UNIVERSIDAD DE EL SALVADOR

FACULTAD DE JURISPRUDENCIA Y CIENCIAS SOCIALES

ESCUELA DE CIENCIAS JURÍDICAS

"LAS VENTAJAS DE SUSCRIBIR Y CONSOLIDAR CONVENIOS DE COOPERACIÓN Y SOPORTE TÉCNICO ENTRE FISCALÍA GENERAL DE LA REPUBLICA Y POLICÍA NACIONAL CIVIL, CON EMPRESAS PROVEEDORAS DE SERVICIOS EN SEGURIDAD INFORMÁTICA DE SITIOS WEB, Y REDES SOCIALES EN LA REPUBLICA DE EL SALVADOR PARA UNA EFICIENTE APLICACIÓN DE LA LEY ESPECIAL CONTRA LOS DELITOS INFORMÁTICOS Y CONEXOS; VIGENTE DESDE FEBRERO DE 2016"

TRABAJO DE GRADO PARA OBTENER EL TITULO DE LICENCIADO EN CIENCIAS JURIDICAS

PRESENTADO POR:

WALTER ALBERTO AYALA GUERRA.

MARVIN ERNESTO TEJADA RODRÍGUEZ.

RENAN ALBERTO QUINTANILLA SERVELLON.

DOCENTE ASESOR:

LIC. FRANCISCO ALBERTO GRANADOS HERNANDEZ.

CIUDAD UNIVERSITARIA, SAN SALVADOR, SEPTIEMBRE DE 2019.

TRIBUNAL CALIFICADOR

LIC. JOSE DAVID CAMPOS VENTURA.
(PRESIDENTE)

LIC. MARVIN HUMBERTO FLORES JUAREZ.
(SECRETARIO)

LIC. FANCISCO ALBERTO GRANADOS HERNANDEZ.
(VOCAL)

UNIVERSIDAD DE EL SALVADOR

Msc. Roger Armando Arias Alvarado.

RECTOR

Dr. Raúl Ernesto Azcúnaga López.

VICERRECTOR ACADEMICO

Ing. Juan Rosa Quintanilla Quintanilla.

VICERECTOR ADMINISTRATIVO

Msc. Francisco Antonio Alarcón Sandoval.

SECRETARIO GENERAL

Lic. Rafael Humberto Peña Marín.

FISCAL GENERAL

FACULTAD DE JURISPRUDENCIA Y CIENCIAS SOCIALES

Dra. Evelyn Beatriz Farfán Mata.

DECANA

Dr. Edgardo Herrera Pacheco.

VICEDECANO

Licda. Digna Reina Contreras de Cornejo.

SECRETARIA

Lic. René Mauricio Mejía Méndez.

DIRECTOR DE ESCUELA DE CIENCIAS JURÍDICAS

Licda. Digna Reina Contreras de Cornejo.

DIRECTORA DE PROCESOS DE GRADUACIÓN

Licda. María Magdalena Morales.

COORDINADORA DE PROCESOS DE GRADUACIÓN DE LA ESCUELA DE CIENCIAS JURÍDICAS

AGRADECIMIENTO

Agradecemos a nuestros padres por ser los principales promotores de nuestros sueños, por confiar y creer en nuestras expectativas, por los consejos, valores y principios que nos han inculcado, por guiarnos a lo largo de nuestra existencia, ser el apoyo y fortaleza en aquellos momentos de dificultad y de debilidad.

Agradecemos a nuestros docentes de la Facultad de Jurisprudencia y Ciencias Sociales de la Universidad de El Salvador, por haber compartido sus conocimientos a lo largo de nuestra preparación profesional, principalmente al Doctor Francisco Alberto Granados por acompañarnos en este proceso de investigación de grado, quien nos guio e incentivo a seguir adelante.

Gracias, por ser parte fundamental de este equipo.

Walter Guerra, Marvin Tejada, Renán Quintanilla.

AGRADECIMIENTO

El presente trabajo de grado es dedicado principalmente a mi abuela Teresa por ser la manifestación plena del amor en esta tierra y ser mi principal referente en enseñarme la bondad y la perseverancia frente a la adversidad.

A mis padres Rosa y Walter, por ser los seres inspiradores en mi vida, por su trabajo y sacrificio en todos estos años, ser mi fortaleza y enseñarme continuar enfrentando los retos académicos y profesionales para obtener uno de los tantos anhelos más deseados. A mi hermano Poncho por estar siempre en los momentos más decisivos de mi vida y acompañarme fielmente tanto en este proceso académico, profesional y personal, demostrándome día a día que la hermandad no solo depende de los lazos sanguíneos si no del afecto espiritual y la solidaridad plena.

A mis amados amigos: Gabriela, Karen, Gaby, Jorge, Edgardo, Mauricio, Ileana, Marcelo, Gerardo, Nelson, Edwin, José, Rafael y Jaime; quienes son parte de mi familia quienes siempre están en los momentos jubilo, tristeza y sensatez. Pero sobre todo han estado ahí en los momentos necesarios en las interminables lecciones de la vida, como parte de mi fortaleza y felicidad. A mis compañeros de tesis Marvin y Renán, a mi compañero y compañeras de la Facultad Francisco, Roció, Norma, Karla, compañeras y compañeros de trabajo con quienes he forjado gran parte de mi aprendizaje académico y profesional.

Es un orgullo y el privilegio ser su nieto, hijo, hermano, amigo y compañero, gran parte del ser humano que ven es gracias a ustedes, gracias por caminar y seguir caminando a mi lado.

Walter Guerra.

INDICE

RESUMEN

El presente trabajo de grado para obtener el título de licenciatura en ciencias jurídicas denominado: “Las ventajas de suscribir y consolidar convenios de cooperación y soporte técnico entre Fiscalía General de la República y Policía Nacional Civil, con empresas proveedoras de servicios en seguridad informática de sitios web, y redes sociales en la República de El Salvador para una eficiente aplicación de la ley especial contra los delitos informáticos y conexos; vigente desde febrero de 2016.” observa el comportamiento del fenómeno cibernético así como la respuesta del Estado Salvadoreño en un contexto internacional.

Por otra parte se inicia la capitulación uno: “historia de las computadoras en el salvador, antecedentes, orígenes y desarrollo de internet”; la Informática en el país. En capítulo dos se aborda “legislación y marco jurídico comparado sobre los delitos informáticos, en el contexto regional e internacional”, de la legislación guatemalteca, mexicana, alemana y española, finalizando con el convenio de Budapest, seguido del capítulo tres reflejando al “marco jurídico nacional y ámbito de aplicación de la ley especial contra delitos informáticos y conexos” en el ordenamiento jurídico jerárquico, así como leyes especializadas, finalizando el capítulo cuatro “las dificultades en investigación de la cibercriminalidad y su ámbito de aplicación en relación con la ley especial contra delitos informáticos y conexos, por la falta de convenios con empresas de seguridad informática, en la República de El salvador”.

Se concluye que las políticas integrales en el aspecto coercitivo del Estado, en cuanto la investigación y peritaje del debido proceso, recomendando la restructuración de Fiscalía General de la República y Policía Nacional Civil, gozando de flexibilidad a la hora de poder nombrar peritos especializados en informática forense.

ABREVIATURAS Y SIGLAS.

ABREVIATURAS

Art.	Articulo
Ed.	Editorial
Etc.	Etcétera
Inc.	Inciso
Lit.	Literal
Ord.	Ordinal
Ref.	Referencia

SIGLAS

ABA-ROLI	Asociación de la Barra Americana de Abogados
ANTEL	Administración Nacional de Telecomunicaciones
AOL	América Online
BSA	Business Software Alliancela
CIRT	Cámara Nacional de la Industria de Radio y Televisión
CNI	Comité Nacional de Informática
COM	Organismos comerciales
CONACYT	Consejo Nacional de Ciencia y Tecnología
DPTC	División de Policía Técnica Científica, abreviada
EDU	Universidades y otras instituciones de enseñanzas.
GOB	Organizaciones gubernamentales o Estatales
IBM	International Business Machines
INCAE	Instituto Centroamericano de Administración de Empresas

ISO 9001- 2008	Sistema de Gestión de Calidad
LECDIC	Ley Especial Contra Delitos Informáticos y Conexos
NET	Sistema de la red y administración de internet
OCDE	Organización para la Cooperación y el Desarrollo Económicos
OEA	Organización de Estados Americanos
ORG	Otras organizaciones
RAM	Random Acceses Memory
ROM	Read Only Memory
SIP	Sociedad Interamericana de Prensa
TIC	Tecnología de la Información y Comunicación
UIT	Unión Internacional de Telecomunicaciones
UNODOC	Oficina de Naciones Unidas contra la Droga y el Delito
VPN	Red Privada Virtual
WWW	World Wide Wed

INTRODUCCIÓN

Los avances tecnológicos a nivel mundial, principalmente en las últimas dos décadas, han sido notorios y progresivos, empujando a la sociedad a nuevas realidades. Con la entrada al "nuevo milenio" en un contexto político cada vez más diversificado vinculada una sociedad económicamente globalizada, la digitalización de la realidad a través de las instituciones tanto públicas como privadas es incuestionable, la transferencia de datos, los equipos de almacenamiento y la información digital son herramientas indispensables, que simplifican la cotidianidad desde cualquier perspectiva que se quiera analizar, de las cuales se puede mencionar la seguridad, educación, salud, comunicación, entre otras. No cabe duda que los beneficios son tangibles, impactando directamente en las personas, el GPS, la red inalámbrica, el internet etc. Son instrumentos que garantizan una sociedad eficiente, las transacciones económicas y el cotejo información había sido más directo en beneficio de la comunicación, superando los alcances de la radio y la televisión.

En cuanto a la era digital, El Salvador no puede quedarse aislado, partiendo del marco jurídico el cual tiene una su esencia desde 1989 una lógica enfocada al modelo neoliberal; es decir la actuación puntal del Estado. Siendo una economía dolarizada, abierta a las relaciones del mercado y con un alto nivel de consumo con una dependencia de los países industrializados, estos elementos permiten que la globalización así como las empresas transnacionales ejerzan de forma más directa su influencia en las relaciones económicas, sociales y culturales del país, siendo la norma o el derecho positivo el último eslabón de la cadena en integrase a este cambio en las relaciones de poder, el cual en la práctica dificulta o limita la actuación oportuna del Estado a través de sus instituciones.

En este mismo contexto se reforman y crean, diferentes instrumento jurídicos donde se encuentra desarrollada la necesidad del Estado en proteger los bienes jurídicos, tanto de las personas Naturales como jurídicas, no obstante pese a que existen parámetros establecidos en el derecho sustantivo salvadoreño, como estudiantes egresados de la carrera de Licenciatura en Ciencias Jurídicas, se analizan las deficiencias procesales que el sistema normativo tiene frente al fenómeno cambiante de las Tecnologías de la Información y Comunicación en cuanto a las practicas que pueden causar lesividad o un impacto negativo en la sociedad salvadoreña; de las cuales se ha tomado a bien investigar "Las ventajas de suscribir y consolidar convenios de cooperación y soporte técnico entre fiscalía general de la república y policía nacional civil, con empresas proveedoras de servicios en seguridad informática de sitios web, y redes sociales en la república de el salvador para una eficiente aplicación de la ley especial contra los delitos informáticos y conexos; vigente desde febrero de 2016."

La que se realiza como una metodología jurídica empírica, a partir del derecho comparado, así como experiencias de campos obtenidas en diferentes conferencias y talleres, tomando en cuenta el registro de diferentes hemerotecas y aportes bibliográficos de diferentes autores y compiladores sobre la materia desde la óptica del derecho penal, con el objetivo general de determinar el trabajo efectivo por medio de convenios de cooperación con entidades que brindan seguridad informática, en coordinación con las instituciones anteriormente mencionadas. Debido a la gran problemática que genera la cibercriminalidad, y de que todos cotidianamente están expuestos a este tipo de delincuencia por ser usuarios cada día más habituales de equipos informáticos, páginas web, redes sociales, aplicaciones de teléfonos celulares y demás formas de transferencia de datos, es necesaria su investigación.

En vista de la novedad que representa en la legislación la Ley Especial Contra Los Delitos Informáticos y Conexo de cuáles son las herramientas de las que en la práctica dispone el Estado Salvadoreño para la persecución de los delitos informáticos; Este trabajo de investigación comprende cuatro capítulos, y están estructurados de la siguiente manera: el Capítulo uno se desarrolla los antecedes y origines de las computadoras, la informática y el internet, se acerca a la historia de manera global, pasando por los avances más importantes y la integración de El Salvador ante la insipiente realidad digital.

Posteriormente en el Capítulo dos explica la legislación y el marco jurídico comparado sobre los delitos informáticos, en el contexto regional e internacional, conociendo los esfuerzos de países Latinoamericanos como europeos, así como los acuerdos internacionales que existen en materia de seguridad informática.

En el Capítulo tres se abordara lo referente al marco jurídico nacional y ámbito de aplicación de la Ley Especial Contra Delitos Informáticos y Conexos, en El Salvador, la cual forma parte del ordenamiento jurídico de el país, desde febrero de 2016, enfocado en articular la normativa existente tanto en el campo sustantivo como procesal, frente a las conductas emergentes con el uso de la Tecnología de Información y Comunicación

En el Capítulo cuatro se abordara las dificultades en investigación de la cibercriminalidad y su ámbito de aplicación en relación con la Ley Especial Contra Delitos Informáticos y Conexos, por la falta de convenios con empresas de seguridad informática, en la república de El Salvador, analizando de forma precisa los conceptos como: Tecnología de la información y Comunicación, desarrollo digital, derecho informático,

colocando en la perspectiva de la investigación, las conductas que pueden ser tipificadas del llamado cibercriminalidad, el cual se acelera y dinamiza de manera constante, debido a la conectividad mundial, frente a las dificultades procesales que los Estados en especial El Salvador enfrentan, al tener herramientas limitadas en la prosecución de este tipo de delitos ya sea por dificultades económicas, políticas y de cooperación con organismos y peritos calificados en la materia principalmente las instituciones del ministerio público, corporación policial y los operadores del sistema judicial al momento de tipificar y sancionar las conductas lesivas que cada vez son más rutinarias y alarmantes a nivel mundial y local, contando con el análisis de las entrevistas realizadas a expertos del tema planteando conclusiones y propuestas viables para el país.

CAPÍTULO I

HISTORIA DE LAS COMPUTADORAS EN EL SALVADOR, ANTECEDENTES, ORÍGENES Y DESARROLLO DE INTERNET

En este capítulo abordara la historia de las computadoras en El Salvador a partir de los años de 1952 y 1953; siendo la Corte de Cuentas una de las pioneras de la época. El desarrollo y organización de los servicios en el internet, puntualizando sus ventajas, componentes y sus denominaciones, con el propósito de establecer el aspecto histórico y general de la informática.

1. Historia de las computadoras en El Salvador

El desarrollo de la Informática en El Salvador, así como en otros países, ha sido de mucha importancia en los procesos administrativos, financieros, industriales y en la rama de la medicina; debido a que es una herramienta que permite realizar las labores cotidianas de una manera más rápida, veraz y oportuna. De esta manera en El Salvador la historia de la Informática se remonta a los años de 1952 y 1953; estos equipos utilizaban tarjetas perforadas y se le llamaban de Registro Unitario porque las tarjetas únicamente podían tener un registro.

Es así como empezó a mecanizarse los primeros procesos administrativos. Para esa época, la IBM no tenía representantes en El Salvador, no tenían sucursales; sino que la empresa que representaba IBM en Centroamérica, ubicada en Guatemala; cuando había algún problema de desperfectos, venían de Guatemala técnicos a reparar las fallas que podían tener los equi-

pos; posteriormente llegó a El Salvador la primera representación de IBM. La primera institución en El Salvador que utilizó el Sistema de Registro Unitario, fue la Corte de Cuentas de la República; posteriormente empresas como la Constancia, El Banco Central de Reserva (BCR)[1]. La empresa La Constancia, S.A. fue posiblemente la primera en traer una computadora a El Salvador, según ha quedado registrado fue una IBM 1401.En febrero de 1970 el Centro Educacional de Procesamiento de Datos ofrece cursos IBM para Perforación y Verificación, de Registro Unitario Teórico-Práctico, Programas de utilidad y Lenguaje RPG en IBM 360/20. Esta institución estaba en Calle Arce de San Salvador y los cursos eran impartidos por los analistas de sistemas Vicente A. Cisnado y José Roberto Ordóñez. Otra institución que daba cursos de RPG y perforación era Instituto Mundial, en la 3a calle poniente.[2]

El 15 de julio 1992, la Asamblea Legislativa aprueba la Ley del Consejo Nacional de Ciencia y Tecnología, conacyt. Básicamente se trataba de una imitación ligera y tardía de iniciativas de otros países, a tal punto que ni para buscarle nombre se usó un poco de creatividad. Con el tiempo no trascendería en su tarea debido al escaso potencial político que siempre se les ha visto a proyectos de este tipo.

