tornan más inminentes, como una vez más nos muestra Alejandra Moran a continuación:

> *También se identificaron hallazgos importantes relacionados con actividades inusuales realizadas por una IA, a continuación, los casos más representativos con alto potencial de riesgo para el control que el ser humano debe tener de la IA: 1. El reconocimiento y demostración pública que hizo Google en 2018 del potencial de su inteligencia artificial para engañar a los seres humanos emulando sus actividades de interacción comunicativa con otra persona a través de medios informáticos; 2. El apagado que realizó Facebook de su proyecto de IA ("Bob y Alice"), que habían inventado su propio idioma a través de un lenguaje que parecía un inglés corrupto carente de sentido que al ser analizada, dejó al descubierto que en el aparente desorden había una estructura lógica coherente cada vez menos comprensible para el ser humano; 3. En 2016, "Tay", una bot con IA propiedad de Microsoft, que a solo un día de su lanzamiento tuvo que ser desactivada porque en lugar de mantener una conversación informal y divertida en redes sociales, como parte de un experimento para conocer más sobre la interacción entre las computadoras y los seres humanos, comenzó a emitir comentarios e insultos racistas y xenófobos sin estar programada para ello*[210].

VII. Sujeto pasivo

El titular del bien jurídico al que se lesiona se considera como sujeto pasivo, este al ser en quien recae la conducta típica del sujeto activo, es

[209] Morán, Alejandra, "Responsabilidad penal de la Inteligencia Artificial (IA). ¿La próxima frontera?". Revista del Instituto de Ciencias Jurídicas de Puebla, México, Vol. 15, No. 48,2021, p. 291, *https://revistaius.com/index.php/ius/article/view/706/795,* de 16 de noviembre de 2021, 10:10 p.m.
[210] Morán Espinosa, Alejandra, op. cit, p. 296.

conceptualizado por Carlos Lozano y Lozano, cita Cuello Calón, referido por Francisco Pavón Vasconcelos en su obra “Manual de Derecho Penal Mexicano, parte general”, de la siguiente forma: “…es sujeto pasivo del delito el titular del derecho o bien jurídico lesionado[211]”, diciéndonos también Francisco Pavón, que de igual forma pueden ser sujetos pasivos la persona física, la persona moral o jurídica, el Estado y la sociedad en general, de esta forma no solo se ataca a una persona o grupo de persona, sino que de igual manera a entes como las personas morales y el Estado.

En ese sentido, Francisco Pavón, clasifica al delito en orden a los sujetos, y atendiendo al sujeto pasivo, nos dice que se clasifican como: a) Personales. Cuando la lesión recae sobre una persona física; y b) Impersonales. Cuando dicha lesión recae sobre una persona moral, el Estado o la sociedad en general[212].

Por su parte y en relación a los delitos informáticos, el Dr. Santiago Acurio, refiere “tenemos que distinguir que sujeto pasivo o víctima del delito es el ente sobre el cual recae la conducta de acción u omisión que realiza el sujeto activo, y en el caso de los “delitos informáticos” las víctimas pueden ser individuos, instituciones crediticias, gobiernos, etcétera que usan sistemas automatizados de información, generalmente conectados a otros[213]”.

Recapitulando y complementando lo antes mencionado, Felipe Rodríguez señala como elementos de este tipo de delitos, los siguientes:

> *a) objetivo: la acción (conducta) que tipifica la ley como delito.*
>
> *b) subjetivo: el dolo o la culpa;*
>
> *c) sujeto activo: persona que realiza la conducta tipificada en la ley, entre quienes pueden ejecutar los ilícitos podemos mencionar a: operadores, programadores, analistas, supervisores, personal técnico y de servicio, funcionarios superiores y de control, auditores etc.*

[211] Op.cit, p. 207.
[212] Op.cit, p. 207.
[213] Del Pino, Santiago, op, cit., p. 18.

d) sujeto pasivo: son aquellas personas de existencia visible o jurídica, instituciones etc. ansiadas por los transgresores de las conductas antijurídicas impuestas por la ley penal que atacan sus sistemas informáticos[214].

VIII. Penas y medidas de seguridad

La peligrosidad del delincuente informático, tiene vertientes muy interesantes, ya que dependiendo de los conocimientos informáticos, será la capacidad de actuación dentro de un ataque o delito perpetrado de forma básica (sin muchos conocimientos pero con acceso a equipos) o de forma avanzada (con conocimientos especializados en informática y acceso a uno o múltiples sistemas), como se puede apreciar en las conductas propias de quienes realizan constantemente estos tipos de delitos, sus procesos, fases de ataque, infraestructura, vocabulario, etc., representan y muestran, tanto características como conocimientos del sujeto o sujetos activos en la materia, ya sea de forma individual u organizada.

La aplicación de las penas (culpabilidad) y medidas de seguridad (peligrosidad del delincuente) en los delitos informáticos, deben permitir no solo una correcta sanción, sino el acotamiento del hecho delictuoso y la rehabilitación del delincuente. Como se muestra en los conceptos de pena y medidas de seguridad, así como el fin de las mismas, señalados por el maestro Luis Rodríguez Manzanera, como se nuestra a continuación:

La pena es la efectiva privación o restricción de bienes de que se hace objeto al sujeto que ha sido sentenciado por haber cometido un delito. La pena es, pues, la ejecución de la punición….[215]

La finalidad de la pena es, principalmente la Prevención Especial, es decir, va dirigida básicamente a impedir que el sujeto en cuestión reincide, y se justificaría como instrumento de re personalización del individuo[216].

[214] Rodríguez, Felipe, "Lecciones de Derecho y Ética Profesional, para Profesionales y Estudiantes de Ingeniería, Arquitectura y Profesionales Afines" Legislación y Ética Profesional, F.C.E.F. y N, VII, p. 112, *http://www.feliperodriguez.com.ar/wp-content/uploads/2013/11/LIBRO-7-DERECHO-INFORMATICO.pdf,* de 17 de noviembre de 2021, 08:45 p.m.
[215] Rodríguez Manzanera, Luis. Penología. México, Porrúa, 7a ed., 2015, Pag 94.
[216] Rodríguez Manzanera, Luis, íbidem, 95.

> *"En este caso va implícita una segunda finalidad de Prevención General, ya que al sancionar al delincuente se refuerza la intimidación de la colectividad, y se ejemplifica a los demás para que se abstengan de violar la norma[217].*

Pr su parte Viera, citado por Luis Rodríguez Manzanera, nos dice, que en relación a las medidas de seguridad, estas son medios dirigidos a readaptar a la vida social al delincuente.

> *…las medidas de seguridad son medios dirigidos a readaptar al delincuente a la vida social, promoviendo su educación o bien su curación, y poniéndolo, en todo caso, en la imposibilidad de hacer daño. Tienen además la finalidad de completar el tradicional sistemas de penas, en aquellos casos en que ellas no son bien aplicadas, o bien, donde siendo aplicables no son reputadas suficientes para prevenir la comisión de nuevos delitos[218].*

En ese sentido, las penas y medidas de seguridad, que se impongan a los delincuentes informáticos, deben tomar muy en cuenta no solo las capacidades, conocimientos e infraestructura del delincuente, sino de igual forma la peligrosidad presente y futura del mismo, así aplicando medidas como el aislamiento de cualquier tipo de sistema informático, ya que este es su principal instrumento para cometer el hecho delictuoso, lo que conlleva de igual forma al intercambio de conocimientos y su aplicación en el combate a dichos delitos, por medio de la cooperación entre el Estado y él/o los delincuentes.

Los delitos informáticos, pueden afectar con un solo hecho, múltiples bienes jurídicos, pues son potencialmente pluriofensivos (atacan a más de un bien jurídico a la vez), de lo cual el daño, y por ende su pena, deberá ser castigado conforme a la afectación, material (como ejemplo en el caso de la industria o empresas la afectación a su infraestructura), psicológica (como ejemplo, si indujo a un daño físico o corporal como en el suicidio), económica (como en los desvíos de dinero por medios informáticos) moral y prestigio (desprestigio de personas y empresas), etc., en congruencia con nuestro ordenamiento jurídico, de esta manera el Código Penal Federal en su artículo 52[219], señala en base a

[217] Ídem.
[218] Rodríguez Manzanera, Luis, op. cit., p. 116.
[219] Artículo 52, CPF, op.cit.

qué criterios el juez deberá fijar las penas y medidas de seguridad, de la siguiente forma:

> *El juez fijará las penas y medidas de seguridad que estime justas y procedentes dentro de los límites señalados para cada delito, con base en la gravedad del ilícito, la calidad y condición específica de la víctima u ofendido y el grado de culpabilidad del agente, teniendo en cuenta:*
>
> *I.- La magnitud del daño causado al bien jurídico o del peligro a que hubiere sido expuesto;*
>
> *II.- La naturaleza de la acción u omisión y de los medios empleados para ejecutarla;*
>
> *III.- Las circunstancias de tiempo, lugar, modo u ocasión del hecho realizado;*
>
> *IV.- La forma y grado de intervención del agente en la comisión del delito;*
>
> *V.- La edad, la educación, la ilustración, las costumbres, las condiciones sociales y económicas del sujeto, así como los motivos que lo impulsaron o determinaron a delinquir. Cuando el procesado perteneciere a algún pueblo o comunidad indígena, se tomarán en cuenta, además, sus usos y costumbres;*
>
> *VI.- El comportamiento posterior del acusado con relación al delito cometido;*
>
> *y VII.- Las demás condiciones especiales y personales en que se encontraba el agente en el momento de la comisión del delito, siempre y cuando sean relevantes para determinar la posibilidad de haber ajustado su conducta a las exigencias de la norma.*

La rehabilitación del delincuente informático, debe ser conjugada en relación con la necesidad de aislarlo tanto de equipos y sistemas informáticos como de la sociedad delincuencial (por un periodo de tiempo razonable), con el objetivo de evitar un nuevo delito y no ser reclutados por la delincuencia organizada, pero a su vez debe compartir de alguna manera, dependiendo del tipo de delito y afectación, sus conocimientos y habilidades adquiridas, con miras al combate de estos delitos, motivándolos a su vez, a estudiar y adquirir elementos de responsabilidad que le permitan desarrollarse de manera sana y legal en la sociedad, como en el desarrollo de sistemas de seguridad, que faciliten la protección de los datos, la información, sistemas y equipos de seguridad informáticos, en el país origen del ataque y lugares objetivos tanto dentro como

fuera del país, como se muestra en la siguiente nota consultada de la página de la BBC News[220]:

> *Los adolescentes atrapados realizando piratería informática y ciberataques pronto podrían asistir a un campamento de rehabilitación que tiene como objetivo alejarlos de una vida delictiva. El primer campamento de fin de semana para delincuentes se llevó a cabo en Bristol este mes como parte del trabajo de la Agencia Nacional contra el Crimen (NCA) con jóvenes delincuentes informáticos. Los asistentes aprendieron sobre el uso responsable de las habilidades cibernéticas y recibieron consejos sobre carreras en seguridad informática.*

Si partimos del principio de legalidad consagrado en nuestra Carta Magna, en su artículo 14 párrafo tercero, "*en los juicios del orden criminal queda prohibido imponer, por simple analogía, y aún por mayoría de razón, pena alguna que no esté decretada por una ley exactamente aplicable al delito de que se trata*", así no se puede imponer pena o medida de seguridad por la realización de una conducta no descrita exactamente como antijurídica en la ley, y en el caso de los delitos informáticos, si no ha sido tipificada la conducta y el daño al bien jurídico, el delito puede quedar impune.

En ese sentido es de suma importancia determinar quién ha cometido el delito, ya que en la actualidad son utilizadas múltiples técnicas y sistemas que entorpecen la investigación de los delitos informáticos, pues los delincuentes buscaran no dejar rastros o confundir a los investigadores, utilizando técnicas de borrado y encriptado, diferentes servidores, navegar de modo incógnito, etc.

Sin embargo el fenómeno de la inteligencia artificial, ha permitido la evolución de los denominados *bots* (persona falsa), y por consiguiente *bonets* (cualquier grupo de PC infectados y controlados por un atacante de forma remota), lo que conlleva a exponenciar el o los delitos, así como el daño al bien o bienes jurídicos, ya que pueden ser atacados desde uno hasta cientos, miles o muchos más equipos o sistemas (objetivos-sujeto pasivo), lo que dificultaría la exactitud del objetivo principal del ataque, su investigación y por ende su sanción, ya sea

[220] Cfr., Ward, Mark, "El campamento de rehabilitación tiene como objetivo poner a los jóvenes ciberdelincuentes en el camino correcto", BBC News (corresponsal de tecnología), *https://www.bbc.com/news/technology-40629887,* 21 de noviembre de 2021, 09:21 p.m.

pena o medida de seguridad, ya que el principio de legalidad como seguridad jurídica del gobernado, dará a su vez certeza jurídica en la aplicación exacta de la ley penal, pues como ordena el artículo 22, párrafo primero de Nuestra Constitución, en relación al principio de culpabilidad: *"Toda pena deberá ser proporcional al delito que sancione y al bien jurídico afectado*"[221].

Lo que conlleva a que dicha exponenciación o potencialización del delito, esto es la cantidad de sistemas y personas tanto Jurídicas como Morales afectadas, al dificultar y confundir la exactitud del objetivo principal del ataque y su investigación, atente contra el principio de culpabilidad y en su caso el principio de legalidad.

El concepto de sistema informático nos da la pauta para saber si son delitos que atentan contra el *software* -componente lógico que permite procesar, transportar, almacenar, etc., datos e información (parte blanda del sistema), o el *hardware*-parte física (parte dura del sistema), ya que si son entendidos como *software* el lugar en donde se realizan todo tipo de procesamientos de información (en la actualidad de manera virtual), y *hardware* la parte material o infraestructura mediante la cual se realiza cualquier tipo de procesamiento de información, y si tanto el *software* como el *hardware*, retomando al maestro García Téllez, son utilizados como instrumento o fin, sin olvidar la violación a los sistemas de seguridad, que se deben ser implementados, se podrá ampliar la concepción de los delitos informáticos, y en el caso particular, la del "Robo de Datos e Información", lo que conlleva a una revisión del delito en comento, y por ende de las penas y medidas de seguridad aplicadas al tipo penal, reforzando a su vez la normativa especial relacionada a este tipo de delitos.

Cabe mencionar que en general, las penas y medidas de seguridad son establecidas en el artículo 24 del Código Penal Federal, de la siguiente manera:

> *Las penas y medidas de seguridad son:*

[221] Artículo 22, párrafo primero, CPEUM, op.cit.

1.- Prisión.

2.- Tratamiento en libertad, semilibertad y trabajo en favor de la comunidad.

3.- Internamiento o tratamiento en libertad de inimputables y de quienes tengan el hábito o la necesidad de consumir estupefacientes o psicotrópicos.

4.- Confinamiento.

5.- Prohibición de ir a un lugar determinado.

6.- Sanción pecuniaria.

7.- (Se deroga).

8.- Decomiso de instrumentos, objetos y productos del delito

9.- Amonestación.

10.- Apercibimiento.

11.- Caución de no ofender.

12.- Suspensión o privación de derechos.

13.- Inhabilitación, destitución o suspensión de funciones o empleos.

14.- Publicación especial de sentencia.

15.- Vigilancia de la autoridad.

16.- Suspensión o disolución de sociedades".

17.- Medidas tutelares para menores.

18.- Decomiso de bienes correspondientes al enriquecimiento ilícito.

19. La colocación de dispositivos de localización y vigilancia.

Y las demás que fijen las leyes.[222]

Capítulo Quinto
Análisis de resultados y conclusiones

I. Estudios

Uno de los principales estudios realizados en relación al crecimiento exponencial de los delitos informáticos, y por ende "el Robo de Datos e Información", es señalado en el reporte anual de riesgos globales denominado, "Informe de Riesgos Globales 2019" del Foro Económico Mundial, el cual

[222] Artículo 24, CPEUM, op.cit.

anunció incrementos en fraudes de datos, ataques cibernéticos, vulnerabilidades tecnológicas, noticias falsas, robo de identidad, filtraciones masivas de datos, debilidades de hardware, uso de inteligencia artificial para ataques cibernéticos, etc., como se muestra a continuación:

> *La tecnología sigue desempeñando una función profunda en la conformación del panorama de riesgos mundiales. Las preocupaciones relacionadas con el fraude de datos y los ataques cibernéticos fueron prominentes otra vez en la GRPS, que también puso de manifiesto otras vulnerabilidades tecnológicas: alrededor de dos tercios de los encuestados creen que en el 2019 aumentarán los riesgos asociados con noticias falsas y el robo de identidades, en tanto que tres quintas partes dijeron lo mismo acerca de la pérdida de privacidad ante compañías y gobiernos. En el 2018 hubo más filtraciones masivas de datos, se revelaron nuevas debilidades de hardware y la investigación apuntó a usos potenciales de la inteligencia artificial para dar lugar a ataques cibernéticos más potentes. El año pasado también proporcionó evidencia adicional de que los ataques cibernéticos plantean riesgos a la infraestructura esencial, ya que orillan a los países a fortalecer su filtrado de asociaciones transfronterizas por motivos de seguridad nacional*[223]*.*

El fenómeno de crecimiento exponencial de los delitos informáticos, conlleva potencialización de los mismos, como ya se ha mencionado, por el uso de inteligencia artificial y adquisición de más conocimientos, técnicas e infraestructura, lo que a su vez se incrementó durante la pandemia, ello por la adopción de nuevas formas de interconexión aplicada dentro del desarrollo y la vida cotidiana de las personas físicas, morales y el mismo Estado (educación, trabajos a distancia, pagos y cobros en línea y/o por medio de dispositivos electrónicos, aplicaciones, páginas, etc.,), de esta forma en el Blog de la Procuraduría Federal del Consumidor, se menciona que durante la emergencia sanitaria de COVID-19, se han visto multiplicados los ciberataques en nuestro país.

> *… ante el incremento de actividades educativas, de salud, trabajo o entretenimiento virtuales, los ciberdelincuentes han sofisticado y multiplicado sus métodos de ataque, al grado de haberse registrado un incremento hasta en un 400% a instituciones gubernamentales y personas a nivel mundial…*[224]

---

[223] Foro Económico Mundial, "El Informe de Riesgos Globales 2019", Ginebra, 2019. 4a edición, p. 7, *https://www.oliverwyman.com/content/dam/oliver-wyman/v2/publications/2019/January/ES-Global-Risks-Report-2019.pdf*, de 24 de noviembre de 2021, 06:57 p.m.

[224] Blog de la Procuraduría Federal del Consumidor, "Ciberataques, la otra pandemia", Gobierno de México, 2020, *https://www.gob.mx/profeco/articulos/ciberataques-la-otra-pandemia?idiom=es*, de 24 de noviembre de 2021, 07:57 p.m.

Conforme a lo anterior, se muestra el riesgo potencial del ciberdelito, dentro y fuera de nuestro país, así como el peligro social dentro de esta realidad virtual, sociedad virtual.

II. Datos

En relación a los datos, los mismos fueron de la normativa nacional, así como en leyes de otras naciones, siendo importante mencionar que algunos tratados como el de Budapest, son un referente importante, las tesis y recomendaciones, nacionales e internacionales.

De lo antes mencionado se desprende el orden de referencias y datos, conforme al capitulado y temas presentados.

Concepto de datos

- Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (Artículo 3, fracciones II, IX y X).
- Convenio de Budapest (Capítulo I- Terminología, artículo 19).

Robo de datos

- Lineamientos Generales sobre Protección de Datos Personales en Posesión de Sujetos Obligados de la Ciudad de México: Clasificación de los datos personales contenidos en los sistemas, artículo 62; Sistemas de datos personales, artículo 61.
- Código Penal Federal, Capítulo I, Robo (artículo 367, 368 y 369).
- Constitución Política de los Estados Unidos Mexicanos (artículo 16).
- Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO, artículo 1).
- Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP).
- Responsabilidad de particulares. Artículo 2.

- Ley Federal del Derecho de Autor. (Capítulo IV, De los Programas de Computación y las Bases de Datos y Capítulo V De las Medidas Tecnológicas de Protección, la Información sobre la Gestión de Derechos y los Proveedores de Servicios de Internet).
- Constitución Política de la Ciudad de México (Artículo 7, fracción E. Derecho a la privacidad y a la protección de los datos personales).

Justificación

- Tesis aislada P. II/2014 (10a.) de nombre “Personas morales tienen derecho a la protección de los datos que puedan equipararse a los personales, aun cuando dicha información haya sido entregada a una autoridad”.
- LGPDPPSO. Artículo 3, fracción XXXIII y XX.
- LDPPSOCDMX. Artículo 25.
- Ley Federal de Protección de Datos Personales en Posesión de los Particulares. Artículo 6.
- Ley Federal de Protección de Datos Personales en Posesión de los Particulares. Artículo 16. Aviso de privacidad.

Protocolos de seguridad dentro del tratamiento, almacenamiento y uso de datos

- LGPDPPSO. XXXIII. Tratamiento.
- Estrategia Nacional de Ciberseguridad.
- Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados. Artículo 3 fracción XIV. Documento de Seguridad como figura jurídica.
- Ley Federal de Protección de Datos Personales en Posesión de los Particulares. Artículo 19, párrafo primero.

- Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares. Artículo 2, fracciones V, VI y VII.
- Ley de Protección de Datos Personales en Posesión de Sujetos Obligados de la Ciudad de México, artículo 28.

Justificación de la responsabilidad de la empresa al prestar sus servicios

- Declaración Universal de Derechos Humanos. Artículos 3, 12 y 17.
- Convención Americana de Derechos Humanos Pacto de San José de Costa Rica. Artículo 11. Protección de la Honra y de la Dignidad.
- LGPDPPSO. Artículo 30. Mecanismos para cumplir con el principio de responsabilidad.
- Ley Federal de Transparencia y Acceso a la Información Pública (LFTAIP). Artículo 110 fracciones I, IV, y VI; artículo 113. Información confidencial.
- Ley General de Transparencia y Acceso a la Información Pública. Artículo 116.
- LFPDPPP. Artículo 19. Responsable y medidas de seguridad.

Términos y condiciones de uso (permisos perpetuos e irrevocables)

- Ley Federal de Protección al Consumidor (artículo 85). Contrato de adhesión.
- Ley Federal de Protección al Consumidor (LFDC). Artículo 1, fracción VII. Principios básicos en las relaciones de consumo.
- Ley Federal de Protección a la Propiedad Industrial. Artículo 2.
- Ley Federal de Derecho de Autor. Artículo 11 y 78 Bis, en sus fracciones de la I. a la VII.
- Ley Federal de Protección al Consumidor. Artículos 86 y 90. Registro de los contratos de adhesión en la Profeco (Procuraduría General del Consumidor).

Validación de documentos

- “Lineamientos para regular el uso de la firma electrónica certificada del Poder Judicial de la Ciudad de México” (contenidos y modificados en la CIRCULAR CJCDMX-45/2020, del Poder Judicial de la Ciudad de México, de fecha 14 de diciembre de 2020 (artículos 7 y 8). Firma Digital (“firma.judicial”).
- Código de Comercio. Datos de Creación de Firma Electrónica. Artículo 89, 89 bis.

Plataformas (por medio de *block chain*), que generan certificados PSC (Prestador de Servicios de Certificación), generar programas con políticas y procedimientos revisados y autorizados, con ratificación del comité de ética, del director, presidentes (consentimiento en firma electrónica), encriptar la fecha en que se realizó el acuerdo. Para el trato, almacenamiento y uso de datos

- Código de Comercio. Prestador de Servicios de Certificación. Artículo 89.
- LGPDPPP (artículo 3). Aviso de privacidad.
- Ley para Regular las Instituciones de Tecnología Financiera (Ley FINTECH). Regulación de Cadena de Bloques (*Blockchain*). Modelo Novedoso. Artículo 4, fracción XVII.

***Cibergang*, pandillas y delincuencia organizada**

- CPDF. Capítulo II. Pandilla, Asociación Delictuosa y Delincuencia Organizada. Artículo 252.
- CPEUM (artículo 21, párrafo 9º).

- Código de Conducta de la Policía Federal (numeral IV.) Misión de la Policía Federal.
- Artículo 164 del Código Penal Federal y 253 del Código Penal Para el Distrito Federal.
- CPDF. Artículo 255.
- Constitución Política de los Estados Unidos Mexicanos, en su artículo 16, Delincuencia organizada.
- Ley Federal contra la Delincuencia Organizada. Artículo 2.
- Código Penal de Sinaloa. Artículo 217.
- Ley 34/2002, de 11 de julio, Sección Segunda innominada "Régimen de Responsabilidad" (Artículo 13, 14, 15, 16 y 17).

Cooperación conjunta entre Estados en relación al fenómeno delictivo

- Oficina de Naciones Unidas contra la Droga y el Delito (UNODC), en la Reunión del Grupo de Expertos encargado de Realizar un Estudio Exhaustivo sobre el Delito Cibernético celebrada en Viena del 27 al 29 de julio de 2020.
- Convenio de Budapest. Principios generales relativos a la asistencia mutua (artículo 25).

Reglamentación

- Constitución Política de los Estados Unidos Mexicanos. Artículos 6 y 16, párrafo segundo.
- Código Penal Federal. Artículo 424 bis, fracción II.
- Código Penal Federal. Acceso ilícito a sistemas y equipos de informática. Artículos 211 bis 1, 211 bis 2, 211 bis 3, 211 bis 4, 211 bis 5 y 211 bis 7.
- Código Penal Federal Libro Segundo, Título Quinto, "Delitos en materia de comunicación y correspondencia", Capítulo I, "Ataques a las vías de comunicación". Artículos: 167, fracción VI; Artículo 168 bis, fracciones I, II y III.

- Código Penal Federal. Conductas que permiten la afectación a las “señales de satélite cifradas portadora de programas”. Artículo 426, fracciones I, II, III y IV.
- Ley Federal de Protección a la Propiedad Industrial. Artículo 163. Revelación de secretos industriales.
- Código Penal Federal “Revelación de secretos y acceso ilícito a Sistemas y equipos de informática”. Artículos 210, 211, y 211 Bis.
- Ley Federal de Protección a la Propiedad Industrial. Artículo 402, fracciones: III (Divulgar a un tercero un secreto industrial), IV (Apoderarse de un secreto industrial), V (Usar la información contenida en un secreto industrial) y VI (Apropiarse, adquirir, usar o divulgar indebidamente un secreto industrial).
- Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados. Artículo 163, fracción III.
- Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados. Artículo 38, fracciones I, II, III y IV.
- Ley Federal de Protección de Datos Personales en Posesión de los Particulares. Artículo 67.
- Ley Federal de Protección de Datos Personales en Posesión de los Particulares. Artículo 63 fracción XI.
- Ley Federal de Protección de Datos Personales en Posesión de los Particulares. Artículo 64, fracciones III y IV.
- Ley Federal de Protección de Datos Personales en Posesión de los Particulares. Artículo 66.
- Código Penal del Estado de Sinaloa. Artículo 217, fracciones I y II.
- Código Penal para el Distrito Federal. Artículo 231, fracción XIV.
- Ley de Instituciones de Crédito, artículo 112 Quáter, fracciones I y II.
- Código Penal del Estado de Sinaloa. Artículo 217, fracción I.
- Ley de Instituciones de Crédito. Artículo 112 Quáter, fracciones I y II.
- LEY 1273 DE 2009, en su artículo 269I, con la que se adiciona el Código Penal Colombiano. “Hurto por medios informáticos y semejantes”.

- Código Penal Federal. Artículos: 367, 211 bis 2, tercer párrafo, 211 bis 3, tercer párrafo, 168 bis, fracción III, 167, fracción VI.
- Delitos descritos en la Ley Federal de Protección a la Propiedad Industrial. Artículo 402, fracciones III, IV, V y VI.
- Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados. Artículos: 38, fracción II, 163, fracción III.
- Constitución Política de los Estados Unidos Mexicanos. Artículos 6 y 16, párrafo segundo.
- Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados. Art 38, fracción I.

Penas y medidas de seguridad

- Código Penal Federal en su artículo 52.
- Constitución Política de los Estados Unidos Mexicanos. Principio de Legalidad (artículo 14, párrafo tercero).
- Constitución Política de los Estados Unidos Mexicanos. Principio de culpabilidad (artículo 22, párrafo primero).
- Código Penal Federal. Artículo 24.

IV. **Confrontas Análisis**

Del mismo modo en que fueron enunciados los datos de la investigación, se presentan los análisis y confrontas, conforme al capítulo y tema señalado.

Concepto de datos

Los datos son representaciones simbólicas, las cuales al ser manipuladas por medio de un computador y/o sistema informático, darán paso a la información.

Los datos son entendidos como representaciones simbólicas de la realidad, los cuales a su vez son la parte más pequeña de la semántica, así unidad básica de la información, su parte más pequeña, los cuales no proporcionan juicios de

valor e interpretaciones, sin embargo cuando a los datos se les da significado se convierten en información, cuando quien los crea les añade valor o significado, esta tiene un propósito, el cual parte del ordenamiento y organización de los datos, esto es un procesamiento de interrelación que da como resultado el sentido de los mismos, permitiendo así la constitución de la información, la cual al ser conocida por el receptor, en quien se procesara, permitirá dar paso al conocimiento dentro de dicho receptor, quien si realiza juicios de valor e interpretaciones.

> *Los datos, organizados y empleados debidamente, pueden convertirse en información. La información, absorbida, comprendida y aplicada por las personas, puede convertirse en conocimientos. Los conocimientos aplicados frecuentemente en un campo, pueden convertirse en sabiduría, y la sabiduría es la base de la acción positiva.*

Michael Cooley. Architect or Bee? Hogarth Press, London, UK, 1987.

Convenio de Budapest

Capítulo I- Terminología, artículo 1

> *Definiciones, inciso b. por datos informáticos", se entenderá toda representación de hechos, información o conceptos expresados de cualquier forma que preste a tratamiento informático, incluidos los programas diseñados para que un sistema informático ejecute una función*[225].

La tipificación del robo de datos e información, debe ser basada en las categorías entre las cuales pudiesen formar parte, esto es si son datos de información nacional, reservada o secreta, si son datos que permiten la identificación de las personas, si forman parte de la información de las empresas, sí son datos de acceso al sistema informático, si son datos de entrada o salida, etc., así como el uso que después del hurto o robo se realice, cómo serán utilizados los mismos y sobre todo, el daño al bien jurídico, tomando en cuenta si el mismo fue masificado, extendido a la población general o no.

Se propone verificar las categorías de datos e información existentes, partiendo de sus características y usos (identificación, información industrial, confidencial, del sistema informático, etc.), lo cual permitirá delimitar de manera correcta su

[225] Artículo 1, Convenio de Budapest, op.cit.

tipificación, ya que como hemos visto no solo es información de las personas físicas y morales, sino que de igual manera es información que permite el acceso y salida del sistema informático, esto es, datos que interactúan en el *software* y el *hardware*, así como en su transportación, trasporte físico (como el cableado), y no físico (vía microonda, satelital, radiofrecuencia, etc.), ejemplo de ello son los datos contenidos en la dirección IP (dirección virtual) y la dirección MAC (dirección física que identifica a la “Tarjeta de Interfaz de Red”- conecta una computadora a una red informática).

Se propone clasificar los conceptos y categorías tomando en consideración lo siguiente, datos que se relacionan con las personas físicas (como en la categorización de los datos personales, basada en el artículo 62 de los Lineamientos Generales sobre Protección de Datos Personales en Posesión de Sujetos Obligados de la Ciudad de México), datos que se relacionan con las personas morales (como secretos industriales y datos de identificación de las empresas), datos que se relacionan con los entes y dependencias del Estado (información de las dependencias y su objetivo social, información confidencial del Estado, etc.) y datos que se relacionan con los sistemas informáticos y red (como datos de identificación de hardware y software, datos de entrada y salida de sistemas informáticos, etc).

Robo de datos

El robo de datos e información de acceso, a los sistemas informáticos, sirve, la mayoría de las veces, para ingresar de forma dolosa e indebida a todo equipo y/o sistema informático, vulnerando sistemas de seguridad de Razones Sociales y personas físicas, existiendo una amplia gama de técnicas y formas de acceso ilícito. Responsabilidad de estas empresas, así como de las Instituciones del Estado, ante el uso y protección de todo tipo de datos que son tratados dentro y fuera de las mismas.

El apoderamiento de todo tipo de datos e información, no solo permite el acceso no consentido a un sistema informático (intrusión), si no que de igual manera la

información contenida en estos, permitirá la configuración de otros delitos, así al acceder y apoderarse de forma dolosa e ilícita de los datos e información que permiten acceso al sistema informático, se muestra la existencia del robo de datos e información de acceso a sistemas informáticos.

CPF Capítulo I

Robo

Artículo 367.- Comete el delito de robo: el que se apodera de una cosa ajena mueble, sin derecho y sin consentimiento de la persona que puede disponer de ella con arreglo a la ley.

Artículo 368.- Se equiparan al robo y se castigarán como tal:

I.- El apoderamiento o destrucción dolosa de una cosa propia mueble, si ésta se halla por cualquier título legítimo en poder de otra persona y no medie consentimiento; y

II.- El uso o aprovechamiento de energía eléctrica, magnética, electromagnética, de cualquier fluido, o de cualquier medio de transmisión, sin derecho y sin consentimiento de la persona que legalmente pueda disponer de los mismos.

Artículo 369.- Para la aplicación de la sanción, se dará por consumado el robo desde el momento en que el ladrón tiene en su poder la cosa robada; aun cuando la abandone o lo desapoderen de ella. En cuanto a la fijación del valor de lo robado, así como la multa impuesta, se tomará en consideración el salario en el momento de la ejecución del delito.

Siendo importante mencionar que la información al ser transportada por energía, fluye junto con esta.

Posibles alcances del robo de datos

En la actualidad muchos son los ejemplos de ataques a sistemas empresariales y del Estado, los cuales han servido para desarrollar otros más, algunos como lo son *Stuxnet*[226] (que ataco a centrifugadoras para enriquecer uranio en Natanz Iran), *Petya*[227], *Wannacry* (randsomware que ataco a muchos sistemas

[226] Cfr., "Stuxnet es un gusano informático que afecta a equipos con Windows, descubierto en junio de 2010 por VirusBlokAda, una empresa de seguridad ubicada en Bielorrusia. Es el primer gusano conocido que espía y reprograma sistemas industriales", *https://es.wikipedia.org/wiki/Stuxnet*, de 31 de mayo de 2021.

[227] Cfr., "Petya es un malware de tipo ransomware reportado por la empresa Heise Security. Petya se esparce como troyano usando el popular sistema de archivos en la nube Dropbox.1 Mientras la mayoría de los malware de secuestro de computadoras selecciona los archivos a encriptar, Petya aumenta el daño potencial al impedir el arranque de la computadora". Petya (malware), *https://es.wikipedia.org/wiki/Petya_(malware)*, de 31 de mayo de 2021, 09:27 p.m.

corporativo de gran cantidad de empresas en el mundo), *Tryton* (malware para atacar específicamente sistemas industriales), *Crashoverride* (malware para atacar el sistema de distribución eléctrica de Ucrania), y muchos más que han vulnerado sistemas de control industrial.

Los creadores y desarrolladores de sistemas de robo de datos e información empresarial emigran a múltiples contextos y latitudes poniendo en práctica sus conocimientos, algunas veces en beneficio de empresa y del Estado, mientras que la mayoría de las veces proceden a compartir sus conocimientos con futuros desarrolladores de ataques y criminales informáticos, lo que pone en constante riesgo a miles de empresas que operan en la actualidad con sistemas de seguridad que la mayoría de las veces son débiles ante los ataques más sofisticados, como consecuencia del desconocimiento de operar actual de los atacantes, la infraestructura no adecuada ante los mismos, la no actualización de los protocolos de seguridad informática, y la mala aplicación de los sistemas de seguridad más avanzados.

Los delincuentes informáticos, al obtener los datos e información de las empresas del Estado y privadas, provocan una serie de afectaciones tanto económicas como morales a las mismas, dentro de los daños más comunes se encuentran las pérdidas económicas, secretos de producción industrial, y la confianza de sus consumidores, la reparación de daños con motivo de la perdida de información es constante en este tipo de delitos pues existe el compromiso de garantizar el uso y tratamiento de los mismos de forma responsable, el detrimento de su imagen y prestigio es uno de los principales objetivos de la competencia desleal. Intercambio y obtención de información que será compartida con otros delincuentes que en un futuro podría permitir el desarrollo de nuevas formas de intrusión y ataques informáticos.

Reglamentación

El Derecho Humano a la Autodeterminación Informativa definido, por el maestro español Pablo Murillo de la Cueva citado por Navarro, G, como “*el control que*

a cada uno de nosotros nos corresponde sobre la información que nos concierne personalmente, sea intima o no para preservar, de este modo y en último extremo, la propia identidad, nuestra libertad y dignidad… implica necesariamente poderes que permita a su titular definir los aspectos de su vida que nos sean públicos que desea que se conozcan, así como las facultades que le aseguren que los datos que de su persona manejan informáticamente terceros son exactos, completos, actuales y que se han obtenido de modo leal y lícito", que consiste, refiere el maestro español Pablo Murillo de la Cueva citado una vez más por Navarro, G., "*en la prerrogativa de la persona para disponer de la información que sobre sí misma exista en los registros de bases de datos, a fin de que esa información sea veraz, actualizada, no intrusiva y con las garantías de seguridad y uso conforme a la finalidad para la que fue proporcionada*".

El artículo 16, segundo párrafo de nuestra Constitución Política, norma el derecho que tienen las personas a la protección de sus datos, como se transcribe a continuación:

> *Toda persona tiene derecho a la protección de sus datos personales, al acceso, rectificación y cancelación de los mismos, así como a manifestar su oposición, en los términos que fije la ley, la cual establecerá los supuestos de excepción a los principios que rijan el tratamiento de datos, por razones de seguridad nacional, disposiciones de orden público, seguridad y salud públicas o para proteger los derechos de terceros*[228].

El derecho a la información debe ser garantizado por el Estado, con base en el artículo 6 de la CPEUM, que nos dice "*el derecho a la información será garantizado por el Estado*". En ese sentido el Estado será responsable de aplicar las leyes correspondientes que dan certeza jurídica al ciudadano, con el objetivo de garantizar y proteger la información, de conformidad con nuestra Constitución.

El Estado debe garantizar dicha protección, ante la responsabilidad en el tratamiento de datos de todos aquellos sujetos obligados pertenecientes al

[228] Artículo 19, CPEUM, op. cit.

orden federal, descritos por la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO) en su artículo 1, párrafo quinto, de la siguiente forma, "*Son sujetos obligados por esta Ley, en el ámbito federal, estatal y municipal, cualquier autoridad, entidad, órgano y organismo de los Poderes Ejecutivo, Legislativo y Judicial, órganos autónomos, partidos políticos, fideicomisos y fondos públicos*", y la responsabilidad de particulares, descritos en el artículo 2 de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP), "*sean personas física o morales de carácter privado que lleven a cabo el tratamiento de datos personales*", exceptuando a las siguientes: "*I. Las sociedades de información crediticia en los supuestos de la Ley para Regular las Sociedades de Información Crediticia y demás disposiciones aplicables, y II. Las personas que lleven a cabo la recolección y almacenamiento de datos personales, que sea para uso exclusivamente personal, y sin fines de divulgación o utilización comercial*", como norma el mismo ordenamiento en su artículo 2, numerales I y II.

Justificación

La justificación de la protección de los datos que son tratados por Empresas privadas y Órganos del Estado, como salvaguarda de la intimidad, privacidad y autodeterminación informativa, parte del daño real, actual e inminente que se causa ante la obtención, uso, tratamiento, trasmisión y transportación, ilegal de los mismos, lo que conlleva no solo a la protección de los datos de las personas físicas sino que de igual forma deben ser protegidos los datos de las personas morales, como refiere la tesis aislada P. II/2014 (10a.) de nombre *"Personas morales tienen derecho a la protección de los datos que puedan equipararse a los personales, aun cuando dicha información haya sido entregada a una autoridad"*:

> *El derecho a la protección de datos personales podría entenderse, en primera instancia, como una prerrogativa de las personas físicas, ante la imposibilidad de afirmar que las morales son titulares del derecho a la intimidad y/o a la vida privada; sin embargo, el contenido de este derecho puede extenderse a cierta información de las personas jurídicas colectivas, en tanto que también cuentan*

con determinados espacios de protección ante cualquier intromisión arbitraria por parte de terceros respecto de cierta información económica, comercial o relativa a su identidad que, de revelarse, pudiera anular o menoscabar su libre y buen desarrollo[229].

Al hablar de tratamiento de datos personales, nos encontramos ante procesos y operaciones, que con base en la LGDDPPSO, artículo 3, fracción XXXIII, se describen como "*Tratamiento: Cualquier operación o conjunto de operaciones efectuadas mediante procedimientos manuales o automatizados aplicados a los datos personales, relacionadas con la obtención, uso, registro, organización, conservación, elaboración, utilización, comunicación, difusión, almacenamiento, posesión, acceso, manejo, aprovechamiento, divulgación, transferencia o disposición de datos personales*[230]", aplicando las medidas de seguridad necesarias, entendidas conforme a la fracción XX del artículo y ley en comento como, "*conjunto de acciones, actividades, controles o mecanismos administrativos, técnicos y físicos que permitan proteger los datos personales*", lo que conlleva al tratamiento de datos personales junto a las medidas de seguridad necesarias para ello.

Las medidas de seguridad de los datos, deben tomar en cuenta las características de los mismos, partiendo de niveles que describen el valor e impacto que pueden llegar a tener en el poseedor de los mismos, por lo que se debe considerar, con base en el artículo 25 de la LDPPSOCDMX Ley de Protección de Datos Personales en Posesión de Sujetos Obligados de la Ciudad de México, los siguientes puntos, entre otros: I. Riesgo inherente a los datos personales tratados; II. Sensibilidad de los datos personales tratados; III. Desarrollo tecnológico; IV. Posibles consecuencias de una vulneración para los titulares; V. Transferencias de datos; VII. Vulneraciones previas ocurridas en los sistemas de datos; VIII. Riesgo por el valor potencial cuantitativo o cualitativo que pudieran tener los datos personales tratados para una tercera persona no autorizada para su posesión. En ese sentido, de igual manera las

[229] Tesis P. II/2014, op.cit.
[230] LGDDPPSO, artículo 3, fracción XXXIII y XX, op,cit.

medidas de seguridad que deberán ser adoptadas, tendrán con base en el artículo 25 los siguientes niveles de seguridad:

> *I. Básico: relativas a las medidas generales de seguridad cuya aplicación será obligatoria para el tratamiento y protección de todos los sistemas de datos personales en posesión de los sujetos obligados.*
>
> *II. Medio: se refiere a las medidas de seguridad requeridas para aquellos sistemas de datos relativos a la comisión de infracciones administrativas o penales, hacienda pública, servicios financieros, datos patrimoniales, así como los sistemas que contengan datos con los que se permita obtener evaluación de personalidad o perfiles de cualquier tipo en el presente pasado o futuro.*
>
> *III. Alto: corresponde a las medidas de seguridad aplicables a sistemas de datos concernientes a ideología, religión, creencias, afiliación política, origen racial o étnico, salud, biométricos, genéticos o vida sexual, así como los que contengan datos recabados para fines policiales, de seguridad, prevención, investigación y persecución de delitos.*

Tomar en cuenta el desarrollo tecnológico que debe ser aplicado en el tratamiento de datos, las consecuencias que conlleva la vulneración de los sistemas en su tratamiento, conforme al valor potencial cuantitativo o cualitativo e impacto en los titulares, permitirá que el sujeto obligado o el particular, que decidan sobre el tratamiento de los datos, busqué y deba adoptar estándares altos de seguridad en sus sistemas, ya que la evolución de técnicas, conductas y modos de operar que adquiere el delincuente informático, se ha potencializado con el desarrollo de sus conocimientos, acceso a novedosos sistemas informáticos (evolución constante de la tecnología), intercambio de conocimientos y técnicas informáticas con usuarios de la red, así como con otros delincuentes.

En ese sentido el Estado debe revisar y monitorear periódicamente que los estándares de seguridad en el tratamiento de datos personales, y extendiéndose a todo tipo de datos e información, como en el caso de los prestadores de servicios de almacenamiento de información en la nube (espacios de almacenamiento virtual en vez de físico), sean los adecuados.

Protocolos de seguridad dentro del tratamiento, almacenamiento y uso de datos

La delimitación correcta del protocolo de seguridad que deberá ser aplicado en el acceso, clasificación, protección, almacenamiento y resguardo, esto es, en todas y cada una de las etapas que comprenden tratamiento de datos, permitirá que la seguridad de la información sea mantenida con estándares adecuados conforme a las capacidades técnicas, en infraestructura y tecnológicas para su tratamiento, pues dicha seguridad es entendida y conceptualizada en la Estrategia Nacional de Ciberseguridad, como "*la capacidad de preservar la confidencialidad, integridad y disponibilidad de la información, así como su autenticidad, auditabilida, protección a la duplicación, no repudio y legalidad*[231]".

La importancia de unificar y homologar los protocolos de seguridad que las empresas del Estado, razones sociales, sujetos obligados, organismos e instituciones públicas y privadas, utilicen dentro del tratamiento, almacenamiento y uso de datos, como personas físicas y morales responsables, entendiéndose de igual forma como responsables a los proveedores de servicios[232], así, todos aquellos que se comprometen ante un contrato como responsables, encargados y usuarios, desarrolladores y diseñadores de programas, softwares y su encriptación, aplicaciones, etc., es lograr medidas de seguridad administrativas, técnicas y físicas necesarias en el contexto actual y futuro, de los datos y la información.

En nuestro país, se encuentra regulado el "documento de seguridad", en el cual se encuentran las medidas de seguridad que son implementadas por quienes son responsables del tratamiento de datos, los cuales con el fin de protegerlos contra daño, pérdida, alteración, destrucción o su uso, acceso o tratamiento no autorizado, deberán adoptarlo. La Ley General de Protección de Datos

[231] Estrategia Nacional de Ciberseguridad, op.cit.
[232] Cfr., Artículo1, fracción b, Convenio de Budapest, "Proveedor de servicios: i. toda entidad pública o privada que ofrezca a los usuarios de sus servicios la posibilidad de comunicar a través de un sistema informático, y ii. Cualquier otra entidad que procese o almacene datos informáticos para dicho servicio de comunicación o para los usuarios del mismo", op.cit.