Más adelante en el año de 1996, antel se convierte en el único proveedor de acceso conmutado al internet a ese momento, en términos comercialmente factibles. Proveía direcciones de correo bajo el dominio es.com.sv con un buzón de 512K de capacidad y ofrecían navegación a 28.8Kbps.

---

[1]Rosa María Elena Cuestas, y Marta Alicia Moreno, *"Avance Tecnológico de las Computadoras en El Salvador y su importancia en el desarrollo del país"*, (tesis de grado Universidad Centroamericana Jose Simeón Cañas, San Salvador, El Salvador, 1979), 30.

[2]José Rivas *Historia de la Computadora en El Salvador,* (El Salvador, blog Hitos salvadoreños en temas de informática, energía, comunicaciones, 2017), 2. http://hist sv.blogsp ot.com/2016/04/historia-de-la-computacion-en-el_23.html.

Se constituye el Comité Nacional de Informática, cni de El Salvador, por parte del conacyt; con el pasar de los años fue una instancia que prácticamente era desconocida incluso para conocedores del sector. Al año siguiente en agosto de 1997 es presentada a la sociedad salvadoreña la Política Nacional de Ciencia y Tecnología, como el resultado de la asistencia de varios sectores académicos, profesionales, empresariales y de gobierno. El conacyt, como dependencia autónoma del Ministerio de Economía, organizó este trabajo.

En noviembre de 1996 y enero de 1998 se registra por los medios de comunicación tradicionales las acciones concretas de Fiscalía General de la República, respaldadas por Business Software Alliancela cual llevo a realizar auditorías al sector privado, para verificar la existencia de piratería.

La Fiscalía explicó que “esto se haría en el marco del combate a la violación a la Ley de Protección a la Propiedad Intelectual y Derechos de Autor”. La bsa explicó en ese momento que en el país el 92% del software era pirateado, y que por esa razón en 1996 en El Salvador se habían tenido pérdidas de unos 11 millones 485 mil dólares.

El delito se contemplaba en el Art. 263 del Código Penal vigente en ese entonces, el uso de programas piratas a ese momento era elevada, pero se tenía una explicación. Era un problema de mercado, culpando a los consumidores.

En ese sentido, los hechos históricos relacionados con el marco legal e institucional es de hacer hincapié que1968 existía el Convenio Centroamericano para la Protección de la Propiedad Intelectual, que aplicaba a todos los países del área, excepto Honduras. Ante el fracaso de la aprobación

del Protocolo de Modificación a dicho Convenio, firmado en San Salvador en 1994, los ministros de economía del istmo, el 17 de septiembre de 1999 acordaron en San José, Costa Rica, denunciar dicho tratado y que cada país redactara su propia ley.[3]

Aunque en el país no es un productor de innovaciones tecnológicas, tampoco está exento de personas, empresas e instituciones que permanecen atentos a las posibles aplicaciones de los avances más importantes en la informática, el tratamiento digital y la transmisión a distancia de la información, datos, imágenes y otras formas de presentar piezas de conocimiento y comunicarse entre los seres humanos.

Un número creciente de profesionales de todas las disciplinas, así como empresarios, empleados, funcionarios y estudiantes de todas las edades comprenden y realizan personalmente la promesa de las tecnologías de información y comunicaciones (TIC).[4]

1.1. Servicios en la internet

Al convertirse el internet en un sistema abierto, éste realiza dos funciones importantes, la primera como medio de comunicación y la segunda como medio de información. Para noviembre de 2001, el informe de la BSA en El Salvador anota que en el país hay un 79% de piratería. Se hace un acuerdo entre Microsoft y el Gobierno para proveer a todos los equipos de oficinas estatales de licencias de ese fabricante. Cinco años después específicamen-

[3]Ibíd.
[4]Lito Ibarra, ¿Cómo está El Salvador en tecnologías de información y comunicaciones (TIC)?, (El Salvador, Blog de Tecnología La Prensa Gráfica, 2011), http://blogs.laprensa grafica.com /litoibarra/?p=1646.

te para agosto de 2007, según la Unión Internacional de Telecomunicaciones -UIT- hasta septiembre de 2006 El Salvador reportaba 637,100 conexiones de internet Según cifras oficiales a mediados de 2006 en el país habría unos 1,526 puntos de acceso conocidos como cibercafés.

En los últimos años el número de conexiones de banda ancha ha crecido, pero también así las deficiencias en el servicio, en nuevo informe de la BSA da a conocer que el país no ha mejorado mucho en cuanta protección de la propiedad de software. El nivel casi es el mismo de hace 10 años.[5]

1.2. Organización de la Internet

Consta, básicamente, de una organización no jerárquica y que todas las computadoras y sistemas de redes con capacidad de acceso a la información, así como de los servicios disponibles en internet, toda esta información y servicios disponibles en internet, toda esta información y servicio no se encuentran depositados en una computadora central o red determinada si no son transmitida en varias computadoras. Tampoco es posible perder la información debido a que se distribuye en la red, encontrando una ruta para recuperarla, con lo que no existe una comunicación directa entre las computadoras a diferencia de la línea telefónica en la que existe un servidor central en la que dependen las comunicaciones entre teléfonos, pero donde la comunicación es directa entre las partes.

1.3. Otras ventajas de la internet

La comunicación exponencial, como los denominados foros de discusión, se lleva a cabo mediante páginas especializadas en el que se mantiene un

[5]Rivas *Historia de la Computadora,* 7.

contacto directo entre las personas a través de preguntas y respuestas, siendo estas unas de las diferentes formas de comunicación a través de la ciberespacio, por otro lado la mensajería instantánea, es considerada como la más eficiente y rápida, permite entablar una conversación escrita por medio de un programa especializado denominado chat, de un usuario a otro, similar a la comunicación telefónica por la característica que es de forma directa, pero con la particularidad que en la web es posible establecer comunicación con múltiples y diferentes personas, ampliando el abanico de posibilidades de recibir y enviar información, inclusive con personas desconocidas.[6]

1.4. Ordenador y sus componentes

El concepto ordenador fue usado por el matemático Húngaro Estadounidense (1903-1957) con el fin de simplificar su propia máquina que podía realizar cálculos.

La Computadora es "una máquina electrónica analógica y digital, dotado de una memoria de tratamiento de la información, capaz de resolver problemas matemáticos y lógicos mediante la utilización automática de programas."

Entendido de otra manera una computadora es un "dispositivo electrónico complejo que puede ser programado para recibir, almacenar, procesar, transmitir y presentar". Ésta se compone de dos elementos esenciales, el software y el hardware, parte importante para una computadora y relacionadas entre sí ya que una no puede existir sin la otra.

[6]Alejandro Armando Montaño Álvareza, *"La problemática jurídica en la regulación de los delitos informáticos",* (tesis de grado, Facultad de Derecho, Universidad Nacional Autónoma de México, 2008), 9.

La capacidad de almacenamiento existen dos tipos de memoria la primara llamada RAM (Random Acceses Memory) la cual consta de pequeñas celdas en un chip que almacenan de forma temporal gran parte de la información, entre mayor, la otra memoria es la ROM (Read Only Memory) consta en memoria semiconductora de lectura utilizada para almacenar datos que nunca necesitan modificarse.[7]

1.5. Denominaciones

Cada servidor de información cuenta con sus propias direcciones, con el fin de acceder de manera fácil y rápida mediante la internet, cada dirección recibe el nombre de dominios, entre los dominios pioneros en el ciberespacio se tiene la World Wide Wed, (WWW), el cual permite extraer elementos de información denominados “documentos” o “páginas web”, estos programas se conocen como exploradores.

Puede referirse a una web, como una página, sitio o conjunto de sitios que proveen información por los medios descritos, también denominada red interconectada, al acceso de la mayoría de sitios de la internet, ejemplo: servicio:// nombre del sistema. dominio. nivel más elevado. Código o país /ruta /archivo; Facultad de Derecho UNAM, el cual codificado se describe http://wwww.derecho.unam.mx. El nivel de domino más elevado es la pieza importante en una dirección, debido a que indica el tipo de organización a la que pertenece el dominio, ejemplos más comunes, se puede mencionar los siguientes:

a) Organismos comerciales. COM

b) Universidades y otras instituciones de enseñanzas. EDU

[7]Ibíd., 10, 11 y 12.

c) Organizaciones gubernamentales o Estatales. GOB. GOV,

d) Sistema de la red y administración de internet, NET

e) Otras organizaciones. ORG

Otra partes importante en la dirección en especial para los portales fuera de los Estados Unidos, es la utilización de códigos referentes al país de origen, por ejemplo: Austria at, Australia au, Belgica be, Gran Bretaña uk.[8]

[8]Ibíd. 21 – 23.

CAPITULO II

LEGISLACION Y MARCO JURIDICO COMPARADO SOBRE LOS DELITOS INFORMATICOS, EN EL CONTEXTO REGIONAL E INTERNACIONAL

A partir de las generalidades, se da lugar, tanto a la diversificación de los delitos tradicionales como a la aparición de nuevos actos ilícitos. Siendo una característica principal, su rapidez y su origen transnacional, siendo difícil individualizarla. En ese sentido la legislación guatemalteca, mexicana, alemana y española, se da a conocer su contexto, finalizando con el convenio de Budapest.

2. Generalidades

El constante progreso tecnológico que experimenta la sociedad, supone una evolución en las formas de delinquir, dando lugar, tanto a la diversificación de los delitos tradicionales como a la aparición de nuevos actos ilícitos. Esta realidad ha originado un debate en torno a la necesidad de distinguir o no los delitos informáticos del resto.

Diversos autores y organismos han propuesto definiciones de los delitos informáticos, aportando distintas perspectivas y matices al concepto. Algunos consideran que es innecesario diferenciar los delitos informáticos de los tradicionales, ya que, según éstos se trata de los mismos delitos, cometidos a través de otros medios. De hecho, el Código Penal español, no contempla los delitos informáticos como tal.

Por otra parte, esta compleja situación y tomando como referencia el “Convenio de Ciber-delincuencia del Consejo de Europa”, se puede definir

los delitos informáticos como: “los actos dirigidos contra la confidencialidad, la integridad y la disponibilidad de los sistemas informáticos, redes y datos informáticos, así como el abuso de dichos sistemas, redes y datos”.

2.1. Características Principales

Según el contexto español, son delitos difíciles de demostrar ya que, en muchos casos, es complicado encontrar las pruebas, depende de actos que pueden llevarse a cabo de forma rápida y sencilla. En ocasiones estos delitos pueden cometerse en cuestión de segundos, utilizando sólo un equipo informático y sin estar presente físicamente en el lugar de los hechos. Los delitos informáticos tienden a proliferar y evolucionar, lo que complica aún más la identificación y persecución de los mismos**.**[9]

Carece de sentido plantearse si la intervención estatal y en particular la intervención penal en internet está justificada o no. La cuestión que hoy debe ser tratada es, pues, directamente la de cómo debe intervenir el Derecho Penal en relación a la aplicaciones y procedimientos informáticos y las redes de transmisión de datos e internet, en un triple sentido: 1) las premisas valorativas en las quede de apoyarse la intervención que conduce a determinar los bienes jurídicos protegidos 2) que tipos de ataques deben ser considerados relevantes, 3) que instrumentos de técnica legislativa resultan preferibles para articular la tutela penal.

De estas tres, la primera es, sin duda, la de mayor importancia. Solo cuando se defina con la suficiente precisión que debe ser protegido en relación a los intereses que se desenvuelven en internet y en las redes de transmisión de

[9] Computer Forensic *definición de delito informático* (El Salvador, recovery labs 2019), 23. htt p://www.delitosinformaticos.info/delitos_informaticos/definicion.html

datos podrá efectuarse de manera certera la determinación de los riesgos, consecuentemente la conductas que deben ser mandadas o prohibidas.[10]

2.2. Legislación guatemalteca

2.2.1. Ámbito de aplicación

La aplicación de una normativa que sancione los actos realizados en el espacio virtual se vuelve compleja, debido a que estos hechos no se desarrollan en un espacio físico o geográfico.

La internet, entendida como una red informática mundial, utilizada como un medio internacional de comunicación no tiene límites políticos, sin embargo todo acto realizado a través de esa red no debe vulnerar los derechos de las personas, tales como la propiedad, la dignidad o el honor entre otros, ni entrañar violación de la ley, la moral o las buenas costumbres.[11]

En atención a lo anterior se deberá tener presente que jurídicamente, territorio no es solamente sinónimo de espacio geográfico, debido a que el territorio comprende todos los lugares a donde se extiende la soberanía del Estado, lo que debe incluir las redes sistemas y ordenadores vinculados al Estado de Guatemala; en atención a este razonamiento, el Código Penal Guatemalteco, que es el cuerpo legal que regula este tipo de ilícitos, establece cual será el ámbito de aplicación de la siguiente manera:

En el Articulo Cuatro del Código Penal, Decreto 17-73 del Congreso Guatemalteco se establece la territorialidad de la ley penal de esta forma: Salvo lo

[10]José María Lidón, *Cuadernos Penales, delitos e informática: Algunos Aspectos*, (Universidad de Deusto, Bilbao, 2007), 13.
[11]Rolando Alvarado y Ronald Morales, *Cibercrimen*, 2° Edición, (IUS Ediciones, España, 2012), VII.

establecido en tratados internacionales, este Código se aplicara a toda persona que cometa delito o falta en el Territorio de La República, o en lugares o vehículos sometidos a su jurisdicción; en este mismo orden de ideas, en el artículo 5 del mismo cuerpo legal, al regular la “extraterritorialidad de la ley penal” en donde se establece que “este código también se aplicara: 1° Por delito cometido en el extranjero por funcionario al servicio de la República, cuando no hubiere sido juzgado en el país en el que se perpetro el hecho. 2° Por el delito cometido en nave, aeronave o cualquier otro medio de transporte guatemalteco, cuando no hubiere sido juzgado en el país en el que se cometió el delito. 3° Por delito cometido por guatemalteco en el extranjero, cuando se hubiese denegado su extradición. 4° Por delito cometido en el extranjero contra guatemalteco, cuando no hubiere sido juzgado en el país de su perpetración, siempre que hubiere acusación de parte o del Ministerio Publico y el imputado se hallare en Guatemala. 5° Por delito que, por tratado o convención, deba sancionarse en Guatemala, aun cuando no hubiere sido cometido en su Territorio. 6° Por delito cometido en el extranjero contra la seguridad del Estado, el orden constitucional, la integridad de su territorio, así como falsificación de la firma del Presidente de la República, falsificación de moneda o de billetes de banco, de curso legal, bonos y demás títulos y documentos de crédito.

2.2.2. Tipificación en el derecho penal guatemalteco

La normativa penal guatemalteca se encuentra que El Congreso de la República introduce modificaciones a la ley sustantiva penal a través del Decreto 33-96 publicado en fecha 21 de junio de 1996. En la normativa ya referida como motivación de la misma se expone: “Que los avances de la tecnología obligan al Estado a legislar en bien de la población de derechos de autor en materia informática tipos delictivos que la legislación no ha

desarrollado". En ese sentido en materia de delitos informáticos se regulan los tipos siguientes:

a) Artículo 274 "A" Destrucción de registros informáticos

b) Artículo 274 "B" Alteración de programas

c) Artículo 274 "C" Reproducción de Instrucciones o programas de Computación

d) Artículo 274 "D" Registros Prohibidos.

e) Artículo 274 "E" Manipulación de Información

f) Artículo 274 "F" Uso de Información

g) Artículo 274 "G" Programas Destructivos

En ese sentido, no están clasificadas específicamente de los delitos informáticos el Código Penal señala otras conductas de las que podrían incluirse de este tipo, (por qué se sirven de un computador para realizarlas o bien van dirigidas a producir daños en el mismo,) de las cuales se enumeran a continuación:

a) Violación a Derechos de Autor: contenida en el artículo 274 del Código Penal.

b) Violación a los Derechos de Propiedad Industrial: contenida en el artículo 275 del Código Penal.

c) Pánico Financiero: contenido en el artículo 342 "B" del Código Penal.

d) Ingreso a espectáculos y distribución de material pornográfico a personas menores de edad contenida en el artículo 189 del Código Penal.

e) Violación a la intimidad sexual contenida en el artículo 190 del Código Penal.

f) Producción de pornografía de personas menores de edad contenida en el artículo 194 del Código Penal.

g) Comercialización o difusión de pornografía de personas menores de edad contenida en el artículo 195 Bis

h) Posesión de material pornográfico de personas menores de edad contenido en el artículo 195 ter.

i) Comercialización de Datos Personales ilícito penal contenido en la Ley de Acceso a la Información Pública, artículo 64.

j) Alteración fraudulenta contenido en el artículo 275 Bis del Código Penal.