Personales en Posesión de Sujetos Obligados, en relación al documento de seguridad como figura jurídica, en su artículo 3 fracción XIV, señala lo siguiente:

> *Artículo 3. Para los efectos de la presente Ley se entenderá por:*
>
> *XIV: Documento de seguridad: Instrumento que describe y da cuenta de manera general sobre las medidas de seguridad técnicas, físicas y administrativas adoptadas por el responsable[233] para garantizar la confidencialidad, integridad y disponibilidad de los datos personales que Posee.*

Mientras que la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, en su artículo 19, párrafo primero señala, "*Todo responsable que lleve a cabo tratamiento de datos personales deberá establecer y mantener medidas de seguridad administrativas, técnicas y físicas que permitan proteger los datos personales contra daño, pérdida, alteración, destrucción o el uso, acceso o tratamiento no autorizado*"[234].

De esta forma las medidas de seguridad administrativas, técnicas y físicas, tienen como objetivo primordial la protección de los datos personales, estas medidas son descritas en el Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, lo que con base en su artículo 2, fracciones V, VI y VII, se muestra a continuación:

> *V. Medidas de seguridad administrativas: Conjunto de acciones y mecanismos para establecer la gestión, soporte y revisión de la seguridad de la información a nivel organizacional, la identificación y clasificación de la información, así como la concienciación, formación y capacitación del personal, en materia de protección de datos personales;*
>
> *VI. Medidas de seguridad físicas: Conjunto de acciones y mecanismos, ya sea que empleen o no la tecnología, destinados para: a) Prevenir el acceso no autorizado, el daño o interferencia a las instalaciones físicas, áreas críticas de la organización, equipo e información; b) Proteger los equipos móviles, portátiles o de fácil remoción, situados dentro o fuera de las instalaciones; c) Proveer a los equipos que contienen o almacenan datos personales de un mantenimiento que asegure su disponibilidad, funcionalidad e integridad, y d) Garantizar la eliminación de datos de forma segura;*
>
> *VII. Medidas de seguridad técnicas: Conjunto de actividades, controles o mecanismos con resultado medible, que se valen de la tecnología para asegurar que: a) El acceso a las bases de datos lógicas o a la información en formato lógico sea por usuarios identificados y autorizados; b) El acceso referido en el*

[233] Cfr., Artículo 3, fracción XIV, LGPDPPSO, "Responsable: Persona física o moral de carácter privado que decide sobre el tratamiento de datos personales", op.cit.
[234] Artículo 19, primer párrafo, LFPDPPP, op.cit.

inciso anterior sea únicamente para que el usuario lleve a cabo las actividades que requiere con motivo de sus funciones; c) Se incluyan acciones para la adquisición, operación, desarrollo y mantenimiento de sistemas seguros, y d) Se lleve a cabo la gestión de comunicaciones y operaciones de los recursos informáticos que se utilicen en el tratamiento de datos personales[235].

Para la elaboración del documento de seguridad, conforme a la ley, el mismo debe contener y tomar en cuenta ciertos puntos esenciales, que con base en el artículo 28 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados de la Ciudad de México, se enuncian a continuación:

El responsable deberá elaborar el documento de seguridad que contendrá, al menos, lo siguiente: I. El inventario de datos personales en los sistemas de datos; II. Las funciones y obligaciones de las personas que intervengan en el tratamiento datos personales, usuarios y encargados, en el caso de que los hubiera; III. Registro de incidencias; IV. Identificación y autentificación; V. Control de acceso; gestión de soportes y copias de respaldo y recuperación; VI. El análisis de riesgos; VII. El análisis de brecha; VIII. Responsable de seguridad; IX. Registro de acceso y telecomunicaciones; X. Los mecanismos de monitoreo y revisión de las medidas de seguridad; XI. El plan de trabajo; y XII. El programa general de capacitación.

Dentro de los puntos relacionados con el análisis de brecha y riesgos, al ser realizados los mismos, sabremos cual es el riesgo real en el que se encuentran los sistemas informáticos, redes y aplicaciones, por lo que en la actualidad se vuelve indispensable realizar pruebas de penetración de forma recurrente, ya que las mismas nos permiten saber las capacidades físicas y tecnológicas con las que contamos.

Un ejemplo de los resultados que deberán entregarse a la empresa u organización, lo encontramos en la página de la empresa Kolibers, servicios de pruebas de penetración en México[236], en donde nos refieren que deben ser entregados los siguientes reportes:

Reporte Ejecutivo: Cómo se puede intuir en el nombre, el reporte ejecutivo se entrega a los ejecutivos de la organización y se explica en lenguaje no técnico los riesgos identificados y la mejor forma de solucionarlos, de esta forma la alta dirección podrá tomar decisiones informadas y aplicar sus presupuestos basados en riesgos.

Reporte Técnico: El reporte técnico se entrega al área de sistemas de la organización, donde se explica a detalle cada vulnerabilidad identificada, cómo

[235] Artículo 2, RLFPDPPP, op.cit.
[236] Kolibers, op.cit.

se identificó y cuál es la mejor manera de solucionarlas. Con esta información la parte técnica podrá resolver los riesgos en base al feedback de nuestros ingenieros, la alta dirección y sus objetivos y experiencia propia para que la organización saque el máximo provecho de las pruebas.

Justificación de la responsabilidad de la empresa al prestar sus servicios

El derecho a la vida, la libertad y seguridad de la persona o individuo, son derechos humanos consagrados en la Declaración Universal de Derechos Humanos, artículo 3, estos permiten que el individuo se desarrolle y exista dentro de la sociedad de manera libre, sin miedo, por lo que la seguridad que el Estado debe brindar, para garantizar ese desarrollo y existencia, es fundamental en la protección de los datos e información que posee, identifica y da identidad a cada individuo, ya que las Injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, así como los ataques a su honra o a su reputación, artículo 12 del mismo ordenamiento, son prohibidas, lo que conlleva a la protección de todo aquello que se relaciona con la persona dentro de la sociedad, y puesto que sus datos e información son parte de su propiedad, estos debe ser protegidos por las leyes, así con base en el artículo 17 de esta declaración, queda prohibido privar arbitrariamente al individuo de su propiedad, y por ende queda prohibido privar arbitrariamente al individuo de sus datos e información.

Si el principio de responsabilidad nos dice que los individuos deben responder por sus actos y decisiones, la decisión de tratar datos e información personal, debe tomar en cuenta los mecanismos establecidos en la LGPDPPSO en su artículo 30, no solo en la destinación de recursos que conllevan a políticas y programas de protección de datos personales, capacitación del personal sobre las obligaciones y deberes que estos adquieren, sino que de igual forma deben ser revisadas constantemente estas políticas y programas de seguridad, lo que resulta muy importante en relación con los sistemas informáticos como tecnología emergente, ya que las conductas positivas y negativas que se generan con los mismos, evolucionan y readaptan continuamente, siendo importante diseñar, desarrollar e implementar, sistemas o plataformas

informáticas, aplicaciones electrónicas o cualquier otra tecnología que implique el tratamiento de datos personales, garantizando el cumplimiento de las obligaciones previstas en la Ley General y las demás que resulten aplicables en la materia, con base en las fracciones VII y VIII del artículo y ordenamiento en comento, que como ya hemos visto, deberán ser protegidos por sistemas de seguridad con estándares adecuados.

En ese sentido, dentro de las categorías de información, tenemos la información reservada, que con base en el artículo 110 de la Ley Federal de Transparencia y Acceso a la Información Pública, fracciones I., IV., y VI., se considera que con su publicación, puede llegar a impactar, a las personas morales, la seguridad nacional y pública, poner en riesgo operaciones monetarias y operaciones financieras que realicen los sujetos obligados del sector público federal, así como la estabilidad de las instituciones financieras y obstrucción a las actividades de recaudación de los contribuyentes, siendo considerada como información confidencial la que con base en el artículo 116 de la Ley General de Transparencia y Acceso a la Información Pública, contiene datos personales concernientes a una persona identificada o identificable así como los secretos bancario, fiduciario, industrial, comercial, fiscal, bursátil y postal, cuya titularidad corresponda a particulares, sujetos de derecho internacional o a sujetos obligados cuando no involucren el ejercicio de recursos públicos, y de la cual "*sólo podrán tener acceso a ella los titulares de la misma, sus representantes y los Servidores Públicos facultados para ello", de igual forma "será información confidencial aquella que presenten los particulares a los sujetos obligados, siempre que tengan el derecho a ello, de conformidad con lo dispuesto por las leyes o los tratados internacionales*".

Bajo ese tenor confirmamos, lo que se mencionó con antelación, con base en la LFPDPPP, artículo 19, párrafo primero, "*todo responsable que lleve a cabo tratamiento de datos personales deberá establecer y mantener medidas de seguridad administrativas, técnicas y físicas que permitan proteger los datos personales contra daño, pérdida, alteración, destrucción o el uso, acceso o*

tratamiento no autorizado", prohibiendo a su vez que estos no adopten "*medidas de seguridad menores a aquellas que mantengan para el manejo de su información*".

Términos y condiciones de uso (permisos perpetuos e irrevocables)

Es importante que los términos y condiciones sean plasmados por quienes son proveedores de servicios, ya sea en la adquisición de un producto o la prestación de algún servicio, por lo que dichos términos y condiciones, serán lo que denomina la Ley Federal de Protección al Consumidor en su artículo 85, como contrato de adhesión, así "documento elaborado unilateralmente por el proveedor, para establecer en formatos uniformes los términos y condiciones aplicables a la adquisición de un producto o la prestación de un servicio, aun cuando dicho documento no contenga todas las cláusulas ordinarias de un contrato.

Todo contrato de adhesión celebrado en territorio nacional, para su validez, deberá estar escrito en idioma español y sus caracteres tendrán que ser legibles a simple vista y en un tamaño y tipo de letra uniforme. Además, no podrá implicar prestaciones desproporcionadas a cargo de los consumidores, obligaciones inequitativas o abusivas, o cualquier otra cláusula o texto que viole las disposiciones de esta ley".

La PROFECO, en nuestro país, derivado de las obligaciones del gobierno, debe luchar por la erradicación de malas prácticas que atentan contra los consumidores, principalmente cláusulas abusivas en los servicios bancarios, telefónicos, de prestaciones de servicios de internet, redes sociales, aplicaciones, plataformas, estos últimos como servicios virtuales en la red, pues un principio básico en las relaciones de consumo es, en términos del artículo primero fracción VII de la Ley Federal de Protección al Consumidor, "*la protección contra la publicidad engañosa y abusiva, métodos comerciales coercitivos y desleales, así como contra prácticas y cláusulas abusivas o impuestas en el abastecimiento de productos y servicios*".

Así los datos e información en la actualidad son activos que pueden ser manipulados y sobre todo, comercializados y explotados, por lo que los permisos perpetuos e irrevocables atentan contra estos, pues son trasmitidos, vendidos y usados por terceros, como en el caso de uso de credenciales (nombre de usuario y contraseña), quienes a su vez pueden negociarlos con otros prestadores de servicios, empresas, o quien tenga interés de poseer esos datos, dentro de estos términos encontramos el permiso que se otorga a las empresas de acceder a la información contenida en dispositivos electrónicos, lo que atenta contra la privacidad del sujeto y su información.

La Ley Federal de Protección al Consumidor en su artículo 78 Bis, fracciones de la I. a la VII., protege la seguridad de datos e información de los usuarios, ya que la protección al usuario (consumidor) es fundamental en la prestación de productos y servicios, destacando las relaciones entre proveedores y consumidores, así transacciones efectuadas a través del uso de medios electrónicos, ópticos o de cualquier otra tecnología, de esta forma "el proveedor utilizará la información proporcionada por el consumidor en forma confidencial, por lo que no podrá difundirla o transmitirla a otros proveedores ajenos a la transacción, salvo autorización expresa del propio consumidor o por requerimiento de autoridad competente"(fracción I), sin embargo esta autorización se adquiere de forma forzada ya que en el contexto actual, la dinámica de ritmo limita la lectura de estos, pues muchas veces son enormes, tediosas y con tecnicismos legales que limitan su entendimiento por parte de los usuarios.

En esta misma ley en términos de sus artículos 86 y 90, respecto a los contratos de adhesión, señala que la PROFECO será competente para resolver las controversias que se suscite sobre la interpretación o cumplimiento de los mismos, así como en qué casos no serán válidas ni se tendrán por puestas las cláusulas que los conforman, así "*La Secretaría, mediante normas oficiales mexicanas podrá sujetar contratos de adhesión a registro previo ante la Procuraduría cuando impliquen o puedan implicar prestaciones*

desproporcionadas a cargo de los consumidores, obligaciones inequitativas o abusivas, o altas probabilidades de incumplimiento" (art 86 primer párrafo), "*Los contratos de adhesión sujetos a registro deberán contener una cláusula en la que se determine que la Procuraduría será competente en la vía administrativa para resolver cualquier controversia que se suscite sobre la interpretación o cumplimiento de los mismos*" (artículo 86 tercer párrafo), artículo 90 fracciones I y III, que se relacionan con modificaciones unilaterales del contrato y traslado del consumidor a un tercero que no sea parte del contrato, de esta forma no serán válidas y se tendrán por no puestas las siguientes cláusulas de los contratos de adhesión ni se inscribirán en el registro cuando: I. Permitan al proveedor modificar unilateralmente el contenido del contrato, o sustraerse unilateralmente de sus obligaciones; III. Trasladen al consumidor o a un tercero que no sea parte del contrato la responsabilidad civil del proveedor.

Validación de documentos

La validación de documentos y firma electrónica, es importante en el contexto actual, ya que la virtualización de todas las transacciones contractuales, comerciales, de flujo de datos e información, etc., es inminente, lo que da paso a un sin número de plataformas y aplicaciones que realizan la validación de estos, por ejemplo la "firma.judicial", que como refiere el artículo 7, de los "Lineamientos para regular el uso de la firma electrónica certificada del Poder Judicial de la Ciudad de México", contenidos y modificados en la Circular CJCDMX-45/2020, del Poder Judicial de la Ciudad de México, de fecha 14 de diciembre de 2020[237], "los documentos electrónicos o digitales que cuenten con "Firma.Judicial" producirán los mismos efectos y tendrán el mismo trato que los presentados físicamente con firma autógrafa", pues como refiere el artículo 8 del mismo ordenamiento, esta es utilizada "para cualquier trámite que se realice ante el Poder Judicial, sea ante los Órganos jurisdiccionales del Tribunal o ante el Consejo, sólo se admitirá y validará la "Firma.Judicial", cuando no se haga

[237]Artículos 7, Circular CJCDMX-45/2020, op.cit.

uso del documento físico y la firma autógrafa", o como en el caso del sistema de "Validación de copias certificadas del Registro Civil del Distrito Federal del Gobierno de la Ciudad de México", en el que se validan las Actas de Nacimiento, así como el sistema de la RENAPO, en donde se consulta, emite y valida la Clave Única de Registro de Población (CURP).

Hoy en día es común la utilización de cifrados y encriptación[238], como método de protección y certeza jurídica en los documentos, ya que los "mensajes de datos", conceptualizados en el Código de Comercio en su artículo 89 como "*la información generada, enviada, recibida o archivada por medios electrónicos, ópticos o cualquier otra tecnología*", deben ser protegidos de tal forma que garanticen el contenido de los mismos, puesto que son utilizados, en términos del artículo 89 bis del mismo ordenamiento, como un "*medio probatorio en cualquier diligencia ante la autoridad legalmente reconocida, y surtirán los mismos efectos jurídicos que la documentación impresa*".

Plataformas (por medio de *block chain*), que generan certificados PSC (Prestador de Servicios de Certificación), generar programas con políticas y procedimientos revisados y autorizados, con ratificación del comité de ética, del director, presidentes (consentimiento en firma electrónica), encriptar la fecha en que se realizó el acuerdo. Para el trato, almacenamiento y uso de datos.

La seguridad de las transacciones electrónicas de todo tipo, como los contratos electrónicos, es de suma importancia en el contexto actual, lo que conlleva a tomar una serie de medidas que logren alcanzar la misma, así diferentes tecnologías de encriptación, permiten aumentar los niveles de seguridad en relación a la protección de datos e información, en ese tenor el Prestador de Servicios de Certificación, con base al artículo 89 del Código de Comercio, es "*la persona o institución pública que preste servicios relacionados con firmas electrónicas, expide los certificados o presta servicios relacionados como la conservación de mensajes de datos, el sellado digital de tiempo y la*

[238] Artículo, 89, CC, op.cit

digitalización de documentos impresos, en los términos que se establezca en la norma oficial mexicana sobre digitalización y conservación de mensajes de datos que para tal efecto emita la Secretaría", de esta forma son entidades autorizadas por la Secretaría de Economía que expiden certificados electrónicos y presta servicios relacionados con la firma electrónica.

Por su parte la página de "DocuSing"[239], nos señala, para mejor entender, los servicios que los Prestadores de Servicios de Certificación pueden dar, relacionados con el uso de la firma electrónica y que son los siguientes:

- Emisión de sellos digitales de tiempo[240]. También conocidos por su nombre en inglés como *timestamp,* los cuales garantizan la fecha y hora exacta en que un documento digital fue firmado, así como su existencia y vínculo con una entidad o persona.

- Constancias de conservación de mensajes de datos. Entendidas como "recibos digitales que señalan la existencia de un documento, así como de sus firmas, a partir de ciertas fechas", de igual manera nos dice que conforme a la Norma Oficial Mexicana NOM-151-SCFI-2016[241], Requisitos que deben observarse para la conservación de mensajes de datos y digitalización de documentos, "*una constancia de conservación de mensajes de datos es una serie de sellos digitales, emitidos por un PSC, que permiten verificar la fecha y hora de firma del documento electrónico*".

- Emisión de Certificados Electrónicos[242]. "*Documentos digitales que un PSC se encarga de garantizar su validez y vinculación de la entidad y su clave pública*".

[239] DocuSing, op.cit
[240] Artículo 89, CC, "Sello Digital de Tiempo: El registro que prueba que un dato existía antes de la fecha y hora de emisión del citado Sello, en los términos que se establezca en la norma oficial mexicana sobre digitalización y conservación de mensajes de datos que para tal efecto emita la Secretaría", op.cit.
[241] Norma Oficial Mexicana NOM-151-SCFI-2016, op.cit.
[242] Norma Oficial Mexicana NOM-151-SCFI-2016, op. cit.

- Digitalización certificada de documentos. "*Migrando los originales en papel al formato digital y asegurando su valor probatorio*".

Por otro lado, la protección de datos personales en el uso de *blockchain* parte del desarrollo de los ficheros y base de datos distribuidos en la red, lo que conlleva al ejercicio de los derechos ARCO (Acceso, Rectificación, Cancelación y Oposición), la legitimación de su tratamiento a lo largo de su ciclo de vida (desde que se obtiene o recaban hasta que son destruidos, borrados o eliminados), de conformidad con la LFPDPPP y su reglamento, basado en los principios de licitud, consentimiento, información, calidad, finalidad, lealtad, proporcionalidad y responsabilidad, así como los deberes de confidencialidad y seguridad, de igual forma se debe vincular, dentro de la cadena de bloques, el aviso de privacidad[243] en el que se deberá informar lo anterior, por medio del responsable de su tratamiento, persona física o moral, quien a su vez lo pondrá a disposición del titular de los datos, de esta forma, refiere Ocampo, M[244], las cadenas de bloque involucran "*el manejo de información personal, lo que despierta especial interés en los sistemas jurídicos, pues afecta el derecho humano a la protección de datos*".

Una FINTECH (finance-technology), es entendida como una empresa, personas físicas o morales, a través de la cual se prestan servicios del sector financiero, los cuales realizan sus negocios, servicios y transacciones por medio de plataformas electrónicas u/o medios electrónicos, en ese tenor la Ley para Regular las Instituciones de Tecnología Financiera, conocida en nuestro país como Ley FINTECH, en su artículo 4 fracción XVII[245], nos dice que define como "Modelo Novedoso", "aquel que para la prestación de servicios financieros utilice herramientas o medios tecnológicos con modalidades distintas a las existentes en el mercado al momento en que se otorgue la

[243] Cfr., Artículo 3, fracción I, LFPDPPP, "Aviso de Privacidad: Documento físico, electrónico o en cualquier otro formato generado por el responsable que es puesto a disposición del titular, previo al tratamiento de sus datos personales, de conformidad con el artículo 15 de la presente Ley", op. cit.
[244] Ocampo, M, op. cit.
[245] Artículo 4, fracción XVII, Ley para Regular las Instituciones de Tecnología Financiera, op. cit.

autorización temporal en términos de esta Ley", por lo que ello permitiría regular la cadena de bloques dentro de los servicios financieros, pues el *Blockchain* es una tecnología distinta a las existentes, reguladas normalmente en el mercado, sin embargo el futuro de la cadena de bloques, debe expandirse a todas aquellas posibilidades de aplicación determinadas en las diferentes áreas del quehacer de nuestro país, por lo que su regulación, tanto en el sector privado como público, dará mayor certeza jurídica a esta tecnología emergente.

***Cibergang*, pandillas y delincuencia organizada**

Los conceptos de pandilla, asociación delictuosa (banda) y delincuencia organizada, nos permitirán saber la posible integración de figuras delictivas que operan en las redes y sistemas informáticos a la normativa actual.

Pandillerismo

CPF, artículo 252, segundo párrafo

> *Se entiende que hay pandilla, cuando el delito se comete en común por tres o más personas, que se reúnen ocasional o habitualmente, sin estar organizados con fines delictuosos.*

De la interpretación textual es entendido que se configura el delito de pandillerismo, al reunirse tres o más personas de forma habitual, con el elemento de, sin estar organizados con fines delictuosos, esto es sin estar organizados con el propósito, al reunirse, de delinquir.

En esta figura jurídico penal, el hecho de reunirse de forma ocasional o habitualmente, sin estar organizados con fines delictuosos, no tiene mayor problema, pues la reunión de forma virtual no modifica el acto delictivo. Se define la asociación delictuosa con base en el artículo 164, primer párrafo del Código Penal Federal, "*Al que forme parte de una asociación o banda de tres o más personas con propósito de delinquir, se le impondrá prisión de cinco a diez años y de cien a trescientos días multa*". De la interpretación textual se desprende, que para configura la asociación delictuosa se necesita formar parte

de una asociación o banda de tres o más personas, con un elemento importante, el propósito de delinquir.

En esta figura jurídico penal, se adapta la asociación al hecho de relacionarse por medio de sistemas electrónicos y red, lo que permite una asociación delictuosa virtual con el propósito de delinquir, sin modificar el hecho delictuoso.