2.3. Legislación mexicana

2.3.1. Ámbito de aplicación

Cabe precisar por lo que respecta a los delitos, éstos serán federales o locales conforme a lo señalado por la propia Constitución Federal a través del principio conocido como “reserva legal”, que es la facultad exclusiva del legislador de definir hipótesis delictivas; El artículo 104 de la Constitución Federal, establece que corresponde a los tribunales de la federación conocer

de todas las controversias del orden criminal que se susciten sobre el cumplimiento y aplicación de leyes federales o de los tratados internacionales celebrados por el Estado mexicano. En razón de ello existen tres órbitas de juzgados que operan sobre el mismo territorio pero que entienden en cuestiones materiales diferentes. Así, por ejemplo, en el Estado de Veracruz, existen tribunales federales, así como juzgados de dicha entidad federativa, ambos con poderes de actuación sobre el mismo ámbito territorial (en este caso el Estado de Veracruz) pero entienden sobre hechos materiales diferentes.

Mientras que los tribunales del estado de Veracruz, son competentes para conocer respecto de los delitos en los que se dilucidan conductas tipificadas por el Código Penal vigente en el estado, los tribunales federales conocen, por su parte, de las controversias del orden criminal que se suscitan sobre el cumplimiento y aplicación de leyes federales o de los tratados internacionales celebrados por el Estado mexicano.

Además, los tribunales federales intervienen en los casos en que se solicite la extradición de una persona con motivo de la comisión de un delito. La cuestión que trae el caso bajo análisis debe plantearse en los siguientes términos: Cuando se trata de una conducta lesiva cometida a través del Internet ¿debe comprenderse que la competencia corresponde a los tribunales de la federación o recae en la de las entidades federativas? y de obtenerse una respuesta en tal o cual sentido ¿existe algún motivo jurídico para establecer por qué debe ser uno u otro?, esto es, no se encuentra restringido la penalización de los ilícitos que se cometen a través del Internet a un solo ámbito.

Sin embargo, se considera eminentemente que los delitos que se generen a través del Internet son del orden federal. En efecto, como un primer argu-

mento a favor de establecer que las conductas delictuosas ejecutadas a través de Internet se comprendan en la legislación federal, obedece a que con regular frecuencia se ejecutan por personas que físicamente se encuentran en un país extranjero, situación que desde luego dificulta en gran medida no tan sólo su identificación, sino también su enjuiciamiento.

Otro factor a tomar en cuenta, es que el problema se reduce nuevamente a no entender quién o quiénes son los actores de la red y cuál es la funcionalidad de cada uno. Cierto, por lo general los órganos jurisdiccionales que atienden las consignaciones correspondientes desconocen y les resulta incomprensible el diferente rol que asume por un lado quien ha elaborado y sistematizado la página, que no es necesariamente la misma que presta el servicio de la página de Internet, e incluso, puede intervenir un tercero que sólo se encuentra al acecho para infiltrarse en la PC del usuario, todo ello genera que los procesos jurisdiccionales no se estructuren con una dirección adecuada e incluso con grandes limitantes para una entidad federativa, que conduce a que en muchas ocasiones queden impunes.

De ahí, que la extraterritorialidad, es un elemento clave para dilucidar la conveniencia de que los delitos informáticos sean de competencia de los tribunales de la federación; puesto que a quien le correspondería la investigación y persecución de los delitos sería al Ministerio Público, de acuerdo con lo establece el artículo 21 Constitucional, relativo a la seguridad pública como función a cargo de la Federación, el Distrito Federal, los Estados y los Municipios que comprende la prevención del Delito, según dicho artículo, el órgano institucional a través de la Procuraduría General de la República, es el que está dotado de mayores recursos financieros, así como mayor cobertura para seguir el estudio de los diferentes tipos de actividades ilícitas que se desarrollan a través de Internet, e incluso al unir

esfuerzos con las diferentes corporaciones policiacas como lo puede ser la interpol, dado su carácter trasnacional, puede coadyuvar a la investigación de los hechos delictuosos, compartiendo información y estableciendo redes de comunicación a su vez, con otras instituciones de policías cibernéticas.

En México ya existe una unidad especializada en delitos informáticos de la Procuraduría General de la República, por lo que sería más conveniente aprovechar los recursos y cobertura tecnológica que se le han asignado para tratar de contrarrestar los ilícitos informáticos que se cometen a través de Internet.[12]Con lo anterior se puede entender entonces la calificación de "delito informático" no como un delito per se, ya que el carácter esencial para el derecho penal es la conducta. Sin embargo, a diferencia de lo señalado por el autor antes citado, se considera que el problema no está en la constitución del delito sino en la forma de probar el mismo, en la forma de establecer fehacientemente el nexo causal. Lo etéreo de una página web, la manera tan sencilla de enviar un virus en la web desde cualquier lugar del mundo.

El problema estriba en encontrar al autor de ese delito, saber dónde lo cometió y donde o que afecto, cabe preguntarse lo siguiente ¿se juzgara donde se fabricó el virus o donde se hizo daño?, ¿ambas legislaciones lo comprenden como delito?, la solución pasa necesaria necesariamente por una coordinación internacional, tanto a la hora de investigar como a la hora de aplicar unas leyes que deben contar con un núcleo común, es decir hay que unificar criterios, en este sentido está trabajando por ejemplo la Unión Europea (Convenio de Budapest).[13]

[12]Jorge Esteban Cassou Ruiz, "Delitos Informáticos en México", *Revista del Instituto de la Judicatura Federal, No. 28, México*, (2015): 216.
[13]Alberto Nava Garces *Delitos Informáticos*, 3° Edición (Editorial Porrúa, México, 2007), 141-142.

Antes que se hiciera un catálogo de conductas, como se encuentra en el Convenio de Budapest, en el año 1999 se incorporaron delitos informáticos al Código Penal Federal Mexicano, los cuales no son aplicables sino cuando se dan las condiciones de competencia que señalan los artículos 104 de la Constitución Política de los Estados Unidos Mexicanos y el Articulo 50 de la Ley Orgánica del Poder Judicial de la Federación.[14]

En el año de 1999 se incorporaron al Código Penal Federal siete artículos para tipificar los delitos informáticos. Sin tener en claro el bien jurídico tutelado se estableció bajo el capítulo de revelación de secretos y acceso ilícito a equipos informáticos. El Código Penal Federal establece:

2.3.2. Tipificación en el derecho penal mexicano

El título noveno, el cual hace referencia a la "Revelación de Secretos y Acceso Ilícito a Sistemas y Equipos de Informática", que incluye en el mencionado título el capítulo II. "Acceso Ilícito a Sistemas y Equipos de Informática", se tipifican los siguientes tipos penales, los cuales son motivos de infracción, los cuales pueden ser sancionados con multa o cárcel, según sea la gravedad en el marco regulatorio mexicano: Artículo 211bis 1.

Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a dos años de prisión y de cien a trescientos días multa. Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, se le impondrán de tres meses a un año de prisión y de cincuenta a ciento cincuenta días multa.

[14] Ibíd.

El artículo siguiente es decir el 211 numeral segundo. Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática del Estado, protegidos por algún mecanismo de seguridad, se le impondrán de uno a cuatro años de prisión y de doscientos a seiscientos días multa. Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática del Estado, protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a dos años de prisión y de cien a trescientos días multa.

Se agrava a quien sin autorización conozca, obtenga, copie o utilice información contenida en cualquier sistema, equipo o medio de almacena-miento informáticos de seguridad pública, protegido por algún medio de seguridad, 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. Si el responsable es o hubiera sido servidor público en una institución de seguridad pública, se impondrá, además, destitución e inhabilitación de cuatro a diez años para desempeñarse en otro empleo, puesto, cargo o comisión pública.

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. De igual forma el Artículo 211 numeral tercero. Estando autorizado para acceder a sistemas y equipos de informática del Estado, indebidamente modifique, destruya o provoque pérdida de información que contengan, se le impondrán de dos a ocho años de prisión y de trescientos a novecientos días multa.

Se agrava en los siguientes casos: 1) Estando autorizado para acceder a

sistemas y equipos de informática del Estado, indebidamente copie información que contengan, se le impondrán de uno a cuatro años de prisión y de ciento cincuenta a cuatrocientos cincuenta días multa. 2) 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. 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.

Por lo tanto, con la tipificación el artículo 211 numeral cuarto. Establece 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, protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a cuatro años de prisión y de cien a seiscientos días multa.

De igual forma al que sin autorización conozca o copie información contenida en sistemas o equipos de informática de las instituciones que integran el sistema financiero, protegidos por algún mecanismo de seguridad, se le impondrán de tres meses a dos años de prisión y de cincuenta a trescientos días multa. El artículo 211 numeral quinto. 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.

De igual forma la figura de la persona autorizada para acceder a sistemas y equipos de informática de las instituciones que integran el sistema financiero, indebidamente copie información que contengan, se le impondrán de tres meses a dos años de prisión y de cincuenta a trescientos días multa.

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. Así como el artículo 211 numeral sexto.

Para los efectos de los artículos 211 numeral cuarto y 211 numeral quinto anteriores, se entiende por instituciones que integran el sistema financiero, las señaladas en el artículo 400 Bis de este Código, los cuales fueron objeto de reforma, adicionado los artículos mediante Decreto publicado en el Diario Oficial de la Federación el 17 de mayo de 1999, por último, el artículo 211 numeral séptimo. Las penas previstas en este capítulo se aumentarán hasta en una mitad cuando la información obtenida se utilice en provecho propio o ajeno.

Es de aclarar que los artículos relacionados anteriormente son parte del marco regulatorio federal, es decir aplicables en los Estados Unidos Mexicanos, existiendo marcos regulatorios del bien jurídico protegido como lo es la información a nivel estatal.

2.4. Legislación alemana

2.4.1. Ámbito de aplicación

El modelo alemán seguido por la legislación penal alemana respecto a la lucha contra la criminalidad informática, se construye sobre la base de

identificar dos supuestos de acciones atentatorias para determinados bienes jurídicos. Se tipifica al fraude informático y al delito de sabotaje informático.

El bien jurídico protegido primordialmente es el patrimonio. En cuanto a conductas atentatorias a la vida personal y la privacidad, el Código penal alemán sanciona el espionaje de datos, pero excluye la información que se encuentre almacenada o que pueda ser transmitida electrónica o magnéticamente o transmitida de forma inmediatamente accesible.

Con ello, prácticamente no se regula ningún tipo penal que pudiera estar referido a un espionaje de datos informatizados. No se quiso punir la mera intrusión informática, sino sólo en aquellos casos de conductas que signifiquen la manipulación de las computadoras y persigan un ánimo de lucro.

2.4.2. Tipificación

En Alemania, para hacer frente a la delincuencia relacionada con la informática y con efectos a partir del 1 de agosto de 1986, se adoptó la Segunda Ley contra la Criminalidad Económica del 15 de mayo de 1986, en la que se contemplan los siguientes delitos: a) espionaje de datos b) Estafa Informática y c) falsificación de datos probatorios entre otros[15], tipificación que posteriormente fue introducida al Código Penal Alemán y en la que se contemplan los siguientes delitos:

Piratería Informática; delito que se regula en el Articulo 202 literal A, del cuerpo legal anteriormente mencionado y cuyo texto dice: “Al que sin autorización se procure para sí, o para terceros, datos que no están destinados

[15]Miguel Estrada Garavilla, *Los Delitos Informáticos tratamiento Internacional,* (El Salvador, 2016). https://la-razon.com/la_gaceta_juridica/delitos-informaticos-Tratamiento-internacional_0_2450155056.html.

para él y que están especialmente protegidos contra el acceso no autorizado, será castigado con prisión de hasta tres años o con pena de multa".

Los datos a los que se refiere el artículo anteriormente mencionado son aquellos que datos electrónicos, magnéticos o no inmediatamente perceptibles, que son almacenados o transmitidos por medio de un equipo informático.

Estafa informática; Delito regulado en el Articulo 263 literal A del Código Penal Alemán, el cual literalmente dice: "Quien, con el propósito de obtener una ventaja patrimonial antijurídica para sí o para un tercero, perjudica el patrimonio de otro, influyendo en el resultado de un proceso de tratamiento de datos, a través de una errónea configuración del programa, a través del uso de datos incorrectos o incompletos, a través del uso no autorizado de datos, o de otra manera a través de una intervención no autorizada en el proceso, se castiga con privación de libertad de hasta cinco años o con multa".

El hecho punible sobre el cual se relaciona el artículo tiene que influir en el proceso de tratamiento de datos informáticos. Esto significa que el autor influye de tal manera que se llega a cambiar el resultado de los datos almacenados en el computador, y el de aquellos que sean utilizados por el programa de trabajo. No juega ningún papel si se pone en marcha un nuevo proceso de tratamiento de datos, o si influye en uno ya existente. Sobre este elemento, se señala en la historia fidedigna de la ley, que la influencia sobre el resultado de un proceso de tratamiento de datos se refiere a aquellos casos en que el autor no se sirve de un computador, sino que influye en una persona, p. ej., en el resultado de un proceso de pensar y decidir, y esta paráfrasis cubriría, en relación con el tipo de estafa, tanto la disposición patrimonial como el error.

Corresponde al proceso de pensar y decidir erróneo el proceso de tratamiento de datos determinado que conduzca a la utilización de los medios mencionados en el tipo, forzando técnicamente a un resultado falso, donde, sin embargo, se comprende la no mencionada –en Alemania– "disposición patrimonial" del tipo de estafa. Por esto, este elemento, en relación con el propósito de enriquecimiento exigido en el tipo subjetivo, hace que el articulo 263 literal a, también sea un delito de desplazamiento patrimonial.

En el lugar de la disposición patrimonial condicionada por error, exigida para el artículo 263 literal a, va la potencialidad del computador falsificada por el autor que conduce a una desventaja del interesado79. Para terminar, a partir de esto, por tanto, se tiene que concluir que la clara intención del legislador alemán es que, en todo caso, el abuso de tarjetas bancarias, de otras tarjetas de código, y de procedimientos técnicos de pago similares, se tengan que juzgar exclusivamente acorde al artículo 263 literal a, pues el engaño del concepto de estafa acontece exactamente con referencia a este tipo de constelaciones.

Por lo tanto, la obtención de dinero en efectivo por el no autorizado, sobre instalaciones técnicas de este tipo, se comprendería únicamente por el artículo 263 literal a como ley especial.

Otro delito tipificado en la Legislación alemana es la Falsificación de datos probatorios regulado en el Artículo 269 del Código Penal Alemán junto a modificaciones complementarias del resto de falsedades documentales como el engaño en el tráfico jurídico mediante la elaboración de datos, falsedad ideológica, uso de documentos falsos (270, 271, 273 del Código Penal Alemán); El artículo 269 tiene como fin proteger a las relaciones jurídicas en

términos de datos de prueba. Permite un castigo en los casos en que los datos no son objetivamente perceptibles y la aplicación del artículo 267 del mismo cuerpo legal.

De igual forma en el Código Penal Alemán se encuentra penalizada la alteración de datos de conformidad al Artículo 303 literal A, en donde se establece que es ilícito cancelar, inutilizar o alterar datos e inclusive la tentativa es punible; lo anterior directamente relacionado con el Articulo 202 literal A, relacionado a la piratería informática.

Asimismo, en el Código Penal Alemán se regula el delito de sabotaje informático en el artículo 303 literal b, el cual literalmente dice: Quien perturba un procesamiento de datos que sea de importancia esencial para una empresa ajena, una industria ajena o una autoridad para, cometer un hecho según el art. 303 a, inciso 1, o; 2. destruir, dañar, inutilizar, eliminar o modificar un equipo de procesamiento de datos o un medio de datos será castigado con pena privativa de la libertad hasta cinco años o con multa; La tentativa es punible.

La Utilización abusiva de cheques o tarjetas de crédito (Art.266b del Código Penal Alemán). Por lo que se refiere a la estafa informática, la formulación de un nuevo tipo penal tuvo como dificultad principal el hallar un equivalente análogo al triple requisito de acción engañosa, causa del error y disposición patrimonial, en el engaño del computador.