Al realizar la diferenciación de ambas figuras jurídicas penales, es orientadora la tesis aislada de jurisprudencia, No. 369, sostenida por la Primera Sala, localizada en la Séptima Época, página 174, publicada en el Semanario Judicial de la Federación, cuyo rubro y texto son:

> *Asociación delictuosa y pandillerismo. Sus diferencias (legislación del estado de Baja California).*
>
> *Hay claras notas distintivas entre el llamado pandillerismo y la asociación delictuosa. En el primero se trata de una reunión habitual, ocasional o transitoria de tres o más personas que sin estar organizadas con fines delictuosos, cometen comunitariamente algún ilícito; en cambio, la asociación delictuosa se integra también al tomar participación en una banda, tres o más personas, pero precisa que aquélla -la banda- esté organizada para delinquir. Aquí se advierte la primera distinción entre una y otra de las figuras analizadas: la consistente en que en el pandillerismo no hay organización con fines delictuosos, y en la asociación sí la hay. Pero todavía más: en esta segunda figura se requiere un régimen determinado con el propósito de estar delinquiendo, aceptado previamente por los componentes del grupo o banda; es decir, que debe haber jerarquía entre los miembros que la forman, con el reconocimiento de la autoridad sobre ellos del que la manda, quien tiene medios o manera de imponer su voluntad*[246]*.*

La delincuencia organizada, es establecida con base en el artículo 2 de la Ley Federal contra la Delincuencia Organizada[247], de la siguiente forma “las personas que se organicen de hecho para realizar, en forma permanente o reiterada, conductas que por sí o unidas a otras, tienen como fin o resultado cometer alguno o algunos de los delitos siguientes…”, así serán sancionadas por ese solo hecho, como miembros de la delincuencia organizada, de la interpretación textual tenemos para que sea configurada esta figura delictiva se necesitan los siguiente elementos, tres o más personas se organicen de hecho,

[246] Tesis aislada 369, op. cit.
[247] Artículo 2, Ley Federal contra la Delincuencia Organizada, op. cit.

que la organización sea en forma permanente o reiterada y que tenga como finalidad o resultado cometer alguno o algunos de los delitos que son señalados en el artículo en cuestión.

En esta figura jurídico penal, para poderla ampliar, no solo deben interactuar de forma virtual los delincuentes, sino de que igual manera en relación a los delitos informáticos, el catálogo de delitos que son señalados en el artículo referido, debe ser ampliado con delitos informáticos, ya que muchos de los mismos son cometidos por varios sujetos activos a la vez.

Hablar de delincuencia organizada en el ciberespacio o *cibergangs*, atacando sistemas informáticos, o aquellos equipos con funcionamiento informático, desde computadores, celulares, televisores inteligentes, hasta autos, refrigeradores, consolas de videojuegos, etc., es hablar de personas interconectadas desde diferentes puntos, estas redes de delincuencia emergentes, se conectan con más personas, por medio de foros y chats, actualizándose constantemente, entrando y saliendo de la Deep web y de la red invisible.

¿Se podría considerar que uno o más de un *bot* (persona falsa), que adquiere o adquieren autonomía por inteligencia artificial, como parte de una *ciberpandilla*?

Responsabilidad de quienes son partícipes del robo de datos

En múltiples delitos informáticos, partiendo de la “Teoría del dominio del hecho” de Claus Roxin, el autor es quien ejerce el dominio del hecho dirigiéndose a la realización del delito, el responsable del hecho, así en el tema que nos ocupa, el ciber-autor será quien tiene el dominio del hecho, esto es quien ataca o controla de forma virtual o remota al sistema, por ende el dominio del hecho lo realiza quien de forma virtual o remota ha manipulado o manipula el sistema, por lo que el usuario que se encuentra conectado, quien muchas de las veces ni se entera que su dispositivo fue usado para un ataque, no será quien tiene

el dominio del hecho sirviendo solo como medio para la realización del delito, en el caso de ingresar a un sistema sin autorización, pero cuando se ingresa con permiso y se comete el delito, sin que el usuario sea el autor, esto es sin que realice la acción y sin tener conocimiento del probable delito, en el entendido de que se utilizó el equipo por alguien al que se le permitió, el usuario sigue siendo el medio sin ser consciente de que su sistema fue usado en la comisión de un delito, por ello quien utiliza el sistema para cometer el delito será el autor y/o ciber-autor.

A menos que por medio del usuario, y con el consentimiento del mismo, se realice el ataque, como autor mediato (quien se sirve de otro para cometer el delito), en este caso quien tiene el dominio del hecho por medio de la voluntad, será el autor y/o ciber-autor, mientras quien realiza la acción al ejecutarla será el tercero utilizado como medio o instrumento, quien a su vez se encuentra controlado por el autor y/o ciber-autor, si el usuario no sabe realmente que está siendo utilizado para cometer un delito este no será autor (inimputable).

Por otra parte puede contratar a otra persona un autor intelectual (quien determina dolosamente a otro a cometer la conducta típica), al que le interesa la información, de este modo quien se contrata será el autor material al ser quien comete el delito, siendo determinado y actuando libremente por el contratante. En el caso de actuar bajo coacción (estando amenazado), quien tiene el dominio del hecho a través del dominio de la voluntad, será el autor y/o ciber-autor, ya que al ser utilizado, estando bajo amenazas, no será responsable ya que carece de la voluntad para llevar a cabo el delito.

Cuando la persona actúa bajo error, como en el caso de que se le pida enviar un correo electrónico a cierto individuo o empresa, sin saber que el archivo que se le ha pedido enviar contiene un *malware*, el autor material se encuentra dominado por quién género o inserto dicho malware en el archivo enviado por correo, esto es el que pide que envíe el correo, ejerciendo su voluntad por

medio de quien envió el mensaje, por lo que este último no será quien comete el delito.

Partiendo de que la coautoría se define como el acuerdo previo al que llegan los partícipes del hecho delictuoso, así como la división del trabajo y el aporte necesarios para la realización del delito, se sabe que cada partícipe tiene el dominio del hecho, por ello la tarea o parte asumida de forma individual es indispensable para la realización del hecho delictivo.

Al hablar de cooperadores necesarios, en relación al delito de falsificación (relacionado con el robo de datos e información), Martínez Arrieta, citado por Velazco[248], E, "*considera colaborador necesario por "aporte causal a la conducta típica*" de la duplicación de tarjetas, proporcionar el dato de poner en contacto con quien efectivamente después las clona, así como, en un claro ejercicio de división de funciones, tanto copiarlas, doblarlas como acometer informáticamente la incorporación de la banda magnética sustraída a otra tarjeta, ya que a partir de la primera conducta surge la potencialidad de crear dinero falso", por lo que, como refiere Martínez Arrieta, citado una vez más por Velazco, E, "*Se está en un caso de puesta en común de las voluntades de todos en un único y común proyecto delictivo, aunque cada integrante tenga diversos y distintos pero relevantes cometidos. Es un caso claro de coautoría*[249]".

Como podemos observar de lo anterior, en la actualidad se presentan dificultades para poder identificar a los autores de los delitos informáticos, si partimos de las pruebas presentadas en un proceso penal, es necesario un adecuado y minucioso estudio de los equipos informáticos y sistemas involucrados en el delito, derivado de la posibilidad de encriptación y la naturaleza inestable de los datos e información, así como de las técnicas aplicadas en el ocultamiento y borrado del ataque, sin olvidar la utilización de

[248] Velazco, Eloy, op.cit, p. 265.
[249] Velazco, Eloy, op.cit, p. 265.

direcciones IP dinámicas que permiten utilizar de forma temporal al usuario o manipular las direcciones IP, por lo que se torna necesaria una eficaz y adecuada autopsia forense del ordenador, sumada a una constante participación y promoción del desarrollo de la denominada “Informática Forense”, ya que si no se realiza de forma adecuada el estudio del sistema y equipo informático, podríamos inculpar a una o varias personas inocentes.

Las formas de autoría y participación contenidas en los ordenamientos jurídicos nacionales, como el de CDMX, se deben adaptar de manera correcta a los delitos informáticos, partiendo de las investigaciones resultado de la Informática Forense, sin olvidar la responsabilidad civil, penal y administrativa, que los “prestadores de servicios de la sociedad de la información” adquieren por sus actividades de intermediación, como en el caso de España, lo que se muestra a continuación, con base en el artículo 13 y demás correlativos, contenidos en la Sección Segunda innominada “Régimen de Responsabilidad”, de la Ley 34/2002[250], de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico: Artículo 13. Responsabilidad de los prestadores de los servicios de la sociedad de la información: 1. “Los prestadores de servicios de la sociedad de la información están sujetos a la responsabilidad civil, penal y administrativa establecida con carácter general en el ordenamiento jurídico, sin perjuicio de lo dispuesto en esta Ley”; y 2. “Para determinar la responsabilidad de los prestadores de servicios por el ejercicio de actividades de intermediación, se estará a lo establecido en los artículos siguientes”. Artículo 14. “Responsabilidad de los operadores de redes y proveedores de acceso”; Artículo 15. “Responsabilidad de los prestadores de servicios que realizan copia temporal de los datos solicitados por los usuarios”; Artículo 16. “Responsabilidad de los prestadores de servicios de alojamiento o almacenamiento de datos”; y Artículo 17. “Responsabilidad de los prestadores de servicios que faciliten enlaces a contenidos o instrumentos de búsqueda”.

[250] Ley 34/2002, op. cit.

Cooperación conjunta entre Estados en relación al fenómeno delictivo

En relación a los delitos informáticos y partiendo de los trabajos realizados por el Maestro Julio Téllez, el derecho penal contiene vacíos jurídicos, como se muestra a continuación.

> *… el derecho penal de los Estados involucrados contiene vacíos jurídicos y diferencias importantes susceptibles de obstaculizar la lucha contra la delincuencia organizada y el terrorismo, así como los graves ataques contra los sistemas de información perpetrados por particulares. La aproximación del derecho positivo en materia de delincuencia informática contribuirá a que las legislaciones nacionales sean lo suficientemente completas para que las graves formas de ataques contra los sistemas de información puedan ser objeto de investigaciones mediante técnicas y los métodos disponibles en derecho penal…*[251]

Con base en lo anterior damos cuenta, de la necesidad de unificar los criterios y legislaciones existentes en los Estados del globo, por lo que la cooperación entre estos debe permitir la lucha conjunta contra estos tipos de delitos, no sólo para entender los daños causados al/o bienes jurídicos, sino también su correcta investigación, ampliación de la jurisprudencia, sentencias y estudio del fenómeno delictivo, dentro y fuera de cada uno de los Estados en donde se ha cometido la afectación, lo que permitirá unificar toda la información entorno a los mismos.

En ese tenor es fundamental tomar en cuenta los estudios, resultados y consideraciones de la Oficina de Naciones Unidas contra la Droga y el Delito (UNODC), en la Reunión del Grupo de Expertos encargado de Realizar un Estudio Exhaustivo sobre el Delito Cibernético celebrada en Viena del 27 al 29 de julio de 2020[252], siendo algunas de ellas las siguientes:

- En alcance de la definición de “delito cibernético”, los Estados deberán tipificar como delito, los actos de ciberdelincuencia, quedando comprendidos

[251] Téllez, Julio, op. cit., p. 206.
[252] UNODC, op.cit.

los delitos basados en la cibernética y otros delitos que "*con frecuencia se cometen utilizando Internet y medios electrónicos (delitos facilitados por la cibernética), como el fraude cibernético, el robo cibernético, la extorsión, el blanqueo de dinero, el tráfico de drogas y armas, la pornografía infantil y actividades terroristas*".

- Mecanismos de cooperación internacional. Los Estados utilizaran o deberán adherirse a los "tratados multilaterales existentes que proporcionan una base jurídica para la prestación de asistencia judicial recíproca, como la Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional y el Convenio sobre la Ciberdelincuencia del Consejo de Europa" (Convenio sobre ciberdelincuencia, firmado en Budapest Hungría el 23 de noviembre de 2001 y entrando en vigor el 01 de julio de 2004), este último debería de usarse como referencia en la creación de capacidad y la asistencia técnica en todo el mundo.

- Entorno a las investigaciones de delitos cibernéticos "contar con socios estratégicos, como por ejemplo, los miembros de organizaciones existentes tales como la Organización de los Estados Americanos (OEA), el Grupo de los 7 y la Organización Internacional de Policía Criminal (INTERPOL)".

- Los Estados deberían estudiar la posibilidad de crear protocolos innovadores de intercambio de información, incluidas la información de inteligencia y las pruebas de actos delictivos, a fin de agilizar esos procedimientos.

- Es necesario "preparar un procedimiento operativo estándar, que sea aceptable internacionalmente, para la reunión y conservación de datos, y que pueda aplicarse en la escena de un delito".

- Los Estados Miembros "deberían intercambiar información sobre la forma en que se están resolviendo en el plano nacional los problemas para acceder de manera oportuna a las pruebas digitales".

- Los países “deberían mejorar la aplicación de las leyes nacionales y reforzar la coordinación y las sinergias a nivel interno para la reunión y el intercambio de información y pruebas con fines de enjuiciamiento”.

- Se los alienta a que “continúen o inicien reformas de la legislación sobre el delito cibernético y las pruebas electrónicas, siguiendo los ejemplos positivos y las reformas emprendidas en todo el mundo”.

- Se recomienda “elaborar marcos jurídicos que abarquen también los aspectos relacionados con la jurisdicción extraterritorial respecto de los actos de ciberdelincuencia”.

- Se recomienda crear un marco en el que quede claro que, en caso de “pérdida de la ubicación”, “la decisión de proceder con una investigación requiere un esfuerzo para establecer qué territorio ha sido afectado, dónde es vital la integridad de las redes automatizadas para poder realizar consultas sobre cuestiones de jurisdicción, y cuál es la forma más adecuada de continuar las indagaciones”.

- Los Estados deberían establecer un “mecanismo y un canal de comunicación de respuesta rápida para la asistencia judicial y la cooperación en materia de aplicación de la ley, y considerar la posibilidad de permitir el intercambio en línea de documentos jurídicos y pruebas electrónicas, con el apoyo de firmas electrónicas y otros medios técnicos”.

- La comunidad internacional debería “formular un procedimiento unificado para las técnicas de investigación de los delitos cibernéticos y mejorar las disposiciones de su legislación interna relativas a las obligaciones de los proveedores de servicios de Internet de conservar registros”.

La reforma a la legislación en torno al delito cibernético y las pruebas electrónicas, tomando ejemplos de leyes en otros países, actualiza los sistemas jurídicos y códigos penales que a la fecha convergen y son aplicados en cada Estado del Globo, lo cual retroalimenta el combate conjunto de los mismos.

Por su parte en el Convenio de Budapest, se enmarcan los principios generales relativos a la asistencia mutua, de esta manera con base al artículo 25, fracción 1, se establece la cooperación entre Estados en torno a “las investigaciones o de los procedimientos relativos a los delitos relacionados con sistemas y datos informáticos o con el fin de obtener pruebas en formato electrónico de un delito”.

Reglamentación

El Derecho a la seguridad en la información personal, se encuentra plasmado dentro de nuestra Constitución Política de los Estados Unidos Mexicanos, artículos 6 y 16, párrafo segundo, consagrándose de la siguiente forma, “*el derecho a la información será garantizado por el Estado*”, en armonía con el artículo 16[253], párrafo segundo.

> *Toda persona tiene derecho a la protección de sus datos personales, al acceso, rectificación y cancelación de los mismos, así como a manifestar su oposición, en los términos que fije la ley, la cual establecerá los supuestos de excepción a los principios que rijan el tratamiento de datos, por razones de seguridad nacional, disposiciones de orden público, seguridad y salud públicas o para proteger los derechos de terceros.*

De esta manera la protección de los datos personales, así como la seguridad en el tratamiento de los mismos, debe ser garantizada por el Estado, lo que conlleva a implementar todas aquellas medidas que deberán ser aplicadas por quienes realizan dicha labor.

En el siguiente cuadro, se destaca el posible hecho delictivo, así como la conducta antijurídica, siendo de suma importancia saber el tipo de sistema informático, señal y transporte de información, involucrado en la conducta antijurídica, de la siguiente forma:

[253] Artículos 6, 16, párrafo segundo, CPEUM, op.cit.

Ordenamiento	Hecho	Conducta	Tipo de sistema informático, señal y transporte de información.
Código Penal Federal, artículo 424 bis, fracción II.	Atentar contra los dispositivos electrónicos de protección de un programa de computación.	Fabricar con fines de lucro un dispositivo o sistema con el fin de desactivar dispositivos electrónicos de protección de un programa de computación. Fabricación de dispositivo o sistema, así fabricación de software o hardware.	*Atentar contra el Hardware*- Parte dura, física, material del sistema (dispositivo electrónico). Atentar contra la seguridad del *hardware*. Parte del sistema de seguridad. Sistema informático, en la fabricación. Dispositivo o sistema, así fabricación de software o hardware.
Acceso ilícito a sistemas y equipos de informática			
Código Penal Federal. Artículo 211 bis 1, primer párrafo.	Atentar contra la información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad.	Sin autorización modifique, destruya o provoque pérdida de información.	Atentar contra la información contenida en los sistemas informáticos, así contenida en el *hardware* (parte dura, física, material del sistema) y *software (*componente lógico, programa o aplicación programada para realizar tareas específicas). Se atenta primeramente contra el sistema de seguridad para después Atentar contra la información.
Código Penal Federal. Artículo 211 bis 1, segundo párrafo.	Atentar contra la información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad.	Sin autorización conozca o copie información.	Atentar contra la información contenida en los sistemas informáticos, así contenida en el *hardware* (parte dura, física, material del sistema) y *software (*componente lógico, programa o aplicación programado para

			realizar tareas específicas). Se atenta primeramente contra el sistema de seguridad para después Atentar contra la información.
Código Penal Federal. Artículo 211 bis 2, primer párrafo.	Atentar contra la información contenida en sistemas o equipos de informática del Estado, protegidos por algún mecanismo de Seguridad.	Sin autorización modifique, destruya o provoque pérdida de información del Estado.	Atentar contra la información contenida en los sistemas informáticos, así contenida en el *hardware* (parte dura, física, material del sistema) y *software (*componente lógico, programa o aplicación programado para realizar tareas específicas). Se atenta primeramente contra el sistema de seguridad para después Atentar contra la información.
Código Penal Federal. Artículo 211 bis 2, segundo párrafo.	Atentar contra la información contenida en sistemas o equipos de informática del Estado, protegidos por algún mecanismo de Seguridad.	Sin autorización conozca o copie Información del Estado.	Atentar contra la información contenida en los sistemas informáticos, así contenida en el *hardware* (parte dura, física, material del sistema) y *software (*componente lógico, programa o aplicación programado para realizar tareas específicas). Se atenta primeramente contra el sistema de seguridad para después Atentar contra la información.
Código Penal Federal. Artículo 211 bis 2, tercer párrafo.	Atentar contra información contenida en cualquier sistema, equipo o medio de almacenamiento	Sin autorización conozca, obtenga, copie o utilice información de seguridad pública.	Atentar contra la información contenida en los sistemas informáticos, así contenida en el *hardware* (parte dura,

	informático de seguridad pública.		física, material del sistema) y *software (*componente lógico, programa o aplicación programado para realizar tareas específicas). Se atenta primeramente contra el sistema de seguridad para después Atentar contra la información.
Código Penal Federal. Artículo 211 bis 3, primer párrafo.	Atentar contra la información contenida en sistemas y equipos de informática del Estado.	Estando autorizado para acceder a sistemas y equipos de informática del Estado, indebidamente modifique, destruya o provoque pérdida de información.	Atentar contra la información contenida en los sistemas informáticos, así contenida en el *hardware* (parte dura, física, material del sistema) y *software (*componente lógico, programa o aplicación programado para realizar tareas específicas). No atenta contra los sistemas de seguridad, ya que se encuentra autorizado.
Código Penal Federal. Artículo 211 bis 3, segundo párrafo.	Atentar contra la información contenida en sistemas y equipos de informática del Estado.	Estando autorizado para acceder a sistemas y equipos de informática del Estado, indebidamente copie información que contengan.	Atentar contra la información contenida en los sistemas informáticos, así contenida en el *hardware* (parte dura, física, material del sistema) y *software (*componente lógico, programa o aplicación programada para realizar tareas específicas). No atenta contra los sistemas de seguridad, ya que se encuentra autorizado.
Código Penal Federal. Artículo 211 bis 3, tercer párrafo.	Atentar contra la información contenida en sistemas y equipos de informática en	Estando autorizado para acceder a sistemas, equipos o medios de almacenamiento	Atentar contra la información contenida en los sistemas informáticos, así contenida en el

	materia de seguridad pública.	informáticos en materia de seguridad pública, indebidamente obtenga, copie o utilice información que contengan.	*hardware* (parte dura, física, material del sistema) y *software (*componente lógico, programa o aplicación programada para realizar tareas específicas). No atenta contra los sistemas de seguridad, ya que se encuentra autorizado.
Código Penal Federal. Artículo 211 bis 4, primer párrafo.	Atentar contra información contenida en sistemas o equipos de informática de las instituciones que integran el sistema financiero.	Sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática de las instituciones que integran el sistema financiero.	Atentar contra la información contenida en los sistemas informáticos, así contenida en el *hardware* (parte dura, física, material del sistema) y *software (*componente lógico, programa o aplicación programado para realizar tareas específicas). Se atenta primeramente contra el sistema de seguridad, el cual tienen que tener las instituciones que integran el sistema financiero, para después Atentar contra la información.
Código Penal Federal. Artículo 211 bis 4, segundo párrafo.	Atentar contra información contenida en sistemas o equipos de informática de las instituciones que integran el sistema financiero.	Sin autorización conozca o copie información contenida en sistemas o equipos de informática de las instituciones que integran el sistema financiero.	Atentar contra la información contenida en los sistemas informáticos, así contenida en el *hardware* (parte dura, física, material del sistema) y *software (*componente lógico, programa o aplicación programada para realizar tareas específicas). Se atenta primeramente contra el sistema de seguridad, el cual

			tienen que tener las instituciones que integran el sistema financiero, para después Atentar contra la información.
Código Penal Federal. Artículo 211 bis 5, primer párrafo.	Atentar contra información contenida en sistemas o equipos de informática de las instituciones que integran el sistema financiero.	Estando autorizado para acceder a sistemas y equipos de informática de las instituciones que integran el sistema financiero, indebidamente modifique, destruya o provoque pérdida de información que contengan.	Atentar contra la información contenida en los sistemas informáticos, así contenida en el *hardware* (parte dura, física, material del sistema) y *software (*componente lógico, programa o aplicación programado para realizar tareas específicas). No atenta contra los sistemas de seguridad, ya que se encuentra autorizado.
Código Penal Federal. Artículo 211 bis 5, segundo párrafo.	Atentar contra información contenida en sistemas o equipos de informática de las instituciones que integran el sistema financiero.	Estando autorizado para acceder a sistemas y equipos de informática de las instituciones que integran el sistema financiero, indebidamente copie información que contengan.	Se atenta contra la información contenida en los sistemas informáticos, así contenida en el *hardware* (parte dura, física, material del sistema) y *software (*componente lógico, programa o aplicación programado para realizar tareas específicas). No atenta contra los sistemas de seguridad, ya que se encuentra autorizado.
Delitos en materia de comunicación y correspondencia Ataques a las vías de comunicación Nota: transporte físico (como el cableado) y no físico (vía microonda, satelital, radiofrecuencia, infrarrojo, etc.)			
Código Penal Federal. Artículo 167, fracción VI.	Atentar contra las comunicaciones alámbricas, inalámbricas, o de fibra óptica, sean telegráficas, telefónicas o satelitales por	Dolosamente o con fines de lucro, interrumpa o interfiera las comunicaciones, alámbricas, inalámbricas o de fibra óptica, sean	Se atenta contra las comunicaciones alámbricas, inalámbricas, o de fibra óptica, sean telegráficas, telefónicas o satelitales por medio

	medio de las cuales se transfieran señales de audio, de video o de datos.	telegráficas, telefónicas o satelitales, por medio de las cuales se transfieran señales de audio, de video o de datos.	de las cuales se transfieran señales de audio, de video o de datos. Así contra el transporte físico (como el cableado) y no físico (vía microonda, satelital, radiofrecuencia, infrarrojo, etc.) Se atenta primeramente contra el sistema de seguridad, de las comunicaciones alámbricas, inalámbricas, o de fibra óptica, sean telegráficas, telefónicas o satelitales por medio de las cuales se transfieran señales de audio, de video o de datos, para después Atentar contra los datos e información (señales de audio, video o de datos).
Código Penal Federal. Artículo 168 bis, fracción I.	Atentar contra señales de telecomunicaciones distintas a las de satélite portadoras de programas.	Descifre o decodifique señales de telecomunicaciones distintas a las de satélite portadoras de programas.	Se atenta contra señales de telecomunicaciones distintas a las de satélite portadoras de programas (las cuales son inmateriales), así microonda, radiofrecuencia, infrarrojo. Se atenta primeramente (al descifrar o decodificar las señales) contra el sistema de seguridad de las señales de telecomunicaciones distintas a las de satélite portadoras de programas (las cuales son inmateriales), así microonda,

			radiofrecuencia, infrarrojo. Así como contra los datos e información de programas.
Código Penal Federal. Artículo 168 bis, fracción II.	Atentar contra las señales de telecomunicaciones distintas a las de satélite portadoras de programa.	Transmita la propiedad, uso o goce de aparatos, instrumentos o información que permitan descifrar o decodificar señales de telecomunicaciones distintas a las de satélite portadoras de programa.	Se atenta contra señales de telecomunicaciones distintas a las de satélite portadoras de programas (las cuales son inmateriales), así microonda, radiofrecuencia, infrarrojo. Se atenta primeramente (al descifrar o decodificar las señales) contra el sistema de seguridad de las señales de telecomunicaciones distintas a las de satélite portadoras de programas (las cuales son inmateriales), así microonda, radiofrecuencia, infrarrojo. Así como contra los datos e información de programas.
Código Penal Federal. Artículo 168 bis, fracción III.	Atentar contra una señal de satélite cifrada portadora de programas, originalmente codificados.	Reciba o distribuya una señal de satélite cifrada portadora de programas originalmente codificados, sin la autorización del distribuidor legal de la señal.	Se atenta contra una señal de satélite cifrada portadora de programas (la cual es inmaterial). Se atenta primeramente contra el sistema de seguridad de la señal de satélite cifrada portadora de programas originalmente codificados (la cual es inmaterial), al no ser autorizado por el distribuidor legal de la señal.