Así como en garantizar las posibilidades de control de la nueva expresión legal, quedando en la redacción que el perjuicio patrimonial que se comete consiste en influir en el resultado de una elaboración de datos por medio de una realización incorrecta del programa, a través de la utilización de datos

incorrectos o incompletos, mediante la utilización no autorizada de datos, o a través de una intervención ilícita.

En ese sentido, cabe mencionar que esta solución, en forma parcialmente abreviada, fue también adoptada en los Países Escandinavos y en Austria. Como se puede observar el legislador alemán ha introducido un considerable número de nuevos preceptos penales, pero no ha llegado tan lejos como otras legislaciones. De esta forma, no sólo ha renunciado a tipificar la mera penetración no autorizada en sistemas ajenos de computadoras, sino que tampoco ha castigado el uso no autorizado de equipos de procesos de datos, aunque tenga lugar de forma cualificada.

Por lo tanto, en el caso de Alemania, se ha señalado que a la hora de introducir nuevos preceptos penales para la represión de la llamada criminalidad informática el gobierno tuvo que reflexionar acerca de dónde radicaban las verdaderas dificultades para la aplicación del Derecho penal tradicional a comportamientos dañosos en los que desempeña un papel esencial la introducción del proceso electrónico de datos, así como acerca de qué bienes jurídicos merecedores de protección penal resultaban así lesionados.

Asimismo, se comprobó que, por una parte, en la medida en que las instalaciones de tratamiento electrónico de datos son utilizadas para la comisión de hechos delictivos, en especial en el ámbito económico, pueden conferir a éstos una nueva dimensión, pero que en realidad tan sólo constituyen un nuevo modus operandi, que no ofrece problemas para la aplicación de determinados tipos.

Por otra parte, sin embargo, la protección fragmentaria de determinados bienes jurídicos ha puesto de relieve que éstos no pueden ser protegidos

suficientemente por el Derecho vigente contra nuevas formas de agresión que pasan por la utilización abusiva de instalaciones informáticas.

En otro orden de ideas, las diversas formas de aparición de la criminalidad informática propician, además, la aparición de nuevas lesiones de bienes jurídicos merecedoras de pena, en especial en la medida en que el objeto de la acción puedan ser datos almacenados o transmitidos o se trate del daño a sistemas informáticos. [16] El tipo de daños protege cosas corporales contra menoscabos de sus sustancias o función de alteraciones de su forma de aparición.

2.5. Legislación española

2.5.1. Tipificación y ámbito de aplicación

Aunque los delitos informáticos no están contemplados como un tipo especial de delito en la legislación española, existen varias normas relacionadas con este tipo de conductas:

a) Ley Orgánica de Protección de Datos de Carácter Personal.

b) Reglamento de medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal.

c) Ley de Servicios de la Sociedad de la Información y Comercio Electrónico.

d) Ley General de Telecomunicaciones.

e) Ley de Propiedad Intelectual

[16]Código procesal penal alemán, 15 de mayo de 1871, reforma 31 de enero de 1998.

f) Ley de Firma Electrónica.[17]

A partir de la creación de la Ley Orgánica de Protección de Datos de Carácter Personal, publicado en el Boletín Oficial del Estado BOE número 298, el 14 de diciembre de 1999, la cual entro en vigencia el 14 de enero del año 2000, la cual fue objeto de revisión en el 6 de marzo del año 2011[18]. En su ámbito de aplicación a los datos de carácter personal registrados en soporte físico, que los haga susceptibles de tratamiento, y a toda modalidad de uso posterior de estos datos por los sectores público y privado.

Se entiende, datos de carácter personal: cualquier información concerniente a personas físicas identificadas o identificables. El tratamiento de datos se define como las operaciones y procedimientos técnicos de carácter automatizado o no, que permitan la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias, como lo establece los artículos 2 y 3 de esta ley[19]

La particularidad de la Ley Orgánica de protección de datos de carácter Personal, radica en la importancia que tiene la seguridad, el acceso, así como su naturaleza (público y privado), establece una estructura definida en cuanto que delimita actores, su participación, así como sus posibles sanciones, tomando de base los derechos de las personas; Los datos de carácter personal que hagan referencia al origen racial, a la salud y a la vida sexual sólo podrán ser recabados, tratados y cedidos cuando, por razones

[17]Division Computer Forensic *Delitos Informáticos*, (España, 2016), https://delitosinformaticos.info/delitos_informaticos/legislacion.html.
[18]Noticia jurídica, Ley *Orgánica de Protección de Datos de Carácter Personal* (España, 1999). http://noticias.juridicas.com/base_datos/Admin/lo15-1999.html
[19]Agencia Estatal *Boletín Oficial del Estado*, (España, 2016). https://boe.es/buscar/act.php?id=BOE-A-1999-23750.

de interés general, así lo disponga una ley o el afectado consienta expresamente, articulo 7 literal 3 de la Ley Orgánica de protección de Datos de Carácter Personal, secreto profesional respecto de los mismos y al deber de guardarlos, obligaciones que subsistirán aun después de finalizar sus relaciones con el titular del fichero o, en su caso, con el responsable del mismo.[20]

El reglamento de medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal, aprobado el 11 de julio de 1999, por medio del Real Decreto 994/1999, nuevamente establece, en su ámbito de aplicación garantizar la seguridad que deben de reunir los ficheros automatizados, en cuanto al tratamiento de datos de carácter personal, el cual es un conjunto de programas, soporte y equipos empleados para el almacenamiento y tratamiento de datos[21]

En materia económica Ley de Servicios de la Sociedad de la Información y Comercio Electrónico, establece en concepto amplio el "servicios de la sociedad de la información", que engloba los siguientes aspectos1) contratación de bienes y servicios por vía electrónica, 2) suministro de información por dicho medio (como el que efectúan los periódicos o revistas que pueden encontrarse en la red), 3) las actividades de intermediación relativas a la provisión de acceso a la red, a la transmisión de datos por redes de telecomunicaciones, a la realización de copia temporal de las páginas de Internet solicitadas por los usuarios, 4) alojamiento en los propios servidores de información, servicios o aplicaciones facilitados por otros o a la provisión de instrumentos de búsqueda o de enlaces a otros sitios de

[20]Computer Forensic *definición de delito informático,* 25.
[21]Campus Usal, *Reglamento de medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal,* (España, 2016), Artículo 1. https://www.boe.es/buscar/doc.php?id=BOE-A-1999-13967.

Internet, así como cualquier otro servicio que se preste a petición individual de los usuarios (descarga de archivos de vídeo o audio...), siempre que represente una actividad económica para el prestador.

Estos servicios son ofrecidos por los operadores de telecomunicaciones, los proveedores de acceso a Internet, los portales, los motores de búsqueda o cualquier otro sujeto que disponga de un sitio en Internet a través del que realice alguna de las actividades indicadas, incluido el comercio electrónico.

Desde un punto de vista subjetivo, la Ley se aplica, con carácter general, a los prestadores de servicios establecidos en España. Por "establecimiento" se entiende el lugar desde el que se dirige y gestiona una actividad económica, definición esta que se inspira en el concepto de domicilio fiscal recogido en las normas tributarias españolas y que resulta compatible con la noción material de establecimiento predicada por el Derecho comunitario.

La Ley resulta igualmente aplicable a quienes sin ser residentes en España prestan servicios de la sociedad de la información a través de un "establecimiento permanente" situado en España. En este último caso, la sujeción a la Ley es únicamente parcial, respecto a aquellos servicios que se presten desde España.

El lugar de establecimiento del prestador de servicios es un elemento esencial en la Ley, porque de él depende el ámbito de aplicación no sólo de esta Ley, sino de todas las demás disposiciones del ordenamiento español que les sean de aplicación, en función de la actividad que desarrollen, asimismo, las obligaciones y responsabilidades de los prestadores de servicios que realicen actividades de intermediación como las de transmisión, copia, alojamiento y localización de datos en la red.

En general, éstas imponen a dichos prestadores un deber de colaboración para impedir que determinados servicios o contenidos ilícitos se sigan divulgando. Las responsabilidades que pueden derivar del incumplimiento de estas normas no son sólo de orden administrativo, sino de tipo civil o penal, según los bienes jurídicos afectados y las normas que resulten aplicables.

Es objeto de la presente Ley la regulación del régimen jurídico de los servicios de la sociedad de la información y de la contratación por vía electrónica, en lo referente a las obligaciones de los prestadores de servicios incluidos los que actúan como intermediarios en la transmisión de contenidos por las redes de telecomunicaciones, las comunicaciones comerciales por vía electrónica, la información previa y posterior a la celebración de contratos electrónicos, las condiciones relativas a su validez y eficacia y el régimen sancionador aplicable a los prestadores de servicios de la sociedad de la información.

Las disposiciones contenidas en esta Ley se entenderán sin perjuicio de lo dispuesto en otras normas estatales o autonómicas ajenas al ámbito normativo coordinado, o que tengan como finalidad la protección de la salud y seguridad pública, incluida la salvaguarda de la defensa nacional, los intereses del consumidor, el régimen tributario aplicable a los servicios de la sociedad de la información, la protección de datos personales y la normativa reguladora de defensa de la competencia.[22].

La Ley General de Telecomunicaciones, promulgada el 9 de mayo de 2014, en el Boletín Oficial del Estado número 114, Sec. I, pagina 35824, España, la cual fue modificada en el marco europeo está compuesto por la Directiva 2009/136/CE, del Parlamento Europeo y del Consejo, de 25 de noviembre de

[22] Boe.es Ley de Servicios de la Sociedad de la Información y Comercio Electrónico (España, 2016), 2. https://www.boe.es/buscar/act.php?id=BOE-A-2002-13758.

2009 (Derechos de los Usuarios), y la Directiva 2009/140/CE, del Parlamento Europeo y del Consejo, de 25 de noviembre de 2009 (Mejor Regulación), y a partir del mismo se introducen en la Ley medidas destinadas a crear un marco adecuado para la realización de inversiones en el despliegue de redes de nueva generación, de modo que se permita a los operadores ofrecer servicios innovadores y tecnológicamente más adecuados a las necesidades de los ciudadanos.[23]

Además de estas normas, en el Código Penal español, se incluyen multitud de conductas ilícitas relacionadas con los delitos informáticos. Las que más se aproximan a la clasificación propuesta por el "Convenio sobre la Ciber-delincuencia" se reflejan en los siguientes artículos descritos a continuación:

a) Delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos, artículo 197 contempla las penas con las que se castigará: 1) quien, con el fin de descubrir los secretos o vulnerar la intimidad de otro, se apodere de cualquier documentación o efecto personal, intercepte sus telecomunicaciones o utilice artificios de escucha, transmisión, grabación o reproducción de cualquier señal de comunicación, 2) a quien acceda por cualquier medio, utilice o modifique, en perjuicio de terceros, a datos reservados de carácter personal o familiar, registrados o almacenados en cualquier tipo de soporte, 3) cuando se difunden, revelan o ceden a terceros los datos o hechos descubiertos. El artículo 278.1 por otra parte se exponen las penas con las que se castigará a quien lleve a cabo las mismas acciones expuestas anteriormente, pero con el fin de descubrir secretos de empresa. Finalmente, en artículo 264.2 se abordan las penas que se impondrán al que por cualquier medio destruya, altere, inutilice o de cualquier otro modo

[23]Boe.es Boletín Oficial del Estado (España, 2016), 5. https://www.boe.es/buscar/act.php?id=BOE-A-2002-13758.

dañe los datos, programas o documentos electrónicos ajenos contenidos en redes, soportes o sistemas informáticos.

b) Delitos informáticos: Los artículos 248 y 249 tratan las estafas, en concreto el artículo 248.2 considera las estafas llevadas a cabo mediante manipulación informática o artificios semejantes. Los artículos 255 y 256 mencionan las penas que se impondrán a quienes cometan defraudaciones utilizando, entre otros medios, las telecomunicaciones.

Los delitos informáticos propiamente establecidos en el Código Penal Español, se pueden categorizar: contra su contenido y contra su propiedad intelectual

a) Delitos relacionados con el contenido: El artículo 186 cita las penas que se impondrán a aquellos, que, por cualquier medio directo, vendan, difundan o exhiban material pornográfico entre menores de edad o incapaces. El artículo 189 trata las medidas que se impondrán quien utilice a menores de edad o a incapaces con fines exhibicionistas o pornográficos, y quien produzca, venda, distribuya, exhiba o facilite la producción, venta, distribución o exhibición de material pornográfico, en cuya elaboración se hayan utilizado menores de edad o incapaces.

b) Delitos relacionados con infracciones de la propiedad intelectual y derechos afines, el articulo 270 enuncia las penas con las que se castigará a quienes reproduzcan, distribuyan o comuniquen públicamente, una parte o la totalidad, de una obra literaria, artística o científica, con ánimo de lucro y en perjuicio de terceros, agravándose en el artículo 273 trata las penas que se impondrán a quienes sin consentimiento del titular de una patente, fabrique, importe, posea, utilice, ofrezca o introduzca en el comercio,

objetos amparados por tales derechos, con fines comerciales o industriales.

En el tema de las obligaciones en cuanto a la seguridad de información el artículo 12 bis. Establece la siguiente regulación:

a) Los proveedores de servicios de intermediación establecidos en España de acuerdo con lo dispuesto en el artículo 2 de esta Ley que realicen actividades consistentes en la prestación de servicios de acceso a Internet, estarán obligados a informar a sus clientes de forma permanente, fácil, directa y gratuita, sobre los diferentes medios de carácter técnico que aumenten los niveles de la seguridad de la información y permitan, entre otros, la protección frente a virus informáticos y programas espía, y la restricción de los correos electrónicos no solicitados.

b) Los proveedores de servicios de acceso a Internet y los prestadores de servicios de correo electrónico o de servicios similares deberán informar a sus clientes de forma permanente, fácil, directa y gratuita sobre las medidas de seguridad que apliquen en la provisión de los mencionados servicios.

c) Igualmente, los proveedores de servicios referidos en el apartado 1 informarán sobre las herramientas existentes para el filtrado y restricción del acceso a determinados contenidos y servicios en Internet no deseados o que puedan resultar nocivos para la juventud y la infancia.

d) Los proveedores de servicios mencionados en el apartado 1 facilitarán información a sus clientes acerca de las posibles responsabilidades en que puedan incurrir por el uso de Internet con fines ilícitos, en particular,

para la comisión de ilícitos penales y por la vulneración de la legislación en materia de propiedad intelectual e industrial.

e) Las obligaciones de información referidas en los apartados anteriores se darán por cumplidas si el correspondiente proveedor incluye la información exigida en su página o sitio principal de Internet en la forma establecida en los mencionados apartados.[24]

2.6. Convenio de Budapest

Como lo ha venido desarrollando en el contexto internacional y la legislación comparada, así como las definiciones básicas y elementos que conformar los delitos cibernéticos también denominada ciber-delincuencia se puede determinar que consiste en toda acción antijurídica, típica y culpable que se realiza, con el objetivo de destruir y dañar computadoras, así como redes por vías informáticas. Aunque las nuevas tecnologías y las conductas delictivas a ellas asociadas se actualizan rápidamente, la legislación siempre se encuentra un paso detrás, lo cual provoca que no todas las conductas criminales estén tipificadas y, por ende, no puedan ser consideradas como delitos. Partiendo de esa afirmación El Convenio sobre ciberdelincuencia, también conocido como el Convenio de Budapest sobre ciberdelincuencia o simplemente como Convenio Budapest, es el primer tratado internacional que busca hacer frente a este fenómeno.

A nivel internacional aparece enmarcado este esfuerzo específicamente el 23 de noviembre del año 2001, se abrió a la firma en Budapest y entró en vigor el 1 de julio de 2004, como el primer tratado que establece delitos penales cometidos a través de medios informáticos con el fin de combatir no sólo los

[24]Computer Forensic *definición de delito informático,* 29.

ciber delitos sino también aquellos delitos cometidos en Internet. elaborado por el Consejo de Europa en Strasbourg con la participación activa de los "Estados Observadores": Canadá, Japón y China. Gracias a él, se establecieron reglas de cooperación internacional para que los países miembros puedan hacer frente a esta nueva delincuencia mediante la armonización de leyes nacionales y la optimización de las técnicas de investigación.

Los esfuerzos relevantes fue la determinación en que las partes adoptarán las medidas necesarias para establecer poderes y procedimientos a los efectos de investigación, o procedimientos penales específicos para ser aplicados a infracciones penales ya previstas en dicho Convenio, u otras de carácter informático, o para la recogida de pruebas electrónicas de cualquier infracción penal, según el artículo 14 del Convenio. Estos se aplicarán sometiéndose a las condiciones y garantías dispuestas en el derecho interno de cada Estado, de manera que se asegure una protección adecuada de los derechos del hombre y de las libertades, como la supervisión judicial u otras formas de supervisión independiente, teniendo siempre en mira el interés público y una buena administración de justicia

Los aspectos relevantes del convenio resalta tres, en primer lugar, conforme a los artículos 16 y 17, se prevé empoderar a las autoridades competentes para ordenar a una persona la conservación inmediata de datos electrónicos especificados, manteniéndolos íntegros durante un plazo máximo de 90 días, en el que deberá mantener el secreto de dichas medidas y luego del cual las autoridades competentes podrán obtener su revelación.

En segundo lugar, lo establecido en el artículo 18, se prevé empoderar a las autoridades competentes para ordenar a una persona la comunicación inmediata de datos electrónicos especificados que se encuentren bajo su

poder y control –incluidos los prestadores de servicios-, almacenados en un sistema o soporte informático.

La información a comunicar por los prestadores de servicios será sobre sus abonados. Puede incluir tanto datos de tráfico como de contenido, como sea el tipo de servicio de comunicación utilizado, las disposiciones técnicas adoptadas, el tiempo del servicio, la identidad, la dirección postal, el número de teléfono del abonado o cualquier otro número de acceso, los datos relativos a la facturación y al pago.

En tercer lugar, el artículo 19 que también se prevé empoderar a las autoridades competentes para registrar o acceder a un sistema informático específico o soporte de almacenamiento informático determinado y los datos en ellos contenidos, para decomisar, realizar y conservar una copia de los mismos y tomar las medidas necesarias para preservar la integridad de los datos informáticos pertinentes y para exigir a la persona que conozca el funcionamiento del sistema informático o medidas aplicadas para su protección, que proporcione todo lo razonablemente necesario para aplicar las medidas antes descriptas.[25]

El convenio de Budapest, aborda ampliamente el fenómeno de la pornografía infantil, específicamente en el artículo 9, el cual a partir del año 2016, existe una nueva etimología para el tratamiento de explotación y abuso infantil (reglas de Luxemburgo).[26] El convenio de Budapest logro establecer un esquema de trabajo en tres áreas:

[25]The Franco Journal, *ciber-delincuencia y el Convenio de Budapest* (Budapest, 2017) https://thefrancojournal.com/2015/06/24/la-ciberdelincuencia-y-el-convenio-de-budapest/.
[26] ONU *Orientaciones terminológicas para la protección de niñas niños y adolescentes contra la explotación y el abuso infantil,* (España, 2017). http://srsg.violenceagainstchildren .org/site s/default/files/documents/docs/Terminology%20guidelines_SPA.pdf

a) Los que atentan contra la confidencialidad

b) Los delitos relacionados con el contenido

c) Los delitos informáticos propiamente establecidos

La cooperación internacional para poder minimizar efectivamente este fenómeno, es fundamental, para que todo lo que regula, tipifica y se sanciona a nivel local como internacional, tenga impactos positivos en una sociedad globalizada que depende de la tecnología, contra restando aquellas conductas que dañan o lesionan los bienes jurídicos protegidos, es por ello que retomando el estudio exhaustivo del problema del delito cibernético y las respuestas de los Estados miembros, la comunidad internacional y el sector privado ante ese fenómeno, Los países que respondieron al cuestionario del estudio señalan que entre el 30% y el 70% de los delitos cibernéticos tienen una dimensión transnacional, con lo cual se plantean cuestiones de investigaciones transnacionales, soberanía, jurisdicción, pruebas extraterritoriales y requerimientos de cooperación internacional.

La dimensión transnacional de un delito cibernético se presenta cuando un elemento o un efecto considerable del delito se dan en otro territorio, o cuando parte del modus operandi está en otro territorio. El derecho internacional establece distintas bases de atribución de la jurisdicción aplicable a estos actos, como la jurisdicción según el territorio y la jurisdicción según la nacionalidad.

Algunas de estas normas también figuran en instrumentos multilaterales sobre el delito cibernético. Mientras que todos los países de Europa consideran que el derecho nacional brinda un marco suficiente para la tipificación del delito cibernético y para el enjuiciamiento en caso de actos

extraterritoriales, entre un tercio y más de la mitad de los países en otras regiones del mundo señalan marcos jurídicos insuficientes.

En muchos países las disposiciones reflejan la idea de que no hace falta que “todo” el acto delictivo se realice en un país para afirmar la jurisdicción territorial. Se pueden establecer vínculos territoriales con respecto a los elementos o efectos del acto, o a la ubicación de los sistemas o datos informáticos empleados en la comisión del delito. Cuando se plantea un conflicto jurisdiccional, generalmente se resuelve con consultas oficiales u oficiosas entre los países. Las respuestas de los países no muestran, en la actualidad, ninguna necesidad de contar con formas adicionales de jurisdicción sobre una presunta dimensión de “ciberespacio”. Más bien las formas de jurisdicción según la territorialidad o según la nacionalidad casi siempre permiten establecer una relación suficiente entre los actos delictivos cibernéticos y al menos un Estado. 28.

Las formas de cooperación internacional incluyen la extradición, la asistencia jurídica recíproca, el reconocimiento recíproco de la sentencia extranjera y la cooperación oficiosa entre policía y policía. Debido al carácter volátil de la prueba electrónica la cooperación internacional en asuntos penales en la esfera de los delitos cibernéticos requiere una respuesta pronta y la habilidad de solicitar diligencias investigativas especializadas, como por ejemplo la conservación de los datos informáticos.

El recurso a formas tradicionales de cooperación es lo más usual para obtener pruebas extraterritoriales en los casos de delincuencia cibernética, ya que más del 70% de los países señalan para este fin el empleo de solicitudes oficiales de asistencia jurídica recíproca. De este tipo de cooperación oficial casi el 60% de las solicitudes se fundan en instrumentos bilaterales.

Los instrumentos multilaterales sirven de fundamento en el 20% de los casos. Se comunicó que el tiempo de respuesta en el caso de los mecanismos oficiales era de meses, tanto para la extradición como para la solicitud de asistencia jurídica recíproca, un plazo que presenta un problema para la recopilación de pruebas electrónicas volátiles. El 60% de los países de África, América y Europa, y el 20% de Asia y Oceanía, comunicaron canales para solicitudes urgentes. Sin embargo, no está claro qué consecuencias tiene esto para el plazo de respuesta. Aproximadamente los dos tercios de los países que respondieron admiten modos oficiosos de cooperación, aunque pocos países tienen una política para el empleo de estos mecanismos.

Las iniciativas para una cooperación oficiosa y para facilitar la cooperación oficial, como por ejemplo redes 24/7, presentan grandes posibilidades de lograr respuestas más rápidas. Sin embargo, se utilizan muy poco, ya que se recurre a ellos en el 3% del total de casos de delitos cibernéticos en manos de las fuerzas del orden del grupo de países que contestaron. 29.

Se han previsto modos oficiales y oficiosos de cooperación que guían el procedimiento de lograr el consentimiento de un Estado para que fuerzas del orden extranjeras realicen investigaciones que afectan su soberanía. Pero cada vez más los investigadores, a sabiendas o no, acceden a datos extraterritoriales en ocasión de reunir pruebas, sin el consentimiento del Estado donde están físicamente situadas. Una de las razones de que se presente esta situación es la informática en la nube, que implica el almacenamiento de los datos en múltiples centros de datos situados en diferentes ubicaciones geográficas.

La “ubicación” de los datos, si bien es técnicamente posible de conocer, es cada vez más artificial, al grado de que las solicitudes tradicionales de

asistencia jurídica recíproca suelen dirigirse al país sede del proveedor del servicio más que al país donde el centro de datos está físicamente ubicado. El acceso directo de fuerzas del orden extranjero a datos extraterritoriales puede ocurrir cuando los investigadores aprovechan una conexión activa desde un dispositivo del sospechoso, o cuando emplean credenciales de acceso a los datos obtenidas legalmente.

Los investigadores pueden, ocasionalmente, obtener datos de los proveedores de servicios extraterritoriales presentando una solicitud directa oficiosa, aunque los proveedores de servicios suelen requerir el debido proceso legal.

Las disposiciones vigentes relativas al acceso “transfronterizo” contenidas en el Convenio sobre el delito cibernético, del Consejo de Europa, y la Conventionon Information Technology Offences, de la Liga de Estados Árabes, no regulan debidamente estas situaciones porque destacan el “consentimiento” de la persona legalmente autorizada para divulgar los datos y presuponen el conocimiento de la ubicación de los datos al momento de acceso o recepción. 30.

El actual panorama de cooperación internacional corre el peligro de que aparezcan grupos nacionales que tengan las facultades y los procedimientos necesarios para cooperar entre ellos pero que con respecto a los demás países están restringidos a emplear modos “tradicionales” de cooperación internacional que no toman en cuenta la especificidad de las pruebas electrónicas ni el carácter mundial de la delincuencia cibernética.

Esto ocurre especialmente en el caso de la cooperación en las diligencias investigativas. La falta de un criterio común, incluso en los instrumentos mul-

tilaterales vigentes sobre el delito cibernético, significa que la solicitud de acción, como por ejemplo la rápida conservación de los datos, será difícil de cumplir fuera de los países que tienen obligaciones internacionales de garantizar este servicio y de brindarlo cuando se solicite.

La inclusión de esta facultad en el proyecto de convenio sobre la seguridad cibernética de la Unión Africana sería un adelanto en el camino de cubrir esta laguna. A nivel mundial las divergencias en el alcance de las disposiciones sobre cooperación contenidas en los instrumentos multilaterales y bilaterales, la falta de obligación en el cumplimiento de los plazos, la falta de acuerdo sobre el acceso directo a los datos extraterritoriales, múltiples redes oficiosas de cumplimiento de la ley y diversidad en las garantías de cooperación representan grandes obstáculos para lograr una cooperación internacional eficaz con respecto a la prueba electrónica en asuntos penales.[27]

[27] UNODC, United Nations Office on Drugs and Crime, *Estudio Exhaustivo del Problema del Delito Cibernético y las respuestas de los Estados miembros, la comunidad internacional y el sector privado ante ese fenómeno*, (Estados Unidos, 2013). 12 - 15

CAPÍTULO III

MARCO JURÍDICO NACIONAL Y ÁMBITO DE APLICACIÓN DE LA LEY ESPECIAL CONTRA DELITOS INFORMÁTICOS Y CONEXOS

En el presente capitulo se establece la importancia del ordenamiento nacional el cual se abordara de forma jerárquica desde la Constitución de la República de El Salvador, hasta las leyes especiales, debido a la complejidad que representa la investigación, con el propósito de abordar en forma sistemática tres áreas en las de los bienes jurídicos protegidos agrupados en: a) Delitos contra el sistema como forma, b) contra la información, como medio, c) Delitos contra el contenido como fin.

3. Legislación nacional e internacional

3.1. Constitución de la República de El Salvador

El Salvador en el artículo uno, reconoce a la persona humana como el origen y el fin de la actividad del Estado, el cual está organizado para la consecución de la justicia, de la seguridad jurídica y del bien común[28] la constitución de la República establece como derecho fundamental la seguridad jurídica, en una forma extensa. Siendo la mejor manera de interpretarlo a través de los Concepto jurídico indeterminado, los cuales se usa en una norma para indicar de manera imprecisa un supuesto de hecho, por ejemplo en el terreno administrativo[29].

[28]Constitución de la República De El Salvador, D.C. 38, del 15 de diciembre de 1983, D.O. No 234, Tomo 281, del 16 de diciembre de 1983.
[29]Universidad de Navarra, Concepto Jurídico Indeterminado, (España, 2016) 2. https://dadun.unav.edu/.../1/CONCEPTO%20JURÍDICO%20INDETERMINADOhttps://dadun.unav.edu/.../1/CONCEPTO%20JURÍDICO%20INDETERMINADO.

La doctrina expresa que, por su referencia a la realidad, son utilizados por las leyes, siendo estos: determinados o indeterminados. Con la técnica del concepto jurídico indeterminado la ley refiere una esfera de realidad cuyos límites no aparecen bien precisados en su enunciado, no obstante, lo cual es claro que se intenta delimitar un supuesto concreto. La ley no determina con exactitud los límites de esos conceptos porque se trata de conceptos que no admiten una cuantificación o determinación rigurosa, pero en todo caso es manifiesto que se está refiriendo a un supuesto de la realidad que, no obstante, la indeterminación del concepto, admite ser precisado en el momento de la aplicación.[30]

En ese sentido, toda persona tiene derecho a la libertad, seguridad, propiedad y posesión, así como ser protegida en la conservación y defensa de los mismos. Por otra parte, el Estado es garante del derecho al honor, a la intimidad personal y familiar, así como a la propia imagen de la persona. En consecuencia, para el ejercicio de los derechos individuales el artículo seis de la constitución de la República establece "Toda persona puede expresar y difundir libremente sus pensamientos siempre que no subvierta el orden público, ni lesione la moral, el honor, ni la vida privada de los demás. El ejercicio de este derecho no estará sujeto a previo examen, censura ni caución; pero los que haciendo uso de él infrinjan las leyes, responderán por el delito que cometan".

Entender los alcances y limitaciones de los derechos individuales, de los derechos fundamentales en la parte dogmática de la Carta Magna, es de gran trascendencia, para analizar las facultades conferidas a los cuerpos coercitivos del Estado, por ende el Ministerio Publico según el artículo ciento

[30]Sala de lo Contencioso Administrativo, *Sentencia declarativa pronunciada por el Registrador de la Propiedad Intelectual y Director Ejecutivo Centro Nacional de Registro, referencia 64-2006.* (El Salvador, Corte Suprema de Justicia, 2006).

noventa y uno de la constitución de la República, establece que será ejercido por el Fiscal General de la República, Procurador General de la República, Procurador para la Defensa de los Derechos Humanos y los demás funcionarios que determine la ley, según el artículo ciento noventa y tres, corresponde al Fiscal General de la República: a)Defender los intereses del Estado y de la sociedad; b) promover de oficio o a petición de parte la acción de la justicia en defensa de la legalidad; c) dirigir la investigación del delito con la colaboración de la policía nacional civil en la forma que determine la ley; y d) promover la acción penal de oficio o a petición de parte.

En relación a lo anterior el artículo ciento cincuenta y cinco de la constitución establece que "la defensa nacional y la seguridad pública estarán adscritas a ministerios diferentes. La seguridad pública estará a cargo de la Policía Nacional Civil, que será un cuerpo profesional, independiente de la fuerza armada. La cual tendrá a su cargo las funciones de: policía urbana y policía rural garantizando el orden, la seguridad y la tranquilidad pública, así como la colaboración en el procedimiento de investigación del delito, todo ello con apego a la ley y estricto respeto a los derechos humanos"

3.2 Código penal de El Salvador

El actual Código penal, emitido el veintiséis de abril de mil novecientos noventa y siete, mediante decreto mil treinta, publicado en el Diario Oficial ciento cinco, tomo trescientos treinta y cinco, de fecha diez de junio de mil novecientos noventa y siete, surge con el objeto de orientar la normativa penal de una concepción garantista, estableciendo parámetros mínimos, es decir principios rectores como el de legalidad, estableciendo que "Nadie podrá ser sancionado por una acción u omisión que la ley penal no haya descrito en forma previa, precisa e inequívoca como delito o falta, ni podrá

ser sometido a penas o medidas de seguridad que la ley no haya establecido con anterioridad".[31]

En el mismo orden de idea el código establece como principio rector el respeto inherente a la dignidad humana, de igual forma se destaca el principio de lesividad del bien jurídico, el cual plantea que "No podrá imponerse pena o medida de seguridad alguna, si la acción u omisión no lesiona o pone en peligro un bien jurídico protegido por la ley penal", íntimamente ligado al principio de responsabilidad en cuanto a la pena o medida de seguridad, tomando en cuenta la acción u omisión no sea realizada con dolo o culpa, es decir, queda prohibida toda forma de responsabilidad objetiva.

La responsabilidad objetiva es aquella que se atribuye a una persona sin considerar la dirección de su voluntad, sino únicamente el resultado material a la que está unido causal o normativamente el hecho realizado por el sujeto. La culpabilidad sólo se determinará por la realización de la acción u omisión.

Al tener claro algunos principios en cuanto al deber ser en términos punitivos, el derecho penal a través del código en mención, plantea los siguientes bienes jurídicos, los cuales son protegidos, por medio de la norma o el derecho positivo.

3.2.1. Derechos a la vida

En un orden de prioridades, en cuanto a los bienes jurídicos protegidos se tienen los relativos a la vida, se vuelve en la primacía del Código penal, tomando en consideración el articulo uno de la constitución de la República.

[31]Código penal de el salvador D.L. No. 1030, de fecha 26 de abril de 1997, D.O. No. 105, Tomo 335, del 10 de junio 1997.