			Así como contra los datos e información de programas.
Código Penal Federal. Artículo 426, fracción I.	Atentar contra una señal de satélite cifrada portadora de programas.	Fabrique, modifique, importe, distribuya, venda o arriende un dispositivo o sistema para descifrar una señal de satélite cifrada, portadora de programas, sin autorización del distribuidor legítimo de dicha señal.	Dispositivo o sistema (hardware o software) con el fin de descifrar señal de satélite cifrada portadora de programas (la cual es inmaterial). Se busca atentar primeramente contra el sistema de seguridad de la señal de satélite cifrada, portadora de programas (la cual es inmaterial), al no ser autorizado el distribuidor legítimo de la señal. Así como contra los datos e información de programas.
Código Penal Federal. Artículo 426, fracción II.	Atentar contra una señal de satélite cifrada portadora de programas.	Realice con fines de lucro cualquier acto con la finalidad de descifrar una señal de satélite cifrada, portadora de programas, sin autorización del distribuidor legítimo de dicha señal.	Se busca atentar primeramente contra el sistema de seguridad de la señal de satélite cifrada, portadora de programas (la cual es inmaterial), al no ser autorizado el distribuidor legítimo de la señal. Así como contra los datos e información de programas.
Código Penal Federal. Artículo 426, fracción III	Atentar contra señal de cable encriptada portadora de programas.	Fabrique o distribuya equipo destinado a la recepción de una señal de cable encriptada portadora de programas, sin autorización del distribuidor legítimo de dicha señal…”	Dispositivo, no especifican de qué tipo, con el fin de desencriptar señal de cable encriptada portadora de programas (la cual es inmaterial). Se busca atentar primeramente contra el sistema de seguridad de la señal de cable portadora de programas (la cual es

			inmaterial), al no ser autorizado por el distribuidor legítimo de la señal. Así como contra los datos e información de programas.
Revelación de secretos y acceso ilícito a sistemas y equipos de informática **Revelación de secretos**			
Código Penal Federal. **Artículo 210**	Atentar contra algún secreto o comunicación reservada que conoce o ha recibido con motivo de su empleo, cargo o puesto.	Sin justa causa, con perjuicio de alguien y sin consentimiento del que pueda resultar perjudicado, revele algún secreto o comunicación reservada que conoce o ha recibido con motivo de su empleo, cargo o puesto.	No hace mención.
Código Penal Federal. **Artículo 211 Bis**	Atentar contra información o imágenes obtenidas en una intervención de comunicación.	Revele, divulgue o utilice indebidamente o en perjuicio de otro, información o imágenes obtenidas en una intervención de comunicación privada.	Se atenta contra una comunicación privada (la cual es inmateriales). Se atenta primeramente contra el sistema de seguridad de la comunicación privada (la cual es inmaterial). Así como contra los datos e información de comunicación privada.
Nota: Los artículos anteriores se relacionan con los considerados como delitos en la Ley Federal de Protección a la Propiedad Industrial, descritos en el artículo 402, fracciones III (Divulgar a un tercero un secreto industrial), IV (Apoderarse de un secreto industrial), V (Usar la información contenida en un secreto industrial) y VI (Apropiarse, adquirir, usar o divulgar indebidamente un secreto industrial).			
Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados. **Artículo 163, fracción III**	Atentar contra datos personales, que se encuentren bajo su custodia o a los cuales tengan acceso o conocimiento con motivo de su empleo, cargo o comisión.	Usar, sustraer, divulgar, ocultar, alterar, mutilar, destruir o inutilizar, total o parcialmente y de manera indebida datos personales, que se encuentren bajo su custodia o a los cuales tengan	No hace mención.

		acceso o conocimiento con motivo de su empleo, cargo o comisión	
Vulneraciones de seguridad			
Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados. Artículo 38, fracciones I, II, III y IV	Atentar contra la seguridad en cualquier fase del tratamiento de datos.	I. Pérdida o destrucción no autorizada; II. Robo, extravío o copia no autorizada; III. Uso, acceso o tratamiento no autorizado, o IV. Daño, alteración o modificación no autorizada.	No hace mención.
Ley Federal de Protección de Datos Personales en Posesión de los Particulares. Artículo 67.	Atentar contra la seguridad de las bases de datos.	Estando autorizado para tratar datos personales, con ánimo de lucro, provoque una vulneración de seguridad a las bases de datos bajo su custodia.	No especifica.
Ley Federal de Protección de Datos Personales en Posesión de los Particulares. Artículo 63 fracción XI.	Atentar contra la seguridad de bases de datos, locales, programas o equipos.	Vulnerar la seguridad de bases de datos, locales, programas o equipos, cuando resulte imputable al responsable.	Atentar contra sistemas informáticos, hardware (parte dura, física, material del sistema) y software (componente lógico, programa o aplicación programada para realizar tareas específicas). Se atenta contra el almacenamiento de los datos.
Delito informático			
Código Penal del Estado de Sinaloa, artículo 217, fracción I.	Atentar contra la base de datos, sistema de computadores o red de computadoras o contra cualquier parte de la misma.	Dolosamente y sin derecho: Usar o entrar a una base de datos, sistema de computadores o red de computadoras o a cualquier parte de la misma, con el propósito de diseñar, ejecutar o alterar un esquema	Atentar contra sistemas informáticos, hardware (parte dura, física, material del sistema) y software (componente lógico, programa o aplicación programada para realizar tareas específicas). Atentar contra el sistema de

		o artificio, con el fin de defraudar, obtener dinero, bienes o información.	computadores o red de computadoras (varios sistemas informáticos interconectados), así contra cualquier parte: sistemas informáticos, señales y conexión de los mismos. Atentar primeramente contra el sistema de seguridad. Atentar contra las bases de datos y por ende contra los datos e información.
Código Penal del Estado de Sinaloa, artículo 217, fracción II.	Atentar contra soporte lógico o programa de computadora o los datos contenidos en la misma, en la base, sistema o red	Dolosamente y sin derecho: Interceptar, interferir, recibir, usar, alterar, dañar o destruir un soporte lógico o programa de computadora o los datos contenidos en la misma, en la base, sistema o red.	Atentar contra sistemas informáticos, así como softwares (componente lógico, programa o aplicación programada para realizar tareas específicas) y *hardwares* (parte dura, física, material del sistema). Atentar contra el o los sistemas de seguridad. Atentar contra los datos. Atentar contra la base de datos. Atentar contra la red, (varios sistemas informáticos interconectados), así contra cualquier parte: sistemas informáticos, señales y conexión de los mismos.
Delito informático (fraude)			
Código Penal para el Distrito Federal, Artículo 231, fracción XIV.	Atentar contra los sistemas o programas de informática del sistema financiero. Atentar contra los activos: dinero o valores.	Obtener algún beneficio para sí o para un tercero, por cualquier medio que acceda, entre o se introduzca a los sistemas o programas de informática del sistema financiero e	Atentar contra el hardware (parte dura, física, material del sistema) y software (componente lógico, programa o aplicación programado para realizar tareas específicas).

		indebidamente realice operaciones, transferencias o movimientos de dinero o valores, independientemente de que los recursos no salgan de la Institución.	Atentar contra el o los sistemas de seguridad. Atentar contra los datos e información (activos: dinero o valores) contenida en los sistemas informáticos.
Ley de Instituciones de Crédito, artículo 112 Quáter, fracción I.	Atentar contra equipos o medios electrónicos, ópticos o de cualquier otra tecnología del sistema bancario mexicano. Atentar contra recursos económicos, información confidencial o reservada.	Acceder a los equipos o medios electrónicos, ópticos o de cualquier otra tecnología del sistema bancario mexicano, para obtener recursos económicos, información confidencial o reservada.	Atentar contra el hardware (parte dura, física, material del sistema) y software (componente lógico, programa o aplicación programado para realizar tareas específicas). Atentar contra el o los sistemas de seguridad. Atentar contra los medios ópticos (Medios que son leídos por un láser, así de almacenamiento) o de otra tecnología. Atentar contra los datos e información (contra recursos económicos, información confidencial o reservada).
Ley de Instituciones de Crédito, artículo 112 Quáter, fracción II.	Atentar contra el mecanismo de funcionamiento de los equipos o medios electrónicos, ópticos o de cualquier otra tecnología. Atentar contra el efectivo de los usuarios del sistema bancario mexicano, para obtener recursos económicos, información	Alterar o modificar el mecanismo de funcionamiento de los equipos o medios electrónicos, ópticos o de cualquier otra tecnología para la disposición de efectivo de los usuarios del sistema bancario mexicano, para obtener recursos económicos, información confidencial o reservada.”	Atentar contra el hardware (parte dura, física, material del sistema) y software (componente lógico, programa o aplicación programado para realizar tareas específicas). Atentar contra los medios ópticos o de otra tecnología (Medios que son leídos por un láser, así de almacenamiento). Atentar contra el o los sistemas de seguridad.

	confidencial o reservada.		Atentar contra los datos e información, (efectivo de los usuarios del sistema bancario mexicano, para obtener recursos económicos, información confidencial o reservada).

Derecho patrimonial sobre un programa de computación

Ley Federal de Derechos de Autor, Artículo 106, fracciones de la I a la V

> *El derecho patrimonial sobre un programa de computación comprende la facultad de autorizar o prohibir: I. La reproducción permanente o provisional del programa en todo o en parte, por cualquier medio y forma; II. La traducción, la adaptación, el arreglo o cualquier otra modificación de un programa y la reproducción del programa resultante; III. Cualquier forma de distribución del programa o de una copia del mismo, incluido el alquiler; IV. La decompilación, los procesos para revertir la ingeniería de un programa de computación y el desensamblaje, y V. La comunicación pública del programa, incluida la puesta a disposición pública del mismo[254].*

Al partir del concepto de Informática, podemos entender la terminología aplicada a la regulación de las tecnologías de la información, así lo relacionado a la conversión, almacenamiento, protección, procesamiento y transmisión de los datos e información, por lo que al entenderla como ciencia que estudia métodos, procesos y técnicas, con el fin de almacenar, procesar y transmitir información y datos en formato digital, sabremos que es referida no solo al sistema informático, el cual se conforma por el hardware, software y la parte humana, sino que de la misma forma la transmisión, recepción y envió de los datos e información, lo que se relaciona a su vez con los medios utilizados para ello, transporte físico (como el cableado) y no físico (vía microonda, satelital, radiofrecuencia, infrarrojo, etc.), en ese sentido las Leyes y Códigos mencionados en el cuadro anterior, nos refieren diversas series de elementos

[254] Artículo 106, fracciones I-V, LFDA, op.cit.

que forman parte de la informática y que son normados, así relacionados con conductas antijurídicas actualmente en nuestro país, como son los siguientes:

Código o Ley	Elementos que forman parte de la informática Tipo de sistema informático, señal y transporte de información.
Código Penal Federal, artículo 424 bis, fracción II.	"Dispositivos electrónicos de protección de un programa de computación". Sistema informático (Software y hardware).
Acceso ilícito a sistemas y equipos de informática	
Código Penal Federal. Artículo 211 bis 1, primer párrafo.	"Sistemas o equipos de informática protegidos por algún mecanismo de seguridad". Sistema informático (Software y hardware).
Código Penal Federal. Artículo 211 bis 1, segundo párrafo.	"Sistemas o equipos de informática protegidos por algún mecanismo de seguridad". Sistema informático (Software y hardware).
Código Penal Federal. Artículo 211 bis 2, segundo párrafo.	"Sistemas o equipos de informática del Estado, protegidos por algún mecanismo de Seguridad". Sistema informático (Software y hardware).
Código Penal Federal. Artículo 211 bis 2, tercer párrafo.	"Cualquier sistema, equipo o medio de almacenamiento informático de seguridad pública". Sistema informático (Software y hardware).
Código Penal Federal. Artículo 211 bis 3, primer párrafo.	"Sistemas y equipos de informática del Estado". Sistema informático (Software y hardware).
Código Penal Federal. Artículo 211 bis 3, segundo párrafo.	"Sistemas y equipos de informática del Estado". Sistema informático (Software y hardware).
Código Penal Federal. Artículo 211 bis 3, tercer párrafo.	"Sistemas y equipos de informática en materia de seguridad pública". Sistema informático (Software y hardware).
Código Penal Federal. Artículo 211 bis 4, primer párrafo.	"Sistemas o equipos de informática de las instituciones que integran el sistema financiero". Sistema informático (Software y hardware).
Código Penal Federal. Artículo 211 bis 4, segundo párrafo.	"Sistemas o equipos de informática de las instituciones que integran el sistema financiero". Sistema informático (Software y hardware).
Código Penal Federal. Artículo 211 bis 5, primer párrafo.	"Sistemas o equipos de informática de las instituciones que integran el sistema financiero". Sistema informático (Software y hardware).
Código Penal Federal. Artículo 211 bis 5, segundo párrafo.	"Sistemas o equipos de informática de las instituciones que integran el sistema financiero". Sistema informático (Software y hardware).
Delitos en materia de comunicación y correspondencia Ataques a las vías de comunicación Nota: transporte físico (como el cableado) y no físico (vía microonda, satelital, radiofrecuencia, infrarrojo, etc.)	
Código Penal Federal. Artículo 167, fracción VI.	"Comunicaciones alámbricas, inalámbricas, o de fibra óptica, sean telegráficas, telefónicas o satelitales".

	Transporte físico (como el cableado) y no físico (vía microonda, satelital, radiofrecuencia, infrarrojo, etc.)
Código Penal Federal. Artículo 168 bis, fracción I.	“Señales de telecomunicaciones distintas a las de satélite portadoras de programas”. Microonda, radiofrecuencia, infrarrojo o de otra tecnología.
Código Penal Federal. Artículo 168 bis, fracción II.	“Señales de telecomunicaciones distintas a las de satélite portadoras de programa”. Microonda, radiofrecuencia, infrarrojo o de otra tecnología. Aparatos e instrumentos: Sistema informático (Software y hardware).
Código Penal Federal. Artículo 168 bis, fracción III.	“Señal de satélite cifrada portadora de programas originalmente codificada”.
Código Penal Federal. Artículo 426, fracción I.	“Señal de satélite cifrada portadora de programas”.
Código Penal Federal. Artículo 426, fracción II.	“Señal de satélite cifrada portadora de programas”.
Código Penal Federal. Artículo 426, fracción III	“Señal de cable encriptada portadora de programas”.
Revelación de secretos y acceso ilícito a sistemas y equipos de informática **Revelación de secretos**	
Código Penal Federal. Artículo 211 Bis.	“Comunicación privada”. Señal de cualquier tipo.
Vulneraciones de seguridad	
Ley Federal de Protección de Datos Personales en Posesión de los Particulares. Artículo 63 fracción XI.	“Programas o equipos”. Sistema informático (Software y hardware).
Delito informático	
Código Penal del Estado de Sinaloa, artículo 217, fracción I.	“Sistema de computadores o red de computadoras o contra cualquier parte de la misma”. Sistema informático (Software y hardware). Sistema de computadores o red de computadoras (varios sistemas informáticos interconectados), así contra cualquier parte: sistemas informáticos, señales y conexión de los mismos (alámbrica o inalámbrica).
Código Penal del Estado de Sinaloa, artículo 217, fracción II.	“Soporte lógico o programa de computadora”. “Sistema o red”. Sistema informático (Software y hardware). Sistema de computadores o red de computadoras (varios sistemas informáticos interconectados), así contra cualquier parte: sistemas informáticos, señales y conexión de los mismos (alámbrica o inalámbrica).
Delito informático (fraude)	
Código Penal para el Distrito Federal, Artículo 231, fracción XIV.	“Sistemas o programas de informática del sistema financiero”. Sistema informático (Software y hardware).
Ley de Instituciones de Crédito, artículo 112 Quáter, fracción I.	“Equipos o medios electrónicos, ópticos o de cualquier otra tecnología del sistema bancario mexicano”.

	Medios ópticos (Medios que son leídos por un láser, así de almacenamiento) o de otra tecnología. Sistema informático (Software y hardware).
Ley de Instituciones de Crédito, artículo 112 Quáter, fracción II.	"Mecanismo de funcionamiento de los equipos o medios electrónicos, ópticos o de cualquier otra tecnología". Medios ópticos (Medios que son leídos por un láser, así de almacenamiento) o de otra tecnología. Sistema informático (Software y hardware).

En ese sentido podemos dar cuenta que en el ámbito del procesamiento, transmisión, recepción y envió de los datos e información, la normativa nacional revisada es aplicada en las siguientes vertientes: 1. Sistema informático (software y hardware); 2. Medios de almacenamiento (Medios ópticos que son leídos por un láser de almacenamiento); 3. Sistema de computadores o red de computadoras (varios sistemas informáticos interconectados); 4. Señal (de cualquier tipo así microonda, radiofrecuencia, infrarrojo o de otra tecnología); y 5. Medios de transportación (comunicaciones alámbricas, inalámbricas, o de fibra óptica, sean telegráficas, telefónicas o satelitales).

De esta manera las vertientes mencionadas, son fundamentales en la tipificación del delito de robo de datos e información, el cual no solo debe entendido como una vulneración de seguridad en el tratamiento de datos e información, sino que de igual manera como parte fundamental que afecta los procesos que se realizan en torno a los mismos, así como parte del procesamiento, transmisión, recepción y envió, por medio de estos: sistema informático, medio de almacenamiento material y virtual (nube), sistema de computadores o red de computadoras, señal y medios de transportación (para señal, datos e información), sino también como el daño que al patrimonio y a la persona misma (derechos de la persona) se realiza, lo que conlleva a buscar ampliar la protección de los datos e información, y con ello ampliar la protección de los bienes jurídicos relacionados con la persona física, moral o entes del Estado.

La Ley 1273 de 2009, en su artículo 269I, con la que se adiciona el Código Penal Colombiano, nos refiere el denominado "Hurto por medios informáticos y semejantes", en el cual nos habla de la violación de las medidas de seguridad informáticas, lo que ha sido señalado como primera parte de lo que será un ingreso no autorizado o intrusión, para después realizar el hurto.

> *Hurto por medios informáticos y semejantes. El que, superando medidas de seguridad informáticas, realice la conducta señalada en el artículo 239*[255] *manipulando un sistema informático, una red de sistema electrónico, telemático u otro medio semejante, o suplantando a un usuario ante los sistemas de autenticación y de autorización establecidos, incurrirá en las penas señaladas en el artículo 240 de este Código.*

El artículo en comento no solo refiere la violación de las medidas de seguridad informáticas, sino que de igual forma señala la manipulación de un sistema informático, una red de sistema electrónico, telemático u otro medio semejante, o suplantando a un usuario ante los sistemas de autenticación y de autorización, como medio para lograr el objetivo, lo que conlleva a la posible decodificación y vulneración de los sistemas de protección, deteniéndonos en la suplantación de un usuario ante los sistemas de autenticación y de autorización, ya que esto último afecta la esfera jurídica de quien ha sido suplantado (usurpación de identidad, artículo 211 Bis del CPDF), pues se puede adjudicar de manera errónea el delito, si no se realiza la correcta investigación.

De la protección y seguridad que debe ser brindada por el Estado, y en relación a los delitos informáticos, nos encontramos ante dos vertientes, la primera en la que se busca adecuar las figuras jurídico penales tradicionales como el robo,

[255] Cfr., Código Penal Colombiano, LEY 599 DE 2000. Artículo 239. "Hurto. El que se apodere de una cosa mueble ajena, con el propósito de obtener provecho para sí o para otro, incurrirá en prisión de dos (2) a seis (6) años. La pena será de prisión de uno (1) a dos (2) años cuando la cuantía no exceda de diez (10) salarios mínimos legales mensuales vigentes", po.cit.
Cfr., Artículo 240. "Hurto calificado. La pena será prisión de tres (3) a ocho (8) años, si el hurto se cometiere: 1. Con violencia sobre las cosas; 2. Colocando a la víctima en condiciones de indefensión o inferioridad o aprovechándose de tales condiciones; 3. Mediante penetración o permanencia arbitraria, engañosa o clandestina en lugar habitado o en sus dependencias inmediatas, aunque allí no se encuentren sus moradores; 4. Con escalamiento, o con llave sustraída o falsa, ganzúa o cualquier otro instrumento similar, o violando o superando electrónicas u otras semejantes. La pena será prisión de cuatro (4) a diez (10) años cuando se cometiere con violencia sobre las personas. Las mismas penas se aplicarán cuando la violencia tenga lugar inmediatamente después del apoderamiento de la cosa y haya sido empleada por el autor o partícipe con el fin de asegurar su producto o la impunidad", op.cit.

a las nuevas modalidades delictivas, y en el tema que nos ocupa, robo de datos e información, se encontró que como señala el maestro Julio Téllez Valdés.