Por ende, todo peligro que atente contra la vida y la integridad personal, se vuelve relevante, garantizar por parte del Estado.

3.2.2. Derechos a la libertad

La libertad como bien jurídico protegido, así como lo relativo a su restricción sin causa justificada, tomando en cuenta la autonomía personal, y la coacción, que se puede ejercer teniendo como medio de violencia, obligando a otro a realizar en contra su voluntad, siendo estas situaciones imputables de delito.

El bien jurídico de la libertad, es protegido en todas sus manifestaciones, más sensible para el código penal, la libertad contra las agresiones sexuales, así como ataques manifiestos en el acoso y actos sexuales diversos, a los cuales la persona puede ser expuesto, el artículo ciento sesenta y cinco y siguientes, establece “El que realice conductas sexuales indeseadas por quien las recibe, que implique tocamiento u otras conductas inequívocas de naturaleza sexual será sancionado con prisión de seis meses a un año” agregando infracción de multa de treinta a cincuenta días multa, a quien realizare dicha acción agravando la penal cuando prevaliéndose de la superioridad originada por cualquier relación tipificada contra este bien jurídico.

En cuanto al “menor incapaz” con la vigencia de la Ley de Protección Integral de niñez y adolescencia, la cual establece como sujetos de derecho a los niños, niñas desde los cero años hasta los doce años y de doce años hasta cumplir los dieciocho como adolescentes; el Código penal en el aspecto punitivo agrava el acoso sexual en los casos cometidos contra menores de doce años, sancionando con una pena de seis a dos años.

Por otra parte, el artículo ciento sesenta y seis estipula el engaño con persona entre catorce y dieciséis años de edad, o cualquier “acto sexual diverso” del “acceso carnal”, siendo este sancionado con prisión de seis meses a dos años, aún con su consentimiento del adolescente, la sanción será de uno a tres años de prisión.

La corrupción de menores incapaces, así como los supuestos de agravante los cuales se establecen en los artículos ciento sesenta seis, ciento sesenta y siete y siento sesenta y ocho del Código Penal elevando la pena de cuatro a ocho años de prisión. Tipificando, la corrupción de menores se realizare en diferentes supuestos: 1) En víctima menor de doce años de edad; 2) Con propósito de lucro; 3) engaño, violencia, abuso de autoridad o confianza, o por cualquier otro medio de intimidación; como medios informáticos, logran masifican en la medida del acceso a las tecnologías de la comunicación, las cuales cada vez más permiten la inducción, promoción y favorecimiento de la prostitución, regulado en el artículo ciento sesenta y nueva, tipificando la prostitución así como sus actos derivados en persona menor de dieciocho años, “será sancionado con prisión de dos a cuatro años”.

Las exhibiciones obscenas, pornografía y utilización de menores con fines pornográficos, del Código Penal Salvadoreño, tiene una preponderancia en cuanto a la protección de la libertad, en lo que corresponde a la sexualidad, de la niñez y adolescencia, situación que se retoma posteriormente en la Ley de Delitos Cibernéticos y Conexos, vigente desde febrero de dos mil dieciséis

3.2.3. Derechos a la seguridad

En relación del derecho a la libertad, la protección del bien jurídico de la intimidad, la seguridad personal y el honor, forman parte de la dignidad hu-

mana de la persona, por ende los hechos punitivos regulados y tipificación como la calumnia y la injuria, la primera se refiere al que atribuyere falsamente a una persona la comisión de un delito o la participación en el mismo, sancionado con prisión de uno a tres años, cuando se realice con publicidad será sancionada con prisión hasta cuatro años, las calumnias pueden recaer sobre el honor de una persona, de forma reiteradas serán sancionadas hasta cuatro años y multa de cincuenta a cien días multa, cuando se realizaren con publicidad, la sanción será de dos a cuatro años y multa de cien a doscientos días multa.

La segunda sanciona la ofensa de palabra o mediante acción la dignidad o el decoro de una persona presente, será sancionado con prisión de seis meses a dos años, la injuria realizada con publicidad será sancionada con prisión de uno a tres años y multa de cincuenta a cien días multa.

Cuando se realice de forma reiterada contra una misma persona serán sancionadas con prisión de uno a tres años y multa de cincuenta a cien días multa, si las injurias reiteradas se realizaren con publicidad, la sanción será de uno a tres años de prisión y multa de cien a doscientos días multa, según lo establecen los artículos ciento setenta siete y ciento setenta nuevas del código penal.

La difamación, regulada en el artículo ciento setenta ocho, se refiere al que atribuyere a una persona que no esté presente una conducta o calidad capaz de dañar su dignidad, menoscabando su fama o atentando contra su propia estimación, será sancionado con prisión de seis meses a dos años. La difamación realizada con publicidad será sancionada con prisión de uno a tres años. Esta acción de forma reiterada contra una misma persona será sancionada con prisión de uno a tres años y multa de cincuenta a cien días multa. La calumnia, difamación e injurias encubiertas según el artículo ciento

ochenta y dos son susceptibles de cometerse no sólo manifiestamente, sino también por medio de alegorías, caricaturas, emblemas o alusiones.

3.2.4. Derechos a la intimidad

Con el fin de conocer la información personal, los artículos ciento ochenta y cuatro, en relación con el ciento ochenta y cinco, para descubrir los secretos o vulnerar la intimidad de otro, se apoderare de comunicación escrita, soporte informático o cualquier otro documento o efecto personal que no le esté dirigido, se apodere de datos reservados de carácter personal o familiar de otro registrados en ficheros, soportes informáticos o de cualquier otro tipo de archivo o registro público o privado, será sancionado con multa de cincuenta a cien días multa.

Difundir o revelar a terceros los datos reservados que hubieren sido descubiertos, la sanción será de cien a doscientos días multa. El tercero a quien se revelare el secreto y lo divulgare a sabiendas de su ilícito origen, será sancionado con multa de treinta a cincuenta días multa. Llegando hacer una acción agravante, si los hechos descritos se realizaren por las personas encargadas o responsables de los ficheros, soportes informáticos, archivos o registros, se impondrá, además de la pena de multa, inhabilitación del respectivo cargo o empleo público de seis meses a dos años.

3.2.5. Derechos a la información

De forma amplia y de la protección al derecho a privacidad, se protege el derecho a la información ya que se sanciona la captación de comunicaciones y la utilización de la imagen o nombre de otro.

El articulo ciento ochenta y seis, establece: “el que, con el fin de vulnerar la intimidad de otro, interceptare, impidiere o interrumpiere una comunicación

telegráfica, telefónica, utilizare instrumentos o artificios técnicos de escucha, transmisión o grabación del sonido, la imagen o de cualquier otra señal de comunicación, será sancionado con prisión de seis meses a un año y multa de cincuenta a cien días multa. Así como difundir o revelar a terceros los datos reservados, en el mismo orden de ideas el articulo ciento noventa regula la utilización por cualquier medio la imagen o nombre de otra persona, sin su consentimiento, con fines periodísticos, artísticos, comerciales o publicitarios, será sancionado con multa de treinta a cien días multa.

3.3. Código procesal penal

3.3.1. Generalidades

El código procesal penal, basado en normas de tendencia acusatoria viabilizando la justicia penal, desarrolla diferentes principios como: la legalidad y el juicio previo, el primero establece “Toda persona a la que se impute un delito o falta, será procesada conforme a leyes preexistentes al hecho delictivo de que se trate y ante un tribunal competente, instituido con anterioridad por la ley”, de igual forma el segundo establece “Nadie podrá ser condenado o sometido a una medida de seguridad sino mediante una sentencia firme, dictada luego de probar los hechos en un juicio oral y público, llevado a cabo conforme a los principios establecidos en la Constitución de la República”, teniendo estos parámetros básicos en cuanto a la ley procedimental o procesal

Legalidad de la Prueba, en el artículo quince, establece que “sólo tendrán valor si han sido obtenidos por un medio lícito e incorporados al procedimiento conforme a las disposiciones de este Código”. El artículo en mención plantea la regla general en cuanto que “No tendrán valor los elementos de

prueba obtenidos en virtud de una información originada en un procedimiento o medio ilícito".

No obstante, lo dispuesto, cuando los elementos de prueba hayan sido obtenidos de buena fe, por hallazgo inevitable o por la existencia de una fuente independiente, podrán ser valorados por el Juez aplicando las reglas de la sana crítica.

La acción penal así como su ejercicio, podrá ser a) Acción pública; b) Acción pública, previa instancia particular; y c) Acción privada. Corresponde a la Fiscalía General de la República ejercer la acción penal pública, para la persecución de oficio de los delitos en los casos determinados por este Código; asimismo, cuando la persecución deba hacerse a instancia previa de los particulares. Y a los particulares en los casos determinados en la ley, el ejercicio de la acción penal privada, articulo diecinueve del Código Procesal Penal.[32]

3.3.2. Peritaje

El nombramiento de especialistas en la materia se vuelve necesaria, bajo la figura de los Peritos, así como su regulación y clasificación en el artículo doscientos veintiséis del código procesal penal, estableciendo que "El juez o tribunal ordenará peritajes, cuando para descubrir o valorar un elemento de prueba, sea necesario o conveniente poseer conocimientos especiales en alguna ciencia, arte o técnica".

En los actos urgentes de comprobación que no requieran autorización judicial "el fiscal podrá disponer el auxilio de peritos". Los peritos serán de dos

[32]Código procesal penal, D.L. No. 733, de fecha 22 de octubre de 2008, D.O. No. 20, Tomo 382, de fecha 30 de enero de 2009.

clases: Permanentes o accidentales, el tipos Peritos permanentes: a) Los nombrados por la Corte Suprema de Justicia en el Instituto de Medicina Legal o en cualquier otra dependencia de la misma. b) Los técnicos y especialistas de la Policía Nacional Civil. c) Los especialistas de las facultades y escuelas de la Universidad de El Salvador y de las dependencias del Estado e instituciones oficiales autónomas. d) Los Directores o jefes de los centros asistenciales del Estado o los que aquéllos designen. e) Los miembros de cualquier asociación o institución cuya finalidad sea el estudio o análisis de la medicina legal y de las ciencias forenses, que desempeñen algún cargo o empleo público.

Tipos Peritos accidentales: son los que nombre la autoridad judicial para una pericia determinada, a diferencia de los peritos permanentes no será necesaria su juramentación o protesta para la práctica de las diligencias; su salario habitual serán sus honorarios y la institución para la cual trabajan estará obligada a conceder el permiso para la pericia. La Calidad habilitante se estipula en el artículo doscientos veintisiete el cual establece que “Los peritos deberán tener título en la materia a que pertenezca el punto sobre el que han de pronunciarse, siempre que la profesión, arte o técnica estén reglamentadas”.

En caso contrario, podrá designarse a personas de idoneidad manifiesta. Es decir, también podrá designarse a un perito con título obtenido en el extranjero cuando posea una experiencia o idoneidad especial. La obligatoriedad del cargo según el artículo doscientos veintiocho “El designado como perito deberá desempeñar fielmente el cargo”, estableciendo el mandato conferido por la autoridad judicial.

La Incapacidad e incompatibilidad según el artículo dos cientos veintinueve, prohíbe a su vez las siguientes situaciones “No podrán ser peritos los

menores de edad, los mentalmente incapaces, los que puedan abstenerse de declarar como testigos o hayan sido citados como tales y los inhabilitados para ejercer la ciencia, arte o técnica de que se trate", los Impedimentos que pueden existir al momento de ejercer la pericia, se delimitan en el artículo dos cientos treinta "Sin perjuicio de lo dispuesto en el artículo anterior, serán causas legales de impedimentos de los peritos las establecidas para los jueces. El incidente será resuelto por el juez o tribunal y se aplicarán, en lo pertinente, las reglas sobre excusa y recusación".

El nombramiento, así como la notificación según la base legal estipulada en el artículo doscientos treinta "El juez o tribunal designará un perito, salvo que estime necesario nombrar otros. La realización de la diligencia será notificada a las partes con la indicación de los puntos de pericia y del nombre del perito".

La facultad de proponer según el artículo doscientos treinta y dos, en el término de tres días a partir de la notificación, establece que las partes podrán proponer a su costa otro perito. También podrán proponer puntos de pericia distintos u objetar los propuestos por el juez o tribunal. Este resolverá de inmediato, sin recurso alguno, "la dirección del peritaje estará a cargo del juez o fiscal que ordene la pericia formulará las cuestiones objeto del peritaje, fijarán el plazo en que ha de realizarse y pondrá a disposición de los peritos las actuaciones y elementos necesarios para cumplir el acto, articulo doscientos treinta y tres.

La conservación de objetos es decir medios objetos de análisis, según el artículo dos cientos treinta y cuatro, establece que: "Al practicar la pericia se procurará que los objetos a examinar sean en lo posible conservados, de modo que el peritaje pueda repetirse. "Si por ejemplo es necesario destruir o

alterar los objetos o sustancias a analizarse o existe discrepancia sobre el modo de realizar las operaciones, los peritos informarán a quien ordenó la diligencia antes de proceder a su realización. Finalmente, en el proceso la Ejecución Dictamen Ampliación y aclaración del dictamen Cotejo de documentos regulados en los artículos doscientos treinta y cinco al doscientos treinta y ocho, del código procesal penal, así como la guardará reserva que el perito está obligado hacer, articulo doscientos treinta y nueve de todo cuanto conozca con motivo de su actuación. El juez o tribunal, mediante resolución fundada, procederá a sustituir a los peritos en caso de mal desempeño de sus funciones.

La Evidencia Digital Pertinencia y utilidad de la prueba, articulo ciento setenta y siete “Será admisible la prueba que resulte útil para la averiguación de la verdad y pertinente por referirse directa o indirectamente a los hechos y circunstancias objeto del juicio, a la identidad y responsabilidad penal del imputado o a la credibilidad de los testigos o peritos.”

La evidencia Digital y Custodia de evidencias dependerá de la Fiscalía General de la República quien deberá contar con un depósito de evidencias, a efecto de conservar y custodiar los objetos y documentos decomisados o secuestrados y garantizar el cumplimiento de las disposiciones de este Código relativas a la cadena de custodia. Los objetos y documentos decomisados o secuestrados serán inventariados y puestos bajo segura custodia en el depósito de evidencias, los últimos sujetos a las decisiones del tribunal competente.

Se podrá disponer la obtención de copias o reproducciones de los documentos decomisados o secuestrados cuando estos puedan desaparecer, alterarse, sean de difícil custodia o convenga así al procedimiento, artículo doscientos ochenta y cinco. Se debe considerar que la evidencia o

cualquier elemento que pueda almacenar información, tales como: Computadoras Almacenamiento portátil, USB, discos, mp3 player, celulares, memorias de cámaras, cámaras, smartwatch, etc. Por ende, la cadena de custodia es de vital importancia.

En la práctica no existe un consenso sobre que debe de contener, sin embargo, para el tema informático se debe considerar: Identificación de la evidencia, serie, modelo, color, etc. Procedimientos a los que son sometidos, copias, análisis, descifrado, etc. Fecha del movimiento, Quien entrega, quien recibe, así como Metodología ISO / 27027 /27050 /17025 No existe una guía metodología publica aceptada en El Salvador, sin embargo, hasta el año pasado la ISO27027 era tomada por la mayoría de examinadores forenses como una guía sobre el manejo de evidencia digital. La preservación de la evidencia es lo más fundamental de la ISO 27037. 17025, sin bien cierto no forma parte del proceso formal del peritaje es una guía del ambiente de examen que se debería tener. Noviembre 2016, se lanza la ISO 27050, y se refiere a la metodología de examinar la evidencia.[33]

3.4. Ley general de telecomunicaciones

Ley general de telecomunicaciones, en el Título V capítulo único. En cuanto a la Cooperación con las instituciones del sistema de justicia, estipula en el artículo cuarenta y dos “a” “Los operadores de redes comerciales de telecomunicaciones están obligados a cooperar con las autoridades y a brindar las facilidades necesarias para investigar hechos punibles.”