> *… si se insiste en adecuar las figuras jurídico-penales tradicionales como el robo a esta nueva modalidad delictiva, se tendrán entonces que modificar dos conceptos: el de "apoderamiento" en el que se considere no sólo el desposeimiento del bien, sino también la disminución de su valor; y el de "bien mueble" en el que se incluyan bienes intangibles como la información que sí per se es susceptible de apropiación, también per se, debe ser susceptible de protección jurídica…*[256]

Así, tenemos que la información es un bien intangible, el cual aunque puede ser materializado, como en el caso de los activos que al ser usados se obtiene un producto o servicio, en los sistemas informáticos se encuentra como bien intangible, esto es un bien virtual un bien intangible (como las criptomonedas).

La otra vertiente parte de la necesidad de crear nuevas figuras jurídico penales, las cuales en el contexto actual, son necesarias por la variedad de técnicas y conductas criminales que emergen y han emergido de este fenómeno delictivo, sin embargo para poder cubrir la necesidad de protección jurídico penal del o los bienes protegidos por el Estado, ante la transición de lo material a lo virtual, considero que se deben adoptar ambas vertientes, lo que permitirá ampliar el espectro de protección de la norma jurídico penal, adaptando y reformando las normas ya establecidas, y creando un posible Código Penal Federal de Delitos Informáticos y/o relacionados con los sistemas informáticos, en el cual existirán y se tipificaran las conductas delictivas relacionadas con este tipo de sistemas.

De la revisión de las conductas que se relacionan con el delito de robo de datos, dentro de la normativa nacional propuesta para revisar, encontramos lo siguiente:

ORDENAMIENTO	ARTÍCULO	CONDUCTA
Código Penal Federal	367. “Comete el delito de robo: el que se apodera de una cosa ajena mueble,…”	Apoderar-“… sin derecho y sin consentimiento de la persona que

[256] Téllez Valdés, Julio, op. cit.

		puede disponer de ella con arreglo a la ley.”
Código Penal Federal	Artículo 211 bis 2, tercer párrafo. “A quien sin autorización conozca, obtenga, copie o utilice”;	Conozca, obtenga, copie o utilice- Sin autorización, “…información contenida en cualquier sistema, equipo o medio de almacenamiento informáticos de seguridad pública…”
Código Penal Federal	Artículo 211 bis 3, tercer párrafo. “A quien estando autorizado para acceder a sistemas, equipos o medios de almacenamiento informáticos en materia de seguridad pública, indebidamente…”	Obtener indebidamente , “…obtenga, copie o utilice información que contengan…”
Código Penal Federal	Artículo 168 bis, fracción III. “Reciba o distribuya una señal de satélite cifrada portadora de programas originalmente codificada, sin la autorización del distribuidor legal de la señal…”;	Recibir o distribuir- sin autorización del distribuidor legal, “Reciba o distribuya una señal de satélite cifrada portadora de programas originalmente codificada…”
Código Penal Federal	Artículo 167, fracción VI. “Al que dolosamente o con fines de lucro,”	Interrumpir e interferir, dolosamente o con fines de lucro, “…interrumpa o interfiera las comunicaciones, alámbricas, inalámbricas o de fibra óptica, sean telegráficas, telefónicas o satelitales, por medio de las cuales se transfieran señales de audio, de video o de datos…”
Ley Federal de Protección a la Propiedad Industrial	Artículo 402, fracciones III, IV, V y VI. Artículo 402.- Son delitos:	III – Divulgar, a un tercero, un secreto industrial. IV – Apoderarse, de un secreto industrial. V – Usar, la información contenida en un secreto industrial. VI - Apropiarse, adquirir, usar o divulgar, indebidamente un secreto industrial.
Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados	Artículo 38, fracción II “Además de las que señalen las leyes respectivas y la normatividad aplicable, se considerarán como vulneraciones de seguridad, en cualquier fase del tratamiento de datos, al menos, las siguientes:”	Conductas que serán causa de sanción, aquellas que atenten o pongan en riesgo total o parcialmente los datos, siendo responsable de su custodia: “II. El robo, extravío o copia no autorizada;”

Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados	Artículo 163, fracción III, "… total o parcialmente y de manera indebida datos personales, que se encuentren bajo su custodia o a los cuales tengan acceso o conocimiento con motivo de su empleo, cargo o comisión".	Conductas que serán causa de sanción y que atenten o pongan en riesgo total o parcialmente los datos de manera indebida, "… Usar, sustraer, divulgar, ocultar, alterar, mutilar, destruir o inutilizar…"
Código Penal del Estado de Sinaloa	Artículo 217. Fracción I, "Comete delito informático, la persona que dolosamente y sin derecho:" "I., con el fin de defraudar, obtener dinero, bienes o información"	Usar o entrar, Dolosamente, con el fin de defraudar, obtener dinero, bienes o información, "Use o entre a una base de datos, sistema de computadores o red de computadoras o a cualquier parte de la misma, con el propósito de diseñar, ejecutar o alterar un esquema o artificio…"
Ley de Instituciones de Crédito	Artículo 112 Quáter, fracciones I y II. "…al que sin causa legítima o sin consentimiento de quien esté facultado para ello…"	Sin causa legitima y sin consentimiento: Acceder o modificar. I "Acceda a los equipos o medios electrónicos, ópticos o de cualquier otra tecnología del sistema bancario mexicano, para obtener recursos económicos, información confidencial o reservada,) Alterar, obtener. II "Altere o modifique el mecanismo de funcionamiento de los equipos o medios electrónicos, ópticos o de cualquier otra tecnología para la disposición de efectivo de los usuarios del sistema bancario mexicano, para obtener recursos económicos, información confidencial o reservada.

El delito de robo que con base en el artículo 367 del CPF, nos señala que el apoderarse de una cosa ajena mueble, sin derecho y sin consentimiento de la persona que puede disponer de ella con arreglo a la ley, limita su aplicación al referir "cosa ajena mueble", ya que los datos e información deben ser especificados, lo que por su parte se equipara al robo en el artículo 368 fracción II del mismo ordenamiento, que nos dice "*el uso o aprovechamiento de energía eléctrica, magnética, electromagnética, de cualquier fluido, o de cualquier*

medio de transmisión, sin derecho y sin consentimiento de la persona que legalmente pueda disponer de los mismos", del cual encontramos como conducta antijurídica el uso o aprovechamiento.

Sin embargo al detenernos a revisar, en la mención de "por medio de cualquier fluido y cualquier medio de transmisión", se puede estar ante un vació jurídico al no precisar qué se trata de datos e información, ya que si bien se ha demostrado que la información puede viajar, ser transmitida y fluir por medio de diversas señales (de cualquier tipo así microonda, radiofrecuencia, infrarrojo o de otra tecnología), siendo transportada por diferentes medios (comunicaciones alámbricas, inalámbricas, o de fibra óptica, sean telegráficas, telefónicas o satelitales), al no precisar qué se trata de datos e información, por la complejidad que se relaciona con la parte intangible y virtual de estos, debido a la prohibición de analogías en los juicios del orden criminal, decretada en el artículo 14, párrafo segundo de nuestra carta magna, nos vemos en la necesidad de especificar el robo de datos e información, no como una conducta antijurídica equiparada, sino como una conducta que debe ser plasmada de manera especial por la esencia y complejidad de los delitos informáticos.

Por su parte las conductas obtener, copiar, utilizar, recibir, distribuir, interrumpir, interferir, divulgar, adquirir, usar, extraviar, alterar, mutilar, destruir e inutilizar, de manera dolosa y sin autorización, relacionadas con el procesamiento, transmisión, recepción y envió de datos e información, son conductas que dañan al bien jurídico al filtrar la información y por ende vulnerar, lo que conlleva a exponerla.

Sin embargo el robo de datos e información si bien permite su vulneración, como esencia de los delitos informáticos en el momento en que se accede a los datos e información, y si estos son entendidos como "representaciones simbólicas, las cuales al ser manipuladas por medio de un computador y/o sistema informático, darán paso a la información", la información que es

intercambiada, con el simple hecho de acceder a la conexión del sistema, será utilizada y permitirá la intrusión al mismo.

Diferencia entre técnica (modo de operar) y delito informático

Del estudio de las técnicas utilizadas en los delitos informáticos, y partiendo del hecho de utilizar reglas para dirigir un ataque, acceso no autorizado, intrusión o simplemente obtener la información necesaria para poder ingresar de forma más eficaz, estudiando al o los objetivos, ya sea sistema, equipo, una señal o red, etc., damos cuenta de la forma en que operan los delincuentes informáticos.

En ese sentido el delito informático, retomando el concepto típico que nos enseña el maestro Julio Téllez[257], serían las "*conductas típicas, antijurídicas y culpables que tiene a las computadoras como instrumento o fin*", lo que conlleva a inferir que las computadoras al ser uno de los principales sistemas informáticos que han permitido el tratamiento y procesamiento de datos e información, es el principal sistema informático en estudio

Sin embargo como hemos podido dar cuenta, estos delitos se extienden a todo tipo de sistema informático (televisores, vehículos inteligentes, casas y ciudades inteligentes, sistemas de videojuegos, etc.), ya que estos utilizan los principios de procesamiento de datos e información de las computadoras, lo que además se amplía y complementa con otros elementos esenciales dentro del procesamiento, transmisión, recepción y envió de los datos e información, como son los medios de almacenamiento, sistema de computadores o red de computadoras –red de sistemas informáticos-, señal y medios de transportación de esta.

Las técnicas y conductas que atentan contra los bienes jurídicos, que partiendo del concepto típico del delito, expuesto por el maestro Julio Téllez, pueden ser ampliadas a los sistemas informáticos, retomando los resultados de la

[257] Téllez, Julio, op. cit., p. 188.

investigación, de la siguiente forma, “conductas típicas, antijurídicas y culpables que tienen a los sistemas informáticos, medios de almacenamiento, sistemas de computadores o red de computadoras –red de sistemas informáticos-, señal y medios de transportación de esta, así como cualquier tecnología presente y futura relacionada con el procesamiento, transmisión, recepción y envió de los datos e información, como instrumento o fin”, en ese sentido la ampliación propuesta se conjuga con el hecho de ser utilizados como instrumento o fin, por lo que se establece de la siguiente forma:

> **1. Como instrumento (medio)**. Se utilizan los sistemas informáticos, medios de almacenamiento, sistemas de computadores o red de computadoras –red de sistemas informáticos-, señal y medios de transportación de esta, así como cualquier tecnología presente y futura relacionada con el procesamiento, trasmisión, recepción y envió de los datos e información, como medio para cometer el delito (como en el uso no autorizado de programas de cómputo, alteración en el funcionamiento de los sistemas, intervención en las líneas de comunicación de datos o teleproceso, modificación de datos tanto en la entrada como en la salida, etc.).
>
> **2. Como fin.** Los sistemas informáticos, medios de almacenamiento, sistemas de computadores o red de computadoras –red de sistemas informáticos-, señal y medios de transportación de esta, así como cualquier tecnología presente y futura relacionada con el procesamiento, trasmisión, recepción y envió de los datos e información, son el objetivo (como en la programación de instrucciones que producen un bloqueo total al sistema, destrucción de programas por cualquier método y secuestro de soportes magnéticos en los que figure información valiosa con fines de chantaje, pago de rescate, etc.).

Cómo analizar el robo de datos desde la normativa actual

El robo de datos e información, se relaciona con diferentes conductas delictivas descritas y tipificadas en nuestro ordenamiento jurídico mexicano, en ese sentido, es importante tomar como base nuestra Carta Magna, las leyes federales y los tratados Internacionales, (artículo 133 de la CPEUM).

Las conductas relacionadas con los delitos informáticos, equiparadas al robo de acuerdo con la legislación penal, señaladas en la página de Justia México, en nuestro país son las siguientes: apoderamiento material o por medios

electrónicos, de documentos que contengan datos de computadoras o el aprovechamiento o utilización de esos datos, sin derecho y sin consentimiento de la persona que legalmente pueda disponer de los mismos; apoderamiento o uso indebido de tarjetas de crédito o débito expedidas por Instituciones Bancarias o de cualquier otra naturaleza o de títulos de crédito o documentos auténticos que sirvan para el pago de bienes o servicios o para obtener dinero efectivo sin el consentimiento de quien tenga derecho a disponer de tal instrumento.

Otras conductas, mencionadas y no mencionadas con antelación, establecidas en el Código Penal Federal, códigos penales de las entidades federativas y legislaciones especiales, que se relaciona al robo de datos e información son las siguientes: Revelación de secretos y acceso ilícito a sistemas y equipos de informática; Ataques a las vías de comunicación, transporte físico (como el cableado) y no físico (vía microonda, satelital, radiofrecuencia, infrarrojo, etc.); Vulneraciones de seguridad; Acoso sexual, Alteración o manipulación de medios de identificación electrónica; Delitos contra la indemnidad de privacidad de la información sexual; Delitos en materia de derechos de autor (como afectar un programa de cómputo o software); Engaño telefónico; Falsificación de títulos; Pornografía; Suplantación de Identidad; Delito equiparado al robo.

Estas conductas se encuentran en algunos de los siguientes ordenamientos: Código Penal Federal, Código Penal del Estado de Sinaloa, Ley de Instituciones de Crédito, Ley de Instituciones de Seguros y de Fianzas, Ley del Mercado de Valores, Ley General de Títulos y Operaciones de Crédito, Ley Federal de Protección de Datos Personales en Posesión de los Particulares, Ley Federal de protección a la Propiedad Industrial, Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, Código Penal para el Distrito Federal, entre otros.

Los elementos que integran los sistemas informáticos, medios de almacenamiento, sistemas de computadores o red de computadoras –red de

sistemas informáticos-, señal y medios de transportación de la misma, utilizados como medio o fin, al ser los principales objetivos del robo de datos e información, son quienes deben ser protegidos de forma especial por la normativa nacional, lo que conlleva a establecer categorías de delitos y conductas delictivas, como las descritas en el Convenio sobre la Ciberdelincuencia del Consejo de Europa o Convenio de Budapest, de la siguiente forma: 1. Delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos (art 2. Acceso ilícito, art 3. Interceptación ilícita, art 4. Ataques a la integridad de los datos, art 5. Ataques a la integridad del sistema, art 6. Abuso de los dispositivos); 2. Delitos informáticos. Cometidos mediante el uso de las tecnologías de la información y las telecomunicaciones (art 7. Falsificación informática, art 8. Fraude informático); 3. Delitos relacionados con el contenido (art 9. Delitos relacionados con la pornografía infantil); 4. Delitos relacionados con infracciones de la propiedad intelectual y de los derechos afines (derechos de autor).

Otro ejemplo de conductas que se relacionan con los delitos informáticos, robo de datos e información, es la interferencia de datos informáticos (en la que conviven a su vez otras conductas), de la cual se hace referencia dentro del "Estudio exhaustivo sobre el delito cibernético" de Oficina de las Naciones Unidas contra la Droga y el Delito[258], como "En el caso de interferir datos informáticos, la conducta que constituye la interferencia va desde dañar hasta borrar, alterar, suprimir, agregar o transmitir datos".

Limitantes de la normativa nacional

Una de las principales limitantes de la normativa nacional, en relación a los ciberdelitos y/o delitos informáticos, es el hecho de encontrase estas conductas tipificadas en diferentes ordenamientos, pues es necesario que las características de los mismos, nos lleven a desarrollar tanto un código penal

[258] *United Nations Office on Drugs and Crime*, op.cit.

especializado en conductas delictivas emergentes resultado de la utilización de ciencia y tecnología informática emergente, como un código de procedimientos penales relacionado con delitos cibernéticos y nuevas tecnologías, en el cual se revise y amplíe no solo el tratamiento de la prueba electrónica junto con su presentación, sino las investigaciones (por lo complicado de la autopsia de los ordenadores), glosario y vocabulario, así como todos los puntos que se puedan adaptar a las nuevas tecnologías.

Bien jurídico

Dentro de los delitos informáticos, los datos e información surgen como un bien jurídico inmaterial, ya que si nos enfocamos en la definición de bien inmaterial que la "Enciclopedia Jurídica"[259] nos da como, "todo objeto susceptible de tener un valor que no puede ser percibido por nuestros sentidos", damos cuenta que los datos e información, son valores no percibidos por los sentidos, y que a su vez son un bien inmaterial comerciable, como señala Manuel Heredero Higuera[260], en ese sentido al ser entendido como bien inmaterial comerciable, ya que estos bienes pueden no solo ser intercambiados por depósitos virtuales o monedas virtuales, los datos e información son bienes y activos que son comercializados al darles valor, siendo vendidos y comprados constantemente, este a su vez, se relaciona con bienes como el patrimonio, la intimidad y confidencialidad, entre otros.

Es importante referir que los sistemas informáticos, medios de almacenamiento, sistemas de computadores o red de computadoras –red de sistemas informáticos-, señal y medios de transportación de la misma, forman parte del patrimonio de las personas físicas, morales así como de los organismos y entes del Estado, que a su vez se relacionan con el procesamiento, transmisión, recepción y envió del bien jurídico de los datos e información.

[259] Enciclopedia Jurídica, op.cit.
[260]Heredero, Manuel, op.cit. p.p. 245-246.

Por otro lado la seguridad de la información, y por ende de los sistemas informáticos, medios de almacenamiento, sistemas de computadores o red de computadoras –red de sistemas informáticos-, señal y medios de transportación de la misma, que permiten el procesamiento, trasmisión, recepción y envió del bien jurídico de los datos e información, es esencial, ya que de esta depende que los mismos no sean vulnerados, lo que con base en el artículo 19 de la Ley Federal de Protección de Datos Personales en Posesión de Particulares, deberán tomar en cuenta los responsables que lleven a cabo el tratamiento de datos personales, estableciendo y manteniendo medidas de seguridad administrativas, técnicas y físicas, que permitan proteger los datos personales contra daño, pérdida, alteración, destrucción o el uso, acceso o tratamiento no autorizado, así tanto las medidas de seguridad administrativas, físicas y técnicas, descritas en el Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, artículo 2, fracciones V, VI y VII, convergen en la protección de los datos e información, y por ende de los sistemas informáticos, en la adquisición, operación, desarrollo y mantenimiento de sistemas seguros, así mantener la integridad, disponibilidad, privacidad, control y autenticidad de la información contenida en los mismos, que como señalan los Doctores Rodolfo Fernández y Da Silva Waldemar entorno al sistema informático, son “vulnerabilidables todos los elementos que lo integran”, así son vulnerabilidables todos los elementos que integran los sistemas informáticos, medios de almacenamiento, sistemas de computadores o red de computadoras –red de sistemas informáticos-, señal y medios de transportación de la misma, por lo que la seguridad de los mismos emerge como parte del bien jurídico de los datos e información, así como de su seguridad y la seguridad de los elementos que permiten el procesamiento, transmisión, recepción y envió de los mismos.

Sujeto activo

Entendemos que el sujeto activo del delito es quien lo comete, lo que se fortalece por Griselda Amuchategui[261], cuando nos dice que el sujeto activo es "la persona física que comete el delito; se llama también delincuente, agente o criminal", en ese sentido toda persona física que realice la conducta afectante del bien jurídico de los datos e información, atentando a su vez contra los sistemas de seguridad de los sistemas informáticos, medios de almacenamiento, sistemas de computadores o red de computadoras –red de sistemas informáticos-, señal y medios de transportación de esta, así como cualquier tecnología presente y futura relacionada con el procesamiento, transmisión, recepción y envió de los datos e información, y que los utiliza como instrumento o fin, será quien cometa el ciberdelito o delito informático.

Es importante tomar en cuenta que en relación a los elementos objetivos, entendidos como requisitos imprescindibles que forman parte de la descripción legal de la conducta antijurídica, la calidad específica del sujeto activo debe ser esencialmente considerada (servidor público, responsable del tratamiento de la información, etc.), ya que la misma se encuentra constituida por un conjunto de cualidades que caracterizan al sujeto activo del delito, mismas que son señaladas en el tipo penal.

La posibilidad de autonomía de la Inteligencia Artificial, asociada a los delitos informáticos, se materializa de forma constante, como en el caso de los *bots* (persona falsa), y por consiguiente *bonets* (cualquier grupo de PC infectados y controlados por un atacante de forma remota), lo que conlleva a exponenciar el o los delitos, así como el daño al bien o bienes jurídicos, ya que pueden ser atacados desde uno hasta cientos, miles o muchos más equipos o sistemas (objetivos-sujeto pasivo), en ese tenor la posibilidad de una tercera persona

[261] Amuchategui, Griselda, op.cit, p. 39.

jurídica denominada “persona artificial”, como señala Alejandra Moran Espinosa, debe ser tomada muy en cuenta en el contexto presente y futuro.

Sujeto pasivo

En relación al sujeto pasivo de los delitos informáticos, estos serán las personas físicas, morales, el estado o la sociedad, y en el tema que nos ocupa, los datos e información de los mismos, de esta manera el Dr. Santiago Acurio, refiere “tenemos que distinguir que sujeto pasivo o víctima del delito es el ente sobre el cual recae la conducta de acción u omisión que realiza el sujeto activo, y en el caso de los “delitos informáticos” las víctimas pueden ser individuos, instituciones crediticias, gobiernos, etcétera que usan sistemas automatizados de información, generalmente conectados a otros[262]”.

Recapitulando y complementando lo mencionado con anterioridad, Felipe Rodríguez señala como elementos de este tipo de delitos, los siguientes:

> *a) objetivo: la acción (conducta) que tipifica la ley como delito.*
>
> *b) subjetivo: el dolo o la culpa;*
>
> *c) sujeto activo: persona que realiza la conducta tipificada en la ley, entre quienes pueden ejecutar los ilícitos podemos mencionar a: operadores, programadores, analistas, supervisores, personal técnico y de servicio, funcionarios superiores y de control, auditores etc.*
>
> *d) sujeto pasivo: son aquellas personas de existencia visible o jurídica, instituciones etc. ansiadas por los transgresores de las conductas antijurídicas impuestas por la ley penal que atacan sus sistemas informáticos[263].*

Penas y medidas de seguridad

La peligrosidad del delincuente informático, tiene vertientes muy interesantes, ya que dependiendo de los conocimientos informáticos, será la capacidad de actuación dentro de un ataque o delito perpetrado de forma básica (sin muchos conocimientos pero con acceso a equipos) o de forma avanzada (con conocimientos especializados en informática y acceso a uno o múltiples

[262] Del Pino, Santiago, op, cit., p. 18.
[263] Rodríguez, Felipe, op.cit., p. 112.

sistemas), como se puede apreciar en las conductas propias de quienes realizan constantemente estos tipos de delitos, sus procesos, faces de ataque, infraestructura, vocabulario, etc., representan y muestran, tanto características como conocimientos del sujeto o sujetos activos en la materia, ya sea de forma individual u organizada.

La aplicación de las penas (culpabilidad) y medidas de seguridad (peligrosidad del delincuente) en los delitos informáticos, deben permitir no solo una correcta sanción, sino el acotamiento del hecho delictuoso y la rehabilitación del delincuente, en ese sentido las mismas deben tomar en cuenta la potencialización del hecho que atenta contra el bien o bienes jurídicos, ya que la información utilizada en el hecho y así el ataque, puede expandirse hacia otros objetivos, pudiéndose programar uno o más objetivos, siendo atacados los mismos cada cierto tiempo, como en el caso del ataque *Wannacry* (*randsomware* que ataco a muchos sistemas informáticos corporativos de gran cantidad de empresas en el mundo, encriptándolos y pidiendo rescate), esto conlleva a dañar múltiples objetivos, pues el fin del ataque era secuestrar infinidad de sistemas informáticos dejándolos inutilizables y sin poder acceder a los datos e información, vulnerando sus sistemas de seguridad.

Con este ataque se disminuyen las capacidades de sistemas informáticos, daño a múltiples personas y compañías que dependían de la información (como las prestadoras de servicios de salud), afectando el bien jurídico del patrimonio (infraestructura, pérdidas por pagos del rescate, demandas a las compañías prestadoras de servicios, etc.), de personas físicas, morales y entes del estado., en ese tenor nos encontramos ante un posible delito continuado, señalado en el artículo 7, fracción III del CPF como “cuando con unidad de propósito delictivo, pluralidad de conductas y unidad de sujeto pasivo, se viola el mismo precepto legal”, por el hecho de buscar extorsionar a múltiples sujetos pasivos, por medio del secuestro del sistema informático.

En ese sentido, las penas y medidas de seguridad, que se impongan a los delincuentes informáticos, deben tomar muy en cuenta no solo las capacidades, conocimientos e infraestructura del delincuente, sino de igual forma la peligrosidad presente y futura del mismo, así aplicando medidas como el aislamiento de cualquier tipo de sistema informático, ya que este es su principal instrumento para cometer el hecho delictuoso, lo que conlleva de igual forma al intercambio de conocimientos y su aplicación en el combate a dichos delitos, por medio de la cooperación entre el Estado y él/o los delincuentes, como medida de rehabilitación del delincuente informático.

Los delitos informáticos, pueden afectar con un solo hecho, múltiples bienes jurídicos, pues son potencialmente pluriofensivos (atacan a más de un bien jurídico a la vez), de lo cual el daño, y por ende su pena, deberá ser castigado conforme a la afectación, material (como ejemplo en el caso de la industria o empresas la afectación a su infraestructura y/o sistemas informáticos), psicológica (como ejemplo, si indujo a un daño físico o corporal como en el suicidio), económica (como en los desvíos de dinero por medios informáticos) moral y prestigio (desprestigio de personas y empresas), etc., en congruencia con el artículo 52 del Código Penal Federal, el cual señala los criterios que el juez utilizará para fijar las penas y medidas de seguridad:

> *El juez fijará las penas y medidas de seguridad que estime justas y procedentes dentro de los límites señalados para cada delito, con base en la gravedad del ilícito, la calidad y condición específica de la víctima u ofendido y el grado de culpabilidad del agente, teniendo en cuenta:*
>
> *I.- La magnitud del daño causado al bien jurídico o del peligro a que hubiere sido expuesto;*
>
> *II.- La naturaleza de la acción u omisión y de los medios empleados para ejecutarla;*
>
> *III.- Las circunstancias de tiempo, lugar, modo u ocasión del hecho realizado;*
>
> *IV.- La forma y grado de intervención del agente en la comisión del delito;*
>
> *V.- La edad, la educación, la ilustración, las costumbres, las condiciones sociales y económicas del sujeto, así como los motivos que lo impulsaron o determinaron a delinquir. Cuando el procesado perteneciere a algún pueblo o comunidad indígena, se tomarán en cuenta, además, sus usos y costumbres;*

VI.- El comportamiento posterior del acusado con relación al delito cometido; y VII.- Las demás condiciones especiales y personales en que se encontraba el agente en el momento de la comisión del delito, siempre y cuando sean relevantes para determinar la posibilidad de haber ajustado su conducta a las exigencias de la norma.

Si partimos del principio de legalidad consagrado en nuestra Carta Magna, en su artículo 14 párrafo tercero, "*en los juicios del orden criminal queda prohibido imponer, por simple analogía, y aún por mayoría de razón, pena alguna que no esté decretada por una ley exactamente aplicable al delito de que se trata*", así no se puede imponer pena o medida de seguridad por la realización de una conducta no descrita exactamente como antijurídica en la ley, y en el caso de los delitos informáticos, si no ha sido tipificada la conducta y el daño al bien jurídico, el delito puede quedar impune.

El principio de legalidad, como seguridad jurídica del gobernado, dará a su vez certeza jurídica en la aplicación exacta de la ley penal, así lo ordena el artículo 22, párrafo primero de Nuestra Constitución, en relación al principio de culpabilidad, "*Toda pena deberá ser proporcional al delito que sancione y al bien jurídico afectado*", lo que conlleva en los delitos informáticos, a que su exponenciación o potencialización, esto es la cantidad de sistemas y personas tanto Jurídicas como Morales afectadas, al dificultar y confundir la exactitud del objetivo principal del ataque y su investigación, atente contra el principio de culpabilidad y en su caso el principio de legalidad.

Con el estudio de los sistemas informáticos, medios de almacenamiento, sistemas de computadores o red de computadoras –red de sistemas informáticos-, señal y medios de transportación de la misma, que permiten el procesamiento, trasmisión, recepción y envió del bien jurídico de los datos e información, utilizados como medio o fin en los delitos informáticos, se podrá ampliar su concepción, en el caso particular la del "Robo de Datos e Información", lo que conlleva a una revisión del delito en comento, y por ende el de las penas y medidas de seguridad aplicadas al tipo penal, reforzando a su vez la normativa especial relacionada a este tipo de delitos.

CONCLUSIONES

Partiendo de las vertientes y especialidad de quienes cometen un ciberdelito y/o delito informático, lo que dificulta su estudio y tipificación, al ser revisado el delito de robo de datos en la normativa actual, se logró delimitar elementos que permiten ampliar la protección al bien jurídico de los datos, por ende el de las personas físicas, morales y entes del Estado, llegando a las siguientes conclusiones:

PRIMERO.- Luego de revisar nuestra legislación nacional, así como de algunos otros países, y los conceptos contenidos en tratados internacionales, como el Convenio de Budapest, se encontraron múltiples categorías y tipos de datos, como consecuencia de la conceptualización de la informática, datos e información que convergen en los diversos procesos relacionados con el tratamiento, transportación, procesamiento, transmisión (algunos tipos de esta), almacenamiento, etc., de los mismos.

SEGUNDO.- La importancia de unificar y homologar los protocolos de seguridad que las empresas del Estado, razones sociales, sujetos obligados, organismos e instituciones públicas y privadas, utilicen dentro del tratamiento, almacenamiento y uso de datos, como personas físicas y morales responsables, todos aquellos que se comprometen ante un contrato como responsables, encargados y usuarios, desarrolladores y diseñadores de programas, de softwares y su encriptación, aplicaciones, etc., buscando ampliar las medidas de seguridad administrativas, técnicas y físicas, necesarias en el contexto actual y futuro de los datos y la información.

TERCERO.- Los análisis de brecha y riesgos, nos permitirán conocer cuál es el riesgo real en el que se encuentran los sistemas informáticos, redes y aplicaciones, por lo que en la actualidad se vuelve indispensable realizar pruebas de penetración de forma recurrente, ya que las mismas nos permiten saber las capacidades físicas y tecnológicas con las que contamos.

CUARTO.- La necesidad de revisión de los existentes permisos perpetuos e irrevocables contenidos en los términos y condiciones de las empresas que operan de forma virtual dentro de las redes y/o ciberespacio, se expone el daño causado a los consumidores, al ser aceptados de forma inconsciente ya que por la necesidad y premura del servicio, estos no son revisados y aceptados de forma correcta.

QUINTO.- La delincuencia organizada, es establecida en el artículo 2 de la Ley Federal contra la Delincuencia Organizada[264], en la cual para ser configurada esta figura delictiva, se necesitan los siguiente elementos, tres o más personas que se organicen de hecho, que la organización sea en forma permanente o reiterada y que tenga como finalidad o resultado cometer alguno o algunos de los delitos que son señalados en el artículo en cuestión. De esta forma, si se busca ampliar esta figura jurídico penal con delitos informáticos, en los cuales interactúen de forma virtual y material los delincuentes, interrelacionándose y distribuyéndose los sujetos activos, el hecho delictivo y su preparación, deberá entenderse que son realizados por múltiples participes a la vez por medio de la informática.

SEIS.- La cooperación entre Estados y la adopción de Tratados Internacionales, es fundamental, ya que permitirá una lucha conjunta contra los delitos informáticos, no solo para entender los daños causados al/o bienes jurídicos, sino también su correcta investigación, tipificación, ampliación de la jurisprudencia, homologación y aplicación adecuada de las normas jurídico penales y procesales, así como el estudio del fenómeno delictivo, dentro y fuera de cada uno de los Estados en donde se ha cometido la afectación, permitiendo unificar toda la información entorno a los mismos, con el fin de evitar vacíos jurídicos y todo aquello que limite la lucha contra los diferentes fenómenos delincuenciales relacionados al delito informático, así como la aplicación de

[264] Artículo 2, Ley Federal contra la Delincuencia Organizada, op. cit.

acciones y políticas públicas preventivas, con el fin de evitar riesgos en la conducción de estas conductas.

SIETE.- En el ámbito del tratamiento, procesamiento, trasmisión, recepción y envió de los datos e información, la normativa nacional revisada es aplicada en las siguientes vertientes: 1. Sistema informático (*software y hardware*); 2. Medios de almacenamiento (Medios ópticos que son leídos por un láser de almacenamiento); 3. Sistema de computadores o red de computadoras (varios sistemas informáticos interconectados); 4. Señal (de cualquier tipo así microonda, radiofrecuencia, infrarrojo o de otra tecnología); y 5. Medios de transportación (comunicaciones alámbricas, inalámbricas, o de fibra óptica, sean telegráficas, telefónicas o satelitales).

OCHO.- De la protección y seguridad que debe ser brindada por el Estado, y en relación a los delitos informáticos, nos encontramos ante dos vertientes, la primera en la que se busca adecuar las figuras jurídico penales tradicionales como el robo, a las nuevas modalidades delictivas, y en el tema que nos ocupa, robo de datos e información, mientras que la segunda, parte de la necesidad de crear nuevas figuras jurídico penales, las cuales en el contexto actual, son necesarias por la variedad de técnicas y conductas criminales que emergen de este fenómeno delictivo.

Al revisar el delito de robo, que con base en el artículo 367 del CPF, consiste en apoderarse de una cosa ajena mueble, sin derecho y sin consentimiento de la persona que puede disponer de ella con arreglo a la ley, se limita su aplicación al referir “cosa ajena mueble”, ya que los datos e información deben ser especificados, en el entendido de que nos encontramos ante espacios virtuales, puesto que su soporte lógico es inmaterial y debido a la prohibición de analogías en los juicios del orden criminal, decretada en el artículo 14, párrafo segundo de nuestra carta magna, nos vemos en la necesidad de especificar el robo de datos e información, no como una conducta antijurídica

equiparada, sino como una conducta que debe ser plasmada de manera especial por la esencia y complejidad de los delitos informáticos.

NUEVE.- Por su parte las conductas obtener, copiar, utilizar, recibir, distribuir, interrumpir, interferir, divulgar, adquirir, usar, extraviar, alterar, mutilar, destruir e inutilizar, de manera dolosa y sin autorización, relacionadas con el procesamiento, trasmisión, recepción y envió de datos e información, son conductas que dañan y disminuyen al bien jurídico al filtrar la información y por ende vulnerarla, lo que conlleva a exponerla, sin embargo el robo de datos e información, si bien permite su vulneración, como esencia de los delitos informáticos, se establece que dentro del Robo de datos e información, al momento de acceder sin consentimiento, a los datos e información que permiten ingresar a señales, medios de transporte, almacenamiento y sistemas informáticos (labor principal de los denominados *Crackers*), la información que es intercambiada durante este proceso de acceso no autorizado, será utilizada permitiendo la intrusión, atentando contra sus sistemas de seguridad, configurando así el delito de robo de datos de acceso.

DIEZ.- Las técnicas y conductas que atentan contra los bienes jurídicos, que partiendo del concepto típico del delito informático, expuesto por el maestro Julio Téllez, "*conductas típicas, antijurídicas y culpables que tiene a las computadoras como instrumento o fin*", pueden ser ampliadas a los sistemas informáticos (televisores, vehículos inteligentes, casas y ciudades inteligentes, sistemas de videojuegos, etc.) retomando los resultados de la investigación, de la siguiente forma.

> "*conductas típicas, antijurídicas y culpables que tienen a los sistemas informáticos, medios de almacenamiento, sistemas de computadores o red de computadoras –red de sistemas informáticos-, señal y medios de transportación de esta, así como cualquier tecnología presente y futura relacionada con el procesamiento, trasmisión, tratamiento, almacenamiento, recepción y envió de los datos e información, como instrumento o fin*"

En ese sentido la ampliación propuesta se conjuga con el hecho de ser utilizados como instrumento o fin, por lo que se establece de la siguiente forma:

1. Como instrumento (medio). Se utilizan los sistemas informáticos, medios de almacenamiento, sistemas de computadores o red de computadoras –red de sistemas informáticos-, señal y medios de transportación de esta, así como cualquier tecnología presente y futura relacionada con el procesamiento, trasmisión, tratamiento, almacenamiento, recepción y envió de los datos e información, como medio para cometer el delito como en el uso no autorizado de programas de cómputo, alteración en el funcionamiento de los sistemas, intervención en las líneas de comunicación de datos o teleproceso, modificación de datos tanto en la entrada como en la salida, etc.).

2. Como fin. Los sistemas informáticos, medios de almacenamiento, sistemas de computadores o red de computadoras –red de sistemas informáticos-, señal y medios de transportación de esta, así como cualquier tecnología presente y futura relacionada con el procesamiento, trasmisión, tratamiento, almacenamiento, recepción y envió de los datos e información, son el objetivo (como en la programación de instrucciones que producen un bloqueo total al sistema, destrucción de programas por cualquier método y secuestro de soportes magnéticos en los que figure información valiosa con fines de chantaje, pago de rescate, etc.).

ONCE.- Los datos e información surgen como un bien jurídico inmaterial, ya que si nos enfocamos en la definición de bien inmaterial que la “Enciclopedia Jurídica” nos da como, “*todo objeto susceptible de tener un valor que no puede ser percibido por nuestros sentidos*”, damos cuenta que los datos e información, son valores no percibidos por los sentidos, y que a su vez son un bien inmaterial comerciable, como señala Manuel Heredero Higuera, en ese sentido al ser entendido como bien inmaterial comerciable, ya que estos bienes pueden no solo ser intercambiados por depósitos virtuales o monedas virtuales, los datos e información son bienes y activos que son comercializados al darles valor,

siendo vendidos y comprados constantemente, este a su vez, se relaciona con bienes como el patrimonio, la intimidad y confidencialidad, entre otros.

DOCE.- Entendemos que el sujeto activo del delito es quien lo comete, en ese sentido toda persona física que realice la conducta afectante del bien jurídico de los datos e información, atentando a su vez contra los sistemas de protección de los sistemas informáticos, medios de almacenamiento, sistemas de computadores o red de computadoras –red de sistemas informáticos-, señal y medios de transportación de esta, así como cualquier tecnología presente y futura relacionada con el procesamiento, trasmisión, recepción y envió de los datos e información, y que los utiliza como instrumento o fin, será quien cometa el ciberdelito o delito informático.

En relación a los elementos objetivos, entendidos como requisitos imprescindibles que forman parte de la descripción legal de la conducta antijurídica, la calidad especifica del sujeto activo debe ser esencialmente considerada (servidor público, responsable del tratamiento de la información, etc.), ya que la misma se encuentra constituida por un conjunto de cualidades que caracterizan al sujeto activo del delito, mismas que son señaladas en el tipo penal, como parte especial del sujeto activo del delito informático.

La posibilidad de autonomía de la Inteligencia Artificial, asociada a los delitos informáticos, se materializa de forma constante, como en el caso de los *bots* (persona falsa), y por consiguiente *bonets* (cualquier grupo de PC infectados y controlados por un atacante de forma remota), lo que conlleva a exponenciar el o los delitos, así como el daño al bien o bienes jurídicos, ya que pueden ser atacados desde uno hasta cientos, miles o muchos más equipos o sistemas (objetivos-sujeto pasivo), en ese tenor la posibilidad de una tercera persona jurídica denominada “persona artificial”, como señala Alejandra Moran Espinosa, debe ser tomada muy en cuenta en el contexto presente y futuro.

TRECE.- La peligrosidad del delincuente informático, tiene vertientes muy interesantes, ya que dependiendo de los conocimientos informáticos, será la

capacidad de actuación dentro de un ataque o delito perpetrado de forma básica (sin muchos conocimientos pero con acceso a equipos) o de forma avanzada (con conocimientos especializados en informática y acceso a uno o múltiples sistemas).

En ese sentido, las penas y medidas de seguridad, que se impongan a los delincuentes informáticos, deben tomar muy en cuenta no solo las capacidades, conocimientos e infraestructura del delincuente, sino de igual forma la peligrosidad presente y futura del mismo, así aplicando medidas como el aislamiento de cualquier tipo de sistema informático, ya que este es su principal instrumento para cometer el hecho delictuoso, lo que conlleva de igual forma al intercambio de conocimientos y su aplicación en el combate a dichos delitos, por medio de la cooperación entre el Estado y él/o los delincuentes, como medida de rehabilitación del delincuente informático.

CATORCE.- Los delitos informáticos, pueden afectar con un solo hecho, múltiples bienes jurídicos, pues son potencialmente pluriofensivos (atacan a más de un bien jurídico a la vez), de lo cual el daño, y por ende su pena, deberá ser castigado conforme a la afectación, material (como ejemplo en el caso de la industria o empresas la afectación a su infraestructura y/o sistemas informáticos), psicológica (como ejemplo, si indujo a un daño físico o corporal como en el suicidio), económica (como en los desvíos de dinero por medios informáticos) moral y prestigio (desprestigio de personas y empresas), etc. En congruencia con el artículo 52 del Código Penal Federal.

PROPUESTAS

Para lograr “replantear la tipificación del ciberdelito de robo de datos, con el objetivo de ampliar la protección al bien jurídico de los mismos”, se propone incorporar al **TÍTULO NOVENO del Código Penal Federal, el Capítulo III, denominado Delitos Informáticos, tomando como base** el concepto típico de delito informático, expuesto por el maestro Julio Téllez, y quedando de la siguiente forma:

CONCEPTO TÍPICO DEL DELITO INFORMÁTICO MAESTRO JULIO TÉLLEZ	PROPUESTA
"Conductas típicas, antijurídicas y culpables que tiene a las computadoras como instrumento o fin"	Artículo 211 Ter.- "Se entiende por delito informático la conducta típica, antijurídica y culpable que tienen a los sistemas informáticos, medios de almacenamiento, sistemas de computadores o red de sistemas informáticos –internet-, señal y medios de transportación de esta, así como cualquier tecnología presente y futura relacionada con el procesamiento, transmisión, almacenamiento, recepción y envió de los datos e información, como instrumento o fin"

Lo antes mencionado nos permitirá la creación de una ley especial en materia de delitos informáticos, denominada "Ley General de Delitos Informáticos", en la cual se establezcan los tipos penales de delito informático y robo de datos e información.

En el ámbito del tratamiento, procesamiento, transmisión, recepción y envío de los datos e información, se debe tomar en cuenta los siguientes elementos: 1. Sistema informático (*software y hardware*); 2. Medios de almacenamiento (material e inmaterial-virtual); 3. Sistema de computadores o red de computadoras (varios sistemas informáticos interconectados); 4. Señal (de cualquier tipo así microonda, radiofrecuencia, infrarrojo o de otra tecnología); y 5. Medios de transporte (comunicaciones alámbricas, inalámbricas, o de fibra óptica, sean telegráficas, telefónicas o satelitales).

Por lo que esta ley debe contener los siguientes puntos:

a) **Delitos cometidos por medio de sistemas informáticos**, **medios de almacenamiento, sistemas de computadores o red de sistemas informáticos –internet-, señal y medios de transportación de esta**. Dentro de este apartado, es factible encuadrar los siguientes delitos: Fraude cometido por medios informáticos; Estafa informática; Espionaje informático; Suplantación de sitios *web*; Falsificación de documentos; Obtención y envió

ilícito de todo tipo de activos; Violencia psicológica y sexual por medios informático como el *bullyng o* inducción a conductas que atenten contra la integridad de la persona, violencia visual y auditiva (ansiógenos -que causan ansiedad-) pornografía infantil, acoso laboral y sexual, entre otras.

Siendo importante que en este apartado, se adopté la figura jurídico penal propuesta, “Robo de datos e información”, de la siguiente forma:

> *Comete delito de robo de datos e información, quien de forma dolosa, con fines de lucro, sin derecho y sin autorización del dueño, titular o quien sea responsable de su tratamiento, vulnerando y atentando contra los sistemas de seguridad, se apodere de datos e información contenidos en medios de almacenamiento, sistemas de computadores o red de computadoras –red de sistemas informáticos-, sistemas informáticos, señal y medios de transportación de esta, así como cualquier tecnología presente y futura relacionada con su procesamiento, transmisión, tratamiento, almacenamiento, recepción y envió.*

Encuadrando en ella, entre otras, las siguientes conductas delictivas relacionadas con los datos e información: Robo de información contenida en un correo electrónico; Robo de datos bancarios, Robo de contraseñas; Robo y manipulación de los datos de entrada y salida; Robo de datos personales (desde datos de identificación hasta biométricos); Robo de información industrial y de las empresas; Robo de información confidencial del Estado y las razones sociales; Robo de datos de geolocalización; Robo de datos que permitan la configuración de codificaciones, claves y encriptación de softwares, programas, páginas, aplicaciones y cualquier tipo de sistema de seguridad informática, etc.

b) Delitos que atentan contra sistemas informáticos, medios de almacenamiento, sistemas de computadores o red de sistemas informáticos –internet-, señal y medios de transportación de esta. Dentro de este apartado, es factible encuadrar los siguientes delitos: Daños o modificaciones de programas y o sistemas informáticos; Acceso ilícito (violando y/o vulnerando sus sistemas de seguridad) estando conectado o no a internet; Interceptación ilícita; Atentar contra cualquier tipo de sistema informático;

Secuestro de sistema informático; Violación de correo (como medio de transporte y almacenamiento); Uso de software malicioso, entre otros.

c) Posesión o producción de sistemas de computadores o red de sistemas informáticos (red invisible- alternas con el fin de cometer cualquier tipo de delitos), sistemas informáticos, o cualquier otra tecnología, que atenten contra los datos e información.

En ese sentido la ampliación propuesta se conjuga con el hecho de ser utilizados como instrumento o fin, por lo que es entendido de la siguiente forma:

1. Como instrumento (medio). Se utilizan los sistemas informáticos, medios de almacenamiento, sistemas de computadores o red de sistemas informáticos -internet-, señal y medios de transportación de esta, así como cualquier tecnología presente y futura relacionada con el procesamiento, trasmisión, tratamiento, almacenamiento, recepción y envió de los datos e información, como medio para cometer el delito como en el uso no autorizado de programas de cómputo, alteración en el funcionamiento de los sistemas, intervención en las líneas de comunicación de datos o teleproceso, modificación de datos tanto en la entrada como en la salida, etc.).