Por otra parte, el articulo cuarenta y dos “b” reconoce la Información concerniente a la identificación de llamadas de la siguiente forma “Los operadores

[33]Policía Nacional Civil *Portafolio de servicios Institucionales*, 2°edición (División policía técnica y científica, El Salvador, 2016) 5.

de redes comerciales de telecomunicaciones brindarán información relativa al origen, dirección, destino o terminación de la marcación o recepción de llamadas telefónicas de los números de sus usuarios que se encuentren bajo investigación, que se hayan generado o recibido por medio de equipo, facilidades o servicios de telecomunicación del operador de telefonía".[34]

Es evidente que en el artículo cuarenta y dos "b" de la ley de telecomunicaciones apenas se refiere a la obligación de colaborar con "información sobre la marcación o recepción de llamadas telefónicas" por parte de operadores de redes comerciales de telecomunicaciones. Se trata entonces, de una información muy diferente al registro de los hábitos de navegación de posibles sospechosos de cometer un delito cibernético, pero en la práctica puede facilitar el origen del IPE, así como el dispositivo telefónico. No obstante, la dificultad radica en que ningún prestador del servicio de red en el país tiene la obligación de conservar o registrar esta "huella digital", una herramienta necesaria en el combate de esta forma de delincuencia.

3.5. Ley sobre la firma electrónica

3.5.1. Definición y generalidades de la firma electrónica

Es un conjunto de datos generados mediante un algoritmo matemático y basado en técnicas criptográficas (de generación de claves) que se añade al documento que se quiere enviar electrónicamente y que permite no solo vincular ese documento a una determinada persona, articulo tres Ley de Firmas Electrónicas. En la legislación salvadoreña, la rama del derecho es económica. El Ministerio de Economía, a través de una Unidad de Firma

[34]Ley general de telecomunicaciones, D.L. No. 142, de fecha 6 de noviembre de 1997, D.O. No. 218, Tomo 337, de fecha 21 de noviembre de 1997.

Electrónica, estarán a cargo, los documentos con soporte electrónico tendrán valor que los consignados de la firma electrónica.

Equivalencia de los Documentos en Soporte Electrónico articulo ocho “Los documentos en soporte electrónico utilizando firma electrónica, tendrán el mismo valor que los consignados de manera tradicional”. Quedando excluidas aquellas actuaciones que para su perfeccionamiento requieren formalidades y solemnidades especiales.

El objetivo de la ley, es equiparar de la mejor manera la firma electrónica simple y certificada con la firma autógrafa, además se debe reconocer el valor jurídico a la firma electrónica certificada (Art. 3 Ley de Firmas Electrónicas), a los mensajes de datos y toda información en formato electrónico, en el cual se encuentren suscritos con una firma electrónica. Otro importante hecho, se debe recalcar quienes son los proveedores de servicios de certificación y los que brindan servicios de almacenamiento.

Existen principios generales y sus definiciones, los cuales abarca la ley, tales como: a) Firma Electrónica Simple, b) Firma Electrónica Certificada., c) Certificado Electrónico y Documento Electrónico, d) Principios de la Firma Electrónica, e) Autenticidad, f) Integridad, g) Confidencialidad y h) No repudiación.

La Autoridad de Control y Vigilancia según el artículo treinta y cinco, establece la creación de la Unidad de Firma Electrónica, como parte del Ministerio de Economía, el que en el texto de esta Ley podrá abreviarse MINEC. El Ministro nombrará al funcionario que estará a cargo de esta Unidad, quien deberá reunir los requisitos que para tal efecto se establezcan en el reglamento de esta Ley.

Los Proveedores de Servicios de Certificación, presentarán ante la Unidad de Firma Electrónica, junto con la correspondiente solicitud, los documentos que acrediten el cumplimiento de los requisitos señalados en el artículo cuarenta y tres de esta Ley. El cumplimiento de los requisitos será verificado por la Unidad de Firma Electrónica, a través de una auditoria inicial.

En relación a las exigencias indicadas en los literales a), b) y e) del referido artículo cuarenta y tres, el solicitante acreditará por escrito, el compromiso de adquirir los equipos especializados necesarios y los servicios de personal técnico adecuado en el plazo máximo de 90 días hábiles, prorrogable por una sola vez por un período igual, por la Unidad de Firma Electrónica, siempre que el solicitante demuestre que el incumplimiento no es imputable a él. Si transcurrido el plazo indicado, el solicitante no hubiere cumplido el citado compromiso, se procederá inmediatamente a dejar sin efecto la acreditación otorgada.

El plazo de duración de la acreditación será por tiempo indefinido, siempre que se demuestre el cumplimiento de los requisitos establecidos en el artículo cuarenta y tres de esta Ley, los cuales serán revisados anualmente al momento de ser solicitada la renovación anual, según lo establece el artículo cuarenta y cuatro. -

3.5.2. Bienes jurídicos protegidos

La punibilidad de la conducta falsaria del documento electrónico, tiene su fin en la protección penal del trafico jurídico en las redes de información (comercio electrónico), consecuencia del principio de buena fe entre los contratantes, extremos que se destruyen con la conducta típica que conforma el delito.

3.5.3. Autoridad reguladora

El Ministerio de Economía es el ente regulador quien tendrá por ende la contraloría de estas firmas, se considera en manera general la ley tomará medidas de seguridad, este permite; ahorrar costos, tiempo, y espacio. Ahora bien, se debe entender que esto es por seguridad, mejorando así las condiciones del servicio del cliente. En el ámbito jurídico, es un nuevo paso, de aquí se dan a conocer que se llevaran de la mano junto con la tecnología, muchos de estos se necesita brindar y conocer los intereses.

3.5.4. Clasificación de delitos

La aparición de la firma electrónica representa una nueva posibilidad para los delitos de falsedad documental. Los avances tecnológicos han ido generando diferentes problemas jurídicos en relación al concepto de documento y, por extensión, al de firma.

Hoy en día se realizan muchos actos jurídicos por medio de redes digitales o redes telemáticas, tales como la declaración de contratos, el libramiento de órdenes de pago, transferencia electrónica de fondos, liquidación de impuestos y otras muchas gestiones con la administración pública.

La firma electrónica, siempre que esté basada en un certificado reconocido y que haya sido producida por un dispositivo seguro de creación de firma, tendrá, respecto de los datos consignados en forma electrónica, el mismo valor jurídico de la firma manuscrita en relación con los consignados en papel y será admisible como prueba en juicio.

Se presumirá que la firma electrónica reúne las condiciones necesarias cuando el certificado reconocido en que se basa haya sido expedido por un

prestador de servicios de certificación acreditado y el dispositivo seguro de creación de firma con el que ésta se produzca se encuentre certificado.

El problema de la falsedad documental, por lo tanto, se da en la existencia de una certificación que no contiene una declaración de la persona que la realiza, como la requerida por los documentos previstos en los artículos trescientos sesenta y siguientes del Código Penal, sino una comprobación automática de un determinado sistema electrónico.

Por lo tanto, un ejemplo en el funcionamiento diario de un negocio: cuando realizas un acto o formulas una instancia ante la administración, firmas físicamente en un papel. Hoy día, muchos de esos trámites se realizan con la firma electrónica. De igual modo que una persona puede suplantar tu identidad haciendo un garabato que simula tu firma y estaría falsificandoun documento, se puede cometer el mismo delito mediante la firma electrónica.

La acción típica consiste en el primer ordinal, al alterar un documento en alguno de sus elementos o requisitos de carácter esencial. Ordinal segundo Simular un documento en todo o en parte, de manera que induzca a error sobre su autenticidad. Ordinal tres Suponer en un acto la intervención de personas que no la han tenido, o atribuir a las que han intervenido en él declaraciones o manifestaciones diferentes de las que hubieran hecho. Ordinal cuarto en faltar a la verdad en la narración de los hechos.[35]

El artículo tres cientos noventa y dos del Código penal castiga al particular que cometa una falsedad de documento público, oficial o mercantil alterando un documento, suponiendo intervención de terceros o simulando un documento, imponiendo las mismas penas a los que sin haber intervenido en

[35]Ley sobre la firma electrónica, D.L. No. 133, de fecha 1 de octubre de 2015, D.O. No. 196, Tomo 409, de fecha 26 de octubre de 2015.

la falsificación, trafiquen de cualquier modo con un documento de identidad falso. Por ello, siempre se recomiendan que pongas a buen recaudo tus tarjetas de firma electrónica y sus claves pues será la única manera de poner difícil a los amigos de lo ajeno de cometer un delito de falsedad documental.[36]

3.6. Ley especial contra delitos informáticos y conexos

El pasado seis de febrero de dos mil dieciséis, se aprueba bajo de algún grado de confrontación en el seno el decreto número doscientos sesenta, de fecha cinco de febrero del dos mil dieciséis , denominado “Ley Especial Contra Delitos Informáticos y Conexos”, el cual retoma en el considerando romano uno “que la constitución de la República, reconoce a la persona humana como el origen y el fin de la actividad del Estado, que está organizado para la consecución de la justicia, de la seguridad jurídica y del bien común”.

Además, que en la actualidad los instrumentos electrónicos por medio de los cuales se envía, recibe o resguarda la información, han adquirido una especial relevancia, tanto a nivel internacional como nacional para el desarrollo económico, político, social y cultural del país; por lo que se vuelve prioridad del Estado, ya que al no protegerla se atenta con la confidencialidad, integridad, seguridad, seguridad y disponibilidad de los datos en general. Esta diversidad de actividades, permiten que la actividad delincuencial sea factible a través de la tecnología de la información y la comunicación, por ende, es necesario ampliar y actualizar la normativa penal vigente regulando nuevos tipos de delitos a partir de la tipificación.[37]

[36]Código penal de El Salvador d.L. No. 1030, de fecha 26 de abril de 1997, D.O. No. 105, Tomo 335, del 10 de junio 1997.
[37]Ley especial contra delitos informáticos y conexos D.L. No. 260, de fecha 4 de febrero de 2016, D.O. No. 40, Tomo 410, del 26 de febrero 2016.

Antes de conocer la tipificación y los bienes jurídicos protegidos, debido a la complejidad que representa la investigación, así como la naturaleza de la infracción o delito, existen tres áreas en las cuales los bienes jurídicos protegidos se agrupan:

a) Delitos contra el sistema: Relacionado al acceso indebido, vulnerando la confidencialidad e integridad de los sistemas informáticos como: el acceso, intercepción y actos constituyentes a la intercepción o sistema de forma ilegal.

b) Delitos contra la información: Son los que atentan contra la información y comunicación, los cuales buscan un beneficio particular que pueda afectar a otra o varis personas ya sea naturales o jurídicas, como por ejemplo la estafa, fraude, espionaje y hurto informático, siendo estos similares a los tipificados de forma tradicional en el código penal. No obstante, está categoría de delitos propiamente informáticos se encuentra la denegación del servicio, es decir aquellas acciones intencionales que utilicen técnicas para denegar servicio en sitios web afectando u obteniendo beneficio económico.

c) Delitos contra el contenido: Vinculado para infligir daño u obtener un beneficio, a través de la manipulación de registros informáticos contenidos en plataformas tecnológicas de forma fraudulenta alterando o dañando la información de datos, así como la suplantación del contenido por otro similar (piratear o craquear)

3.6.1. Bienes jurídicos protegidos

El objeto de la ley, en el artículo uno es “proteger los bienes jurídicos de aquellas conductas delictivas cometidas por medio de las tecnologías de la

información y la comunicación", los delitos cometidos en prejuicio de los datos almacenados, procesados o transferidos; los sistemas, su infraestructura o cualquiera de sus componentes, a los cometidos mediante el uso de dichas tecnologías que afecten intereses asociados a la identidad, propiedad, intimidad e imagen de las personas naturales o jurídicas, actúando de forma preventiva o sancionatoria.

Los delitos informáticos, se puede decir que la tendencia es que la protección a los bienes jurídicos, se le haga desde la perspectiva de los delitos tradicionales, con una re-interpretación teleológica de los tipos penales ya existentes, para subsanar las lagunas originadas por los novedosos comportamientos delictivos. Esto sin duda da como regla general que los bienes jurídicos protegidos, serán los mismos que los delitos re-interpretados teleológicamente o que se les ha agregado algún elemento nuevo para facilitar su persecución y sanción por parte del órgano jurisdiccional.

Por otra parte, la vertiente doctrinaria supone que la emergente Sociedad de la Información hace totalmente necesaria la incorporación de valores inmateriales y de la información misma como bienes jurídicos de protección, esto tomando en cuenta las diferencias existentes por ejemplo entre la propiedad tangible y la intangible. Esto por cuanto la información no puede a criterio de autor ser tratada de la misma forma en que se aplica la legislación actual a los bienes corporales, si bien dichos bienes tienen un valor intrínseco compartido, que es su valoración económica, es por tanto que ella la información y otros intangibles son objetos de propiedad, la cual esta constitucionalmente protegida.

En fin, la protección de la información como bien jurídico protegido debe tener siempre en cuenta el principio de la necesaria protección de los bienes jurídicos que señala que la penalización de conductas se desenvuelva en el

marco del principio de “lesividad”. Así, una conducta sólo puede conminarse con una pena cuando resulta del todo incompatible con los presupuestos de una vida en común pacífica, libre y materialmente asegurada.

Así inspira tanto a la criminalización como a descriminalización de conductas. Su origen directo es la teoría del contrato social, y su máxima expresión se encuentra en la obra “Los Delitos y las Penas” (1738-1794). Se define como un bien vital, “bona vitae”, estado social valioso, perteneciente a la comunidad o al individuo, que, por su significación, es garantizada, a través del poder punitivo del Estado, a todos en igual forma. En conclusión, se puede decir 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; los mismos que se equiparan a los bienes jurídicos protegidos tradicionales tales como:

a) La reserva, la intimidad y confidencialidad: Como ya se ha desarrollado anteriormente la libertad, así como la intimidad y privacidad forman parte de los derechos fundamentales, los cuales en la actualidad se registran en base de datos, los cuales forman un perfil no solo personal, sino que profesional y laboral de las personas naturales, así como la información reservada de las personas jurídicas, como lo son en materia lo relativo al secreto profesional. 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.

b) La seguridad: También relacionado a la fiabilidad del tráfico jurídico y probatorio, en el caso de falsificaciones de datos o documentos probatorios vía medios informáticos.

c) El patrimonio: En el caso de la amplia gama de fraudes informáticos y las manipulaciones de datos que da a lugar. 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. 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.

d) La información: La forma de materializar el acceso a la intimidad, el patrimonio y vulnerar la seguridad que representan estos bienes jurídicos protegidos, antes relacionados es a través del acceso injustificado de la información, la cual recoge una serie de datos los cuales al ser recopilados pueden ser utilizados de forma maliciosa en contra de un sujeto. Los delito informático o ciberdelito: es toda aquella acción anti jurídica, que tiene por objeto manipular dañar o destruir ordenadores, medios electrónicos y redes de internet, su relación con el bien jurídico protegido, antes de desarrollarlos es necesario revisar los delitos o conductas contra la persona como el bien protegido a la salud, honor, integridad y desarrollo personal, en un contexto comparativo con la conceptualización tipificados en otras legislaciones, pero que en esencia es similar su aplicación en el marco jurídico nacional.

3.6.2. Clasificación de delitos

En ese sentido, se puede catalogar los delitos informáticos, también conocidos como cibernéticos, ciberdelitos en tres formas: a) como un fin en sí mismo: es decir como acceso ilegal al sistema, b) como medio: ya sea como amenaza, estafa, o delitos más complejos como la explotación infantil y c) como método o herramienta: piratería de música y software.

3.6.3. Conceptos atípicos y conductas tipificadas como delitos contra la persona

a) Sexting: la palabra sexting es un neologismo tomado de la lengua inglesa compuesto por las voces inglesas “sex” y “texting”; sextingenvió de imágenes sexuales (eróticos o pornográficos) por medio de teléfonos móviles, uncialmente era característico mensajes sexuales sms de naturaleza sexual, posteriormente al envió de material pornográfico. la conducta es la divulgación indebida, este acto cada vez es más común entre aquellas personas que poseen teléfonos móviles, y en la actualidad con los teléfonos inteligentes, debido a que a través de ellos pueden enviar cualquier tipo de contenido y archivos, que puede incluir a una o varias personas; y cabe destacar que independiente de la edad de las personas, es un fenómeno que va en aumento; hoy en día ha salido a relucir hasta figuras famosas posando para así enviar fotografías de este tipo.

Las primeras apariciones del término sexting datan del año 2005 en el periódico sundaytelegraph, a partir de allí se ha manifestado en distintos lugares del mundo, claro está que con mayor auge en los países anglosajones tales como nueva zelanda, estados unidos de américa, reino unido y australia. en el año 2008 fue realizada una encuesta en la campaña estadounidense para la prevención del embarazo en adolescentes, arrojo que este tipo de acto se extendió rápidamente junto con otros comportamientos similares vía online entre los adolescentes.

El sexting puede acarrear diversos riesgos dado a que al enviar este tipo de imágenes, textos y videos puede significar que sea visto por muchas personas y así llegar a perder el control sobre este y luego equivaldría un

daño mayor, como un daño emocional porque podría deteriorar la reputación de una persona.

Últimamente se ha evidenciado que el menor no es sólo el objeto, sino que en ocasiones también es consumidor y autor de dichos contenidos. El sexting, se define como la producción de fotos o vídeos en actitudes sexuales que posteriormente se envían a móviles o se publican en internet.

Asimismo, el acto de enviar una foto con connotaciones sexuales a otros, ya sea mediante el móvil (mms o bluetooth) o internet, puede suponer que esas imágenes acaben en manos de cualquiera e incluso los menores podrían ser víctimas de chantajes. En el país se encuentra regulado en el artículo 26 LECDIC, la crítica este artículo es que está encaminado al acoso sexual, y no otras conductas que pueden ser atentatorias.

b) Extorsión:(extorsión sexual) es una forma de explotación sexual en la cual una persona chantajea con imágenes con una imagen o video de si misma desnuda o realizando actos sexuales que generalmente han sido previamente compartidos mediante el sexting. Lleva un componente emocional.

c) Ciberbullying: (ciberacoso) también denominado acoso virtual o acoso cibernético, es el uso de medios de comunicación digital para acosar a una persona o grupo de personas mediante ataques personales, divulgación de información confidencial o falsa, humillaciones, vejaciones, insultos amenazas.

Por lo tanto, el acoso o maltrato escolar siempre ha estado presente de una u otra manera en la vida escolar. con la aparición de internet esta problemática ha cambiado de escenario y este tipo de acoso se agrava aún más,

por la rapidez en su difusión, por la cantidad de personas que pueden ser conocedoras de ello y porque ciertos contenidos o textos pueden permanecer para toda la vida y pueden ser fácilmente accesibles. el ciberbullying puede ir desde obligar a otro a que haga cosas que no quiere, hacerle el "vacío" y que nadie le haga caso, humillarlo, hasta insultarlo, coaccionarlo y amenazarlo a veces la situación puede llegar a ser insostenible.

Los menores, por tanto, se presentan no sólo como objeto de abusos sino también como el sujeto que lleva a cabo esas agresiones o abusos. Padres y educadores deben tener en cuenta esta doble vertiente del problema para enfrentarse a él desde ambos frentes. Deben hacer entender a los menores que este tipo de conductas son impropias, no están admitidas socialmente y además tienen consecuencias negativas.

el ciberbullying puede llegar a ser un delito si es demostrable que ha habido amenazas, calumnias, coacciones, etc. la pena impuesta por la justicia depende del tipo de acoso que se haya ejercido sobre la víctima y de la edad del acosador. En él esa se encuentra regulada en los artículos 27 y 32 LECDIC

d) grooming: el término grooming hace referencia al conjunto de acciones realizadas deliberadamente por un adulto para debilitar emocionalmente al niño y ganarse su confianza con la intención de abusar sexualmente de él. como parte del proceso captador, alimentan la confianza del menor con mentiras, luego los chantajean y se aprovechan de su sentimiento de culpa. los padres, por su parte, no suelen vigilar muy de cerca las personas con las que contactan sus hijos porque no se aprecia la peligrosidad que puede manifestar como podría hacerlo un extraño en la calle.

e) happyslapping: (paliza feliz) el consiste en grabar una agresión física ya sea empujones golpes incluso torturas, por un medio de un medio electrónico como celulares o tableta, los cuales son posteriormente cargados a internet para promover su difusión. En el país no están regulados

f) stalking: es un anglicismo, que se refiere a conductas constitutivas de acoso, acecho u hostigamiento y que hasta 2015 no contaba aun con una tipificación especifica en el código penal español, “cyberstalking” a raíz de la jurisprudencia del 25 de marzo Tudela navarra el cual debe de llenar ciertos requisitos como lo son: a) acoso reiterado e insistir b) continuado y temporal c) debe perjudicar la vida de la víctima c) no está legítimamente.

En el país algo muy positivo es que el capítulo IV de la LEDICC, que consta de los artículos 28 al 33 es dedicado a la tipificación de delitos informáticos cometidos contra niños, niñas y adolescentes. es necesario integrar la norma y ver otros cuerpos normativos para establecer la presunción de niñez desde su concepción hasta los 12 años y de 12 años hasta que cumplan los 18 son adolescentes artículo 3 inciso segundo y 4, seguidamente del artículo 5 de LEPINA que los cataloga como sujetos de derechos. la ley penal juvenil en el artículo 2 establece que es aplicable a las personas mayores de 12 años y menores de 18, en lo que establece las conductas ilícitas bajo un régimen correctivo especial.

3.6.4. Conceptos atípicos relacionados con los delitos contra sistemas informáticos, información digital y contenido de datos

En El Salvador, a partir del Título II en los capítulos I, II y III de la LEDIC, regula la manipulación indebida, violación, fraude y estafas digitales en los sistemas informáticos, siendo el bien jurídico protegido la información

a) Estafas informáticas (10 LEDICC) la manipulación, influencia de ingresos de datos con el fin de alterar un resultado por media la tecnología con datos falsos incompletos para obtener beneficio patrimonial para si o para otro (de 2 a 5 años) tendrá un agravante cuando a) sea contra el estado, b) contra sistemas financieros o bancarios c) cuando el sujeto activo sea un administrador o sepa de soporte informático (5 a 8 años)

b) interferencia de datos (20 LEDICC) la interrupción u obstrucción del uso legitimo de datos o destruir y alterar datos de terceros sanción (3 a 6 años) pero si recae sobre documentos públicos destinados a la prestación de salud, comunicación sistema bancarios entidades financieras energía transporte u otros servicios públicos se agrava de (5 a 8 años)

c) Acceso indebido a sistemas informáticos (4 LEDICC) quien sin autorización o excediendo la que se le hubiere concedido, acceda, intercepté o utilice parcial o totalmente un sistema informático que utilice las tecnologías de la información o la comunicación, para un fin determinado (1 a 4 años)

d) Acceso indebido a los programas o datos informáticos (5 LEDICC) posesión de equipos o prestación de servicios para la vulneración de seguridad (8) la conducta tipificada es dirigida a quien posea produzca facilite, venda equipos, dispositivos, programas informáticos contraseñas con el fin de cometer cualquier delito señalado en esta ley (3 a 5 años)

e) phishing: técnica de ingeniería social utilizada por delincuentes para obtener información confidencial, haciéndose pasar por una institución confiable con la finalidad de obtener contraseñas, información personal datos de tarjetas de créditos etc.

Es una técnica de ingeniería social utilizada por los delincuentes para obtener información confidencial como nombres de usuario, contraseñas y detalles de tarjetas de crédito haciéndose pasar por una comunicación confiable y legítima. si desea puede denunciar casos de phishing a segu-info. el término phishing proviene de la palabra inglesa "fishing" (pesca), haciendo alusión al intento de hacer que los usuarios "muerdan el anzuelo".2 a quien lo practica se le llama phisher.3 también se dice que el término phishing es la contracción de passwordharvestingfishing (cosecha y pesca de contraseñas), La primera mención del término phishing data de enero de 1996, se dio en el grupo de noticias de hackers alt.2600,5 aunque es posible que el término ya hubiera aparecido anteriormente en la edición impresa del boletín de noticias hacker 2600 magazine.6 el término phishing fue adoptado por quienes intentaban "pescar" cuentas de miembros de AOL.

Quienes comenzaron a hacer phishing en aol durante los años 1990 solían obtener cuentas para usar los servicios de esa compañía a través de números de tarjetas de crédito válidos, generados utilizando algoritmos para tal efecto. Estas cuentas de acceso a AOL podían durar semanas.

En 1995 AOL tomó medidas para prevenir este uso fraudulento de sus servicios, de modo que los crackers recurrieron al phishing para obtener cuentas legítimas en AOL. el phishing en AOL estaba estrechamente relacionado con la comunidad de warez que intercambiaba software falsificado. un cracker se hacía pasar como un empleado de aol y enviaba un mensaje instantáneo a una víctima potencial. Para poder engañar a la víctima de modo que diera información confidencial, el mensaje podía contener textos como "verificando cuenta" o "confirmando información de factura". Una vez el usuario enviaba su contraseña, el atacante podía tener acceso a la cuenta de la víctima y utilizarla para varios propósitos criminales,

incluyendo el spam. Tanto el phishing como el warezing en aol requerían generalmente el uso de programas escritos.

f) smishing: técnica deingeniería social, dirigido a los usuarios de teléfonos móviles (una variante de phishing) que por medio de mensajes de texto sms, se solicitan datos personales como convenciendo al usuario de ingresar algún vínculo o contestar el mensaje.

g) pharming: es la explotación de una vulnerabilidad en el software de los servidores dns (domainnamesystem) o en el de los equipos de los propios usuarios para redirigir un nombre de dominio (domainname) todos los ordenadores conectados a internet tienen un ip única (consiste en 4 actetos ósea 4 grupos de 8 dígitos) la técnica de pharming se utiliza normalmente para realizar ataques de phishing redirigiendo el nombre de dominio de una identidad de confianza a una página wad en apariencia idéntica, pero que es creada para robar información de la víctima.

h) spoofing: uso de técnicas a través de las cuales un ataque generalmente con usos maliciosos por medio de una falsificación de los datos, el más conocido es el ipspoofing es la suplantación del IP.

i) ransomware: secuestro de datos por dinero en el país se puede vincular a los delitos tipificados en los artículos 12, 15,19 22 al 26 de la LEDICC.

j) espionaje informático (12 LEDICC) fines indebidos obtenga datos, información reservada o confidencial contenidas en un sistema sanción (5 a 8 años) la cual es agravante cuando se cometieren con el fin de obtener beneficio para sí o para otro, se pusiere en peligro la seguridad del estado, personas naturales o jurídicas como consecuencia de la revelación de la información de carácter reservada (6 a 10 años) ver la LAI.

k) manipulación de registros (15 LEDICC) los administradores de las plataformas tecnológicas de instituciones públicas o privadas, que deshabiliten, alteren, oculten, destruyan, o inutilicen en todo o en parte cualquier información, dato contenido en un registro sanción (5 a 8 años)

l) alteración, daño a la integridad y disponibilidad de los datos (19 LEDICC) violación de seguridad de un sistema informático destruya, altere, duplique, inutilice o dañe la información, datos o procesos, en cuanto a su integridad, disponibilidad y confidencialidad en cualquiera de sus estados de ingreso, procesamiento, transmisión o almacenamiento, sanción (3 a 6 años)

m) Hurto de identidad (22 LEDICC) la suplantación, el apoderarte de la identidad de una persona natural o jurídica por medio de las tecnologías de la información y la comunicación tendrá una sanción de (3 a 6 años) la cual tiene un agravante si con la conducta descrita en el inciso anterior se daña, extorsiona, defrauda, injuria o amenaza a otra persona para ocasionar perjuicio u obtener beneficios para sí mismo o para terceros (de 5 a 8 años)

n) divulgación no autorizada (23 LEDICC) dar a conocer un código, contraseña de acceso o cualquier otro medio de acceder a un programa o datos almacenados en un equipo o dispositivo tecnológico, con el fin de lucrarse a sí mismo, a un tercero, quien sin autorización revele o difunda los datos o información, contenidos en un sistema informático que utilice las tecnologías de la información y la comunicación sanción (5 a 8 años), será un agravante para la pena si se pone en peligro la seguridad del estado, la confiabilidad de la operación de las instituciones afectadas o resultare algún daño para las personas naturales o jurídicas (6 a 12 años)

o) Utilización de datos personales (24 LEDICC) utilice datos personales a través del uso de las tecnologías de la información y la comunicación, violando sistemas de confidencialidad y seguridad de datos, insertando o modificando los datos en perjuicio de un tercero. sanción de (3 a 4 años) y podrá aumentarse en una tercera parte si quien proporcione o revele a otro, información registrada en un archivo o en un banco (secreto bancario)

p) Obtención y transferencia de información de carácter personal (25 LEDICC) obtener deliberadamente obtenga y transfiera información de carácter confidencial y que mediante el uso de esa información vulnere un sistema o datos informáticos apoyándose en cualquier clase de las tecnologías de la información y la comunicación, incluidas las emisiones electromagnéticas. sanción (5 a 8 años)

q) revelación indebida de datos o información de carácter personal (26 LEDICC) cuando sin el consentimiento del titular de la información de carácter privado y personal revele, difunda o ceda en todo o en parte, dicha información o datos, sean éstos en imágenes, video, texto, audio u otros, obtenidos por alguno de los medios indicados (sanción de 3 a 5 años) si la conducta es con ánimo de lucro, la comisión de otro delito o se difunda material sexual explícito en perjuicio de un tercero la sanción será de (4 a8 años), pudiéndose elevar hasta en una tercera parte si recae sobre datos personales o confidenciales definidos en la Ley Acceso a la Información Pública.

3.6.5. Delitos económicos y patrimoniales

En el país se encuentra especialmente regulado en el capítulo v de la LEDIC, “delitos relativos al orden económico”, La Ley Especial Contra Delitos Infor-

máticos y Conexos vigente en El Salvador, es de los primeros intentos del país de sancionar a aquellos que cometen delitos cibernéticos. Con su aprobación, dicha ley establece sanciones meramente penales, por lo que es importante conocer aquellas conductas indicadas en esas leyes como ilegales, por ejemplo:

a) Estafas electrónicas

b) Manipulación de registros públicos o privados

c) Acoso

d) Accesos indebidos a sistemas informáticos

e) Interferencia de sistemas informáticos, etc.

Los aspectos que contempla la normativa destacan y se dividen por naturaleza en: Delitos contra los sistemas tecnológicos de información; delitos informáticos; delitos informáticos relacionados con el contenido de los datos; delitos informáticos contra niñas, niños y adolescentes o personas con discapacidad y delito contra el orden económico.

En relación a los delitos informáticos se regulan: la estafa, fraude y espionaje informático; así como el hurto por medios informáticos y; las técnicas de denegación de servicio. También se protegerá la integridad de las personas naturales o jurídicas, en relación a obtener información de carácter confidencial. El artículo veinticinco dedicha normativa establece “el que deliberadamente obtenga y transfiera información de carácter confidencial y que mediante el uso de esa información vulnere un sistema o datos informáticos apoyándose en cualquier clase de las Tecnologías de la

Información y Comunicación, incluidas las emisiones electromagnéticas, será sancionado con prisión de cinco a ocho años".

Además, se regula la pornografía a través del uso de las TIC. "El que por cualquier medio involucre el uso de las Tecnologías de la Información y la Comunicación fabrique, transfiera, difunda, distribuya, alquile, venda, ofrezca, ejecute, exhiba o muestre material pornográfico, sexual entre niñas, niños y adolescentes o personas con discapacidad, será sancionado con prisión de tres a cinco años". Cabe mencionar que las sanciones previstas en la normativa, serán aplicables sin perjuicio de otras responsabilidades penales, civiles o administrativas en que se incurra; según establece el artículo 35 de la misma.

Al observar la Ley Especial contra los Delitos Informáticos y Conexos es notoria la influencia del Convenio de Budapest, pues los delitos que reconoce este tratado son igualmente reconocidos por el Gobierno de El Salvador, los cuales se mencionaron anteriormente en este artículo.

Situaciones como el fraude y la falsificación informática, accesos ilícitos o ataques a sistemas informáticos, entre otras, son bien definidas en las leyes salvadoreñas, además de ello también se contemplan los ataques de denegación de servicio, el uso fraudulento de tarjetas inteligentes, interceptación de transmisiones de sistemas informáticos, el robo de identidad y el comercio de credenciales de acceso a equipos informáticos o datos personales. Sin embargo, no se toma en cuenta el uso de sistemas informáticos con respecto a los derechos de autor y la propiedad intelectual, siendo este un punto endeble en la legislación. Sumado a ello, otro punto que no retoma esta ley es con respecto al derecho procesal y la forma en que las autoridades reaccionarían ante un delito informático.

A nivel centroamericano, El Salvador tiene intenciones de construir una estructura de combate al cibercrimen, un punto muy fuerte es la recién publicada Ley Especial contra los Delitos Informáticos y Conexos. Sin embargo su preparación general para el combate al cibercrimen no sale tan bien evaluada como Panamá o Costa Rica, por el hecho que El Salvador recién ha incorporado en su agenda nacional el tema de delitos informáticos, a diferencia de estas otras naciones, que ya establecieron su legislación correspondiente y se incorporaron a tratados internacionales, como Panamá, suscrito al Convenio de Budapest desde 2014, y determinaron, organizaron y forjaron instituciones que se encargarían de delitos informáticos, delimitando tareas y responsabilidades asesorándose de otros organismos especializados.[38]

[38]Miriam Guardiola Salmerón y Mario Orellana, Conferencia "Delitos Cibernéticos" *promovida