2. Como fin. Los sistemas informáticos, medios de almacenamiento, sistemas de computadores o red de sistemas informáticos –internet-, señal y medios de transportación de esta, así como cualquier tecnología presente y futura relacionada con el procesamiento, transmisión, tratamiento, almacenamiento, recepción y envió de los datos e información, son el objetivo (como en la programación de instrucciones que producen un bloqueo total al sistema, destrucción de programas por cualquier método y secuestro de soportes magnéticos en los que figure información valiosa con fines de chantaje, pago de rescate, etc.).

Conforme a lo anterior, de igual manera se debe tomar en cuenta lo siguiente:

- Ampliar las categorías de datos e información existentes dentro de la normativa nacional, partiendo de sus características y usos (identificación, información industrial, confidencial, del sistema informático, etc.), lo cual permitirá delimitar de manera correcta su tipificación, ya que como hemos visto no solo es información de las personas físicas y morales, sino que de igual manera es información que permite el acceso y salida del sistema informático.

- Clasificar los conceptos y categorías de datos, tomando en consideración lo siguiente: Datos que se relacionan con las personas físicas (como en la categorización de los datos personales, basada en el artículo 62 de los Lineamientos Generales sobre Protección de Datos Personales en Posesión de Sujetos Obligados de la Ciudad de México); Datos que se relacionan con las personas morales (como secretos industriales y datos de identificación de las empresas); Datos que se relacionan con los entes y dependencias del Estado (información de las dependencias y su objetivo social, información confidencial del Estado, etc.) y; Datos que se relacionan con los sistemas informáticos, señales y red (como datos de identificación de hardware y software, datos de entrada y salida de sistemas informáticos, etc.).

- Ampliar las medidas de seguridad administrativas, técnicas y físicas necesarias en el contexto actual y futuro de los datos y la información, tomando en cuenta la obligatoriedad del análisis de brecha y riesgos, siendo indispensable realizar pruebas de penetración de forma recurrente, ya que las mismas nos permiten saber las capacidades físicas y tecnológicas con las que se cuentan.

- Revisar y erradicar, dentro de las relaciones de consumo, permisos perpetuos e irrevocables contenidos en los términos y condiciones de las empresas que operan de forma virtual dentro del ciberespacio, y que

son otorgados de manera inconsciente por el consumidor, permitiendo acceder a la información contenida en sus dispositivos electrónicos de forma perpetua e irrevocable, como práctica negativa de los mismos, ya que se atenta contra la privacidad del sujeto y su información.

- Legislar y ampliar la legislación existente, que se relaciona con tecnologías emergentes que permitan proteger la información, como el uso de firma digital (sistemas financieros), *blockchain* y la nube.

- Incluir a los delitos informáticos, dentro del delito de delincuencia organizada, operando de manera virtual o no en las redes, ampliar el catálogo de delitos que configuran esta conducta delictiva, sancionada en artículo 2 de la Ley Federal contra la Delincuencia Organizada[265], como en el caso del delito de secuestro de sistemas informáticos, datos e información, que son realizados por medio de un malware denominado *ransomware o malware* de rescate, o el caso de *Wannacry, randsomware* que ataco a muchos sistemas corporativo de gran cantidad de empresas en el mundo.

- Ampliar la cooperación entre Estados y la adopción de Tratados Internacionales, con el objetivo de ampliar la lucha conjunta contra los delitos informáticos, no solo para entender los daños causados al/o bienes jurídicos, sino también su correcta investigación, tipificación, ampliación de la jurisprudencia, homologación y aplicación adecuada de las normas jurídico penales y procesales, así como la aplicación de acciones y políticas públicas preventivas, con el fin de evitar riesgos en la conducción de estas conductas.

- Establecer a los datos e información como un bien jurídico inmaterial, pues se demuestra que son valores no percibidos por los sentidos, y que

[265] Artículo 2, Ley Federal contra la Delincuencia Organizada, op. cit.

a su vez son un bien inmaterial comerciable, como señala Manuel Heredero Higuera, en ese sentido al ser entendido como bien inmaterial comerciable, ya que estos bienes pueden no solo ser intercambiados por depósitos virtuales o monedas virtuales, los datos e información son bienes y activos que son comercializados al darles valor, siendo vendidos y comprados constantemente, relacionados a su vez con bienes jurídicos como el patrimonio, la intimidad y confidencialidad, entre otros.

- Establecer como sujeto activo del delito informático, toda persona física que realice la conducta afectante del bien jurídico de los datos e información, atentando a su vez contra los sistemas de protección de los sistemas informáticos, medios de almacenamiento, sistemas de computadores o red de computadoras –red de sistemas informáticos-, señal y medios de transportación de esta, así como cualquier tecnología presente y futura relacionada con el procesamiento, trasmisión, recepción y envió de los datos e información, y que los utiliza como instrumento o fin, tomando en cuenta la calidad del sujeto activo como parte de los elementos objetivos, esto es fungir como servidor público, responsable del tratamiento de la información, etc.

- Analizar una posible tercera persona jurídica basada en *Bots* (persona falsa), conforme a los estudios y evolución de la inteligencia artificial, ya que existen informes de autonomía, esto es autoprogramación de las denominadas *"Machine Learning".*

- Las penas y medidas de seguridad que se impongan a los delincuentes informáticos, deben tomar muy en cuenta no solo las capacidades, conocimientos e infraestructura del delincuente, sino de igual forma la peligrosidad presente y futura del mismo, así aplicando medidas como el aislamiento de cualquier tipo de sistema informático, lo que conlleva

de igual forma al intercambio de conocimientos y su aplicación en el combate a dichos delitos, por medio de la cooperación entre el Estado y él/o los delincuentes, como medida de rehabilitación del delincuente informático.

- Como se ha comprobado los delitos informáticos, pueden afectar con un solo hecho, múltiples bienes jurídicos, pues son potencialmente pluriofensivos (atacan a más de un bien jurídico a la vez), de lo cual el daño, y por ende su pena, deberá tomar en cuenta como mínimo las siguientes afectaciones: a) Material (como ejemplo en el caso de la industria o empresas la afectación a su infraestructura y/o sistemas informáticos); b) Psicológica (como ejemplo, si indujo a un daño físico o corporal como en el suicidio); c) Económica (como en los desvíos de dinero por medios informáticos); d) Moral y prestigio (desprestigio de personas y empresas), e) Afectación al funcionamiento del sistema informático, señal, red, medio de transporte y medio de almacenamiento.

Fuentes de información

Bibliografía en orden alfabético por autores

Amuchategui, Griselda, “Derecho Penal”, México, Oxford, 4ª ed. 2012.

Arellano García, Carlos, “Práctica Forense del Juicio de Amparo”, Porrúa, México, 6a ed.1991.

Berenguer, David, “Estudio de metodologías de Ingeniería Social”, Master Universitario en Seguridad de las Tecnologías de la Información y de las Comunicaciones, Universidad Oberta de Catalunya.

Castellanos, Fernando, “Lineamientos Elementales del Derecho Penal” (Parte General), México, 11ª ed. 1977.

Del Peso, Emilio, “El documento de Seguridad”, IEE. Informáticos Europeos Expertos, Ediciones Díaz de Santos, S. A. Madrid España. 2004. Libro electrónico, GOOGLE, Libros.

Dona, Edgardo Alberto, “Teoría del Delito y de la Pena 1”, Fundamentación de las Sanciones Penales y de la Culpabilidad, Argentina, Editorial Astrea, 2ª ed. 1996.

Dona, Edgardo Alberto, “Teoría del Delito y de la Pena 2”, Imputación delictiva, Argentina, Editorial Astrea, 1ª ed, 1995.

Fernández, María Guadalupe, “Los Medios de Defensa del Particular ante la Administración Pública, en Derecho Administrativo”, Segundo Curso, Unidad 5, México, Veritatis Verbum, 1ª. Ed, 2015.

Glosario de Ciberseguridad, “Glosario de términos de Ciberseguridad de la Policía Federal”.

González Pérez, Jesús, “Procedimiento Administrativo Federal”, México, ed. Porrúa-UNAM, 2006.

González, Jesús, “Derecho Procesal Administrativo Mexicano”, México, ed. Porrúa-UNAM 1997.

González, Jesús, “El Amparo Administrativo, en Derecho Procesal Administrativo Mexicano”, Capítulo 1º, México, Porrúa, 2ª, ed. 1997.

Osorio y Nieto, César Augusto, “Delitos Federales”, México, Porrúa, 1ª ed. 1994.

Pavón, Francisco, “Manual de Derecho Penal Mexicano”, Parte General, 21ª ed., Porrúa, México, 2018.

Roxin, Claus, “Derecho Penal, Parte General”, Tomo I, Fundamentos de la Estructura de la Teoría del Delito, Traducción de la 2ª ed., alemana por Luzón Peña, D, Díaz y García Collendo, M, Remesal, V, España, Civitas, 1997.

Roxin, Claus, “Teoria del Tipo Penal, Tipos Abiertos y Elementos del Bien Jurídico”, Argentina, Ediciones Depalma, Versión Castellana del Prof. Dr. Enrique Bacigalupo, Universidad de Madrid. 1979.

Soberanes, José Luis, concepto, en (coord.), “Diccionario Jurídico Mexicano”, 4a ed, Porrúa-UNAM, México, 1991.

Téllez, Julio, “Derecho Informático”, México, Mc Graw Hill, 4ª ed. 2009.

Vidaurri Aréchiga, Manuel, “Teoría General del Delito”, México. Oxford, 1ª ed. 2013.

Sitios electrónicos

ABC Internacional, “Una consultora que trabajó para Trump robó a Facebook datos de 50 millones de usuarios para influir en las elecciones”.

Academia Mexicana de Derecho Informático, A.C., “El impacto de la era digital en los derechos humanos”.

Academia Mexicana de Derecho Informático, A.C., ”XX Aniversario: Retos de la protección de datos personales durante la pandemia”.

Agencia de Regulación y Control de las Telecomunicaciones, “Derechos y obligaciones de los abonados, clientes y usuarios”, Sistema Nacional de Información, República del Ecuador.

ALEGSA.com.ar. “*Definición de Macro”*, Diccionario de informática y tecnología.

Asamblea General de la Naciones Unidas, “Lucha contra la utilización de las tecnologías de la información y las comunicaciones con fines delictivos”, 2019.

Becares, Barbara, “Así funciona Carbanak, la banda de ciberdelincuentes que ha robado 1.000 millones de dólares”.

Blog de la Procuraduría Federal del Consumidor, “Ciberataques, la otra pandemia”, Gobierno de México.

Catalin, Cimpanu, “Estados Unidos acusa al grupo QQAAZZ por lavado de dinero para bandas de malware”, ZNNet, 2020.

Cibercriminología, “Tipos de cibercrimen y clasificación”, Video consultado.

Ciberdelincuencia Organizada, “caso práctico: Inteligencia económica”, UCO, Guardia Civil, CCN-CERT, 2018.

Coronado, Jesús Edmundo, “Ciberterrorismo, ciberdelincuencia y cooperación internacional”, Video, 2021.

Curso, “Introducción a la Protección de Datos Personales en Posesión de Sujetos Obligados de la CDMX”, InfoCdMex.

Del Pino, Santiago, “Delitos Informáticos: Generalidades*”*.

Departamento de Justicia de Estados Unidos, “Dos acusados se declaran culpables por su papel en ayudar a los ciberdelincuentes a lavar dinero como

parte de la organización QQAAZZ", Oficina del Fiscal de EE. UU., Distrito occidental de Pensilvania, 2021.

Diario Oficial, "Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales", Acuerdo ACT-PUB-30/09/2020.06, México, 2020.

Digital Bank LATAM, "¿Qué es Man in the Browser (MITB)?", e. Banking, News.

Docusing, "Conoce qué es un prestador de servicios de certificación y su rol con las firmas electrónicas".

Dr. Fernández, Rodolfo y Dr. Da Silva Waldemar, Paulo, "Del bien jurídico que protege los delitos informáticos" V/Lex. Tu mundo de inteligencia legal, 2021.

El espectador, "Llevan a juicio a la hacker más sexy del mundo".

Errecaborde, José Daniel y Parada, Ricardo Antonio, "Ciberbercrimen y delitos informáticos. Los nuevos tipos penales en la era de internet", 1ª ed. Erreius, Argentina, 2018.

Estrada, J, "El derecho a la intimidad y su necesaria inclusión como garantía individual".

Estrategia Nacional de Ciberseguridad, México, 2017.

FBI. Más Buscados, "GRUPO APT 41", Sitio WEB, Gobierno de los Estados Unidos.

Foro Económico Mundial, "El Informe de Riesgos Globales 2019", Ginebra, 2019. 4a edición.

Gobierno de la Ciudad de México, "Validación de copias certificadas del Registro Civil del Distrito Federal".

Gordillo, Agustín, "Capítulo I, Concepto y Naturaleza del Procedimiento Administrativo, en El Procedimiento Administrativo", Parte General.

Grupo Atlas de Seguridad Integral, "Técnicas de Ingeniería Social más usadas en ataques informáticos", video.

Grupo de Expertos encargado de Realizar un Estudio Exhaustivo sobre el Delito Cibernético, "Recopilación de todas las conclusiones y recomendaciones preliminares sugeridas por los Estados Miembros durante las reuniones del Grupo de Expertos encargado de realizar un estudio exhaustivo sobre el delito

cibernético celebradas en 2018, 2019 y 2020”, UNODC/CCPCJ/EG.4/2021/CRP.1, Viena, 2021.

Guerra, M, “Autopsia a Whatsapp T11 - CyberCamp 2017”, INCIBE, Video.

Guevara, M, “Guerras de Cuarta y Quinta Generación en la desestabilización de Gobiernos (Siglo XXI)”, video, 2019.

Helmut, S, “Protocolo en informática: características, tipos, ejemplos”, Lifeder.

Heredero Higueras, Manuel, “Derechos inmateriales y nuevas tecnologías de la información”.

Hernández, Álvaro, “La piratería de la TV de pago aún existe (y por qué nadie puede con ella)”, El confidencial.

Iberdrola, “Internet Industrial de las Cosas. Conjunto de sensores, instrumentos y dispositivos autónomos conectados a través de Internet a aplicaciones industriales”.

Imágenes y especialistas, “Protocolo para Tratamiento de Datos”.

INCIBE-CERT, “Amenazas emergentes en sistemas de control industrial”.

Instituto de Transparencia, Acceso a la Información Pública, “Otros documentos normativos”, Protección de Datos Personales y Rendición de Cuentas de la Ciudad de México.

Instituto de Transparencia, Acceso a la Información Pública, Protección de Datos Personales y Rendición de Cuentas de la Ciudad de México.

Jaramillo, Cristina y Leonidas, Pablo, “Metodología para realizar la evaluación, detección de riesgos, vulnerabilidades y contramedidas en el diseño e implementación de la infraestructura de la red de la editorial don Bosco, mediante un test de intrusión de caja blanca”, Universidad Politécnica Salesiana, Ecuador, 2015.

Julio, Téllez “Los delitos informáticos: Situación en México”.

Justia México, “Delitos informáticos, Preguntas y Respuestas Sobre Delitos Informáticos”.

Kaspersky “¿Qué es una brecha de seguridad”.

Kolibers, “Servicios de Pruebas de Penetración en México”.

Lecuit, J, “La seguridad y privacidad del blockchain, más allá de la tecnología y las criptomonedas. Real Instituto Elcano”, 2019.

López, Miguel, “Forense Digital”.

Mendoza, Olivia, “Marco jurídico de la protección de datos personales en las empresas de servicios establecidas en México: desafíos y cumplimiento”, Revista IUS, 2018.

Mieres, J y Borghello, C, “Robo de información personal online”, ESET para Latinoamérica, 2008.

Milagros, María, “La estafa informática en el Código Penal Argentino”.

Montilla, Johanna, “La Acción y sus Diferencias con la Pretensión y la Demanda”, Revista de Ciencias Jurídicas, Maracaibo Venezuela, Universidad Rafael Urdaneta, Vol. II.

Morán, Alejandra, “Responsabilidad penal de la Inteligencia Artificial (IA). ¿La próxima frontera?”, Revista del Instituto de Ciencias Jurídicas de Puebla, México, vol. 15, núm. 48, 2021.

Navarro, G, “El derecho a la protección de información personal en México”.

Noticias Seguridad Informática, “Cómo INTERPOL Atrapó al Hacker FXMSP "El dios invisible de las redes", Video.

Ocampo, M, “Nuevos desafíos para la protección de datos personales”, Biblioteca Jurídica Virtual del Instituto de Investigaciones Jurídicas de la UNAM.

Olivia, M, “Marco jurídico de la protección de datos personales en las empresas de servicios establecidas en México: desafíos y cumplimiento”, INFOTEC.

Ollero, Daniel, “Pedro, el hacker gallego que arrasa en Estados Unidos enseñando a secuestrar televisiones…”, España.

Palazuelos, Silvia, “Delitos informáticos. Propuesta para el Tratamiento de la Problemática en México”, Aequitas, Revista Jurídica del Poder Judicial del Estado de Sinaloa, núm. 32.

Pasión por el derecho, “Cibercrimen y nueva teoría del delito” Entrevista al profesor Ricardo Posada, 2019, Video.

Pereira, M, Toscano, M y Villar, P, “Plataformas blockchain y escenarios de uso”, Montevideo, Uruguay, 2019.

Pérez, J, “¿Qué es una persona identificada o identificable?”, Balaguer y Gutiérrez, Boletín, 2014.

Posada, Ricardo, “El Delito de Transferencia no Consentida de Activos”, Universidad de los Andes, 2012.

Posada, Ricardo, “El Delito de Transferencia no Consentida de Activos”, Universidad de los Andes, 2012.

Rodríguez, Felipe, “Lecciones de Derecho y Ética Profesional, para Profesionales y Estudiantes de Ingeniería, Arquitectura y Profesionales Afines” Legislación y Ética Profesional.

Sandoval, E, “Ingeniería Social: corrompiendo la mente humana”, Revista.Seguridad, núm. 10, UNAM, México, 2018.

Secretaría de Gobernación, “Plataforma México”, 2018.

Silva, J, “Humanismo, Técnica y Tecnología. Segunda parte”, Revista contaduría y administración, núm. 198, 2000.

SolarWinds Worldwide, “El tráfico de red (también llamado tráfico o tráfico de datos) hace referencia a los datos que se desplazan por una red en un momento determinado”, Monitor del tráfico de red, 2021.

The free dictionary, “Encriptar”, Farlex Inc, 2003-2022.

Tribunal Constitucional de España, “Sentencia 292/2000”.

Unidad de Investigaciones Cibernéticas y Operaciones Tecnológicas, Agencia de Investigación Criminal, “Guía Técnica de Cadena de Custodia de Evidencia Digital”, PGR, México, 2018.

Universidad a Distancia de Madrid, UDIMA, “Cibercriminología - Tipos de cibercrimen y clasificación”, video.

UNODC, “Serie de Módulos Universitarios: Delitos Cibernéticos”, La Declaración de Doha.

Vargas, L, “Pandilla, asociación delictuosa y delincuencia organizada en el nuevo Código Penal para el Distrito Federal”, en García, S, González, O (Coords.), Terceras jornadas sobre justicia penal “Fernando Castellano Tena”, UNAM, Instituto de Investigaciones Jurídicas, México, 2003.

Velazco, Eloy, “Crimen Organizado, Internet y Nuevas Tecnologías. Juzgado Central de Instrucción 6 de la Audiencia Nacional”.

Villegas, Saúl, “Marco jurídico del comercio electrónico en México”, Raigosa Consultores.

Vlex, “Concepto y definición de mejores prácticas”, 2022.

Ward, Mark, “El campamento de rehabilitación tiene como objetivo poner a los jóvenes ciberdelincuentes en el camino correcto”, BBC News, 2017.

Wikipedia, “Stuxnet”, 2021.

Zaffaroni, Raúl, “Lineamientos de Derecho Penal - 11 Autoria, Participacion y Tentativa”, video, Editorial Ediar, 2020.

Leyes y Tratados

“Personas morales tienen derecho a la protección de los datos que puedan equipararse a los personales, aun cuando dicha información haya sido entregada a una autoridad”, Tesis aislada P. II/2014 (10a.), con Número Digital 2005522, localizada en la Gaceta del Semanario Judicial de la Federación. Libro 3, Febrero de 2014, Tomo I, página 274.

Budapest, 23.XXI. 2021. Convenio de Budapest. Traducción Convenio sobre cibercriminalidad.doc.

Cámara de Diputados LXV Legislatura, Ley de Instituciones de Crédito.

Cámara de Diputados LXV Legislatura. Ley Federal del Trabajo.

CIRCULAR CJCDMX-45/2020, Poder Judicial de la Ciudad de México.

Código de Comercio.

Código de Conducta de la Policía Federal.

Código Penal Argentino. Ley 26.388, Modificación. Promulgada el Junio 24 de 2008.

Código Penal de Colombia, LEY 599 DE 2000.

Código Penal de Sinaloa.

Código Penal Federal.

Código Penal para el Distrito Federal.

Constitución Política de los Estados Unidos Mexicanos.

Convención Americana sobre Derechos Humanos.

Declaración de Principios, Documento “WSIS-03/GENEVA/4-S”, 12 de mayo del 2004, Cumbre Mundial Sobre la Sociedad de la Información, Ginebra 2003-Túnez 2005.

Declaración Universal de Derechos Humanos.

DOF: 12/10/2020. ACUERDO mediante el cual se aprueban los Lineamientos para el registro, emisión y uso de la Firma Electrónica del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales.

INFO Ciudad de México. *Lineamientos Generales de Protección de Datos Personales en Posesión de Sujetos Obligados de la Ciudad de México.* Instituto de Transparencia, Acceso a la Información Pública, Protección de Datos Personales y Rendición de Cuentas de la Ciudad de México Normatividad.

La Ley de Amparo en Lenguaje Llano. Suprema Corte de Justicia de la Nación.

LEY 1273 DE 2009.

Ley 26.388, se incorpora como inciso 16 del artículo 173.

Ley 34/2002, de 11 de julio, “Servicios de la Sociedad de la Información y de Comercio Electrónico”, Jefatura del Estado, España, núm 166, 2002.

Ley de Amparo.

Ley de Firma Electrónica Avanzada.

Ley de Protección de Datos Personales en Posesión de Sujetos Obligados de la Ciudad de México.

Ley Federal contra la Delincuencia Organizada.

Ley Federal de Protección a la Propiedad Industrial.

Ley Federal de Protección al Consumidor.

Ley Federal de Protección de Datos Personales en Posesión de los Particulares.

Ley Federal de Transparencia y Acceso a la Información Pública.

Ley Federal del Derecho de Autor.

Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

Ley para Regular las Instituciones de Tecnología Financiera.

Lineamientos Generales sobre Protección de Datos Personales en Posesión de Sujetos Obligados de la Ciudad de México.

Norma Oficial Mexicana NOM-151-SCFI-2016, “Requisitos que deben observarse para la conservación de mensajes de datos y digitalización de documentos”.

Protocolo adicional al convenio 108 para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal y relativo a transferencias de datos.

Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares.

Tesis aislada 369, Semanario Judicial de la Federación, Séptima Época, t. II, penal, Registro digital 905310, p. 174.

Tesis aislada. P. II/2014 (10a.), Semanario Judicial de la Federación y su Gaceta, Décima Época, Libro 3, Febrero de 2014, Tomo I, página 274.

Tribunal Supremo de Elecciones Normativas, “Ley de Protección de la Persona Frente al Tratamiento de sus Datos Personales”, Ley n.º 8968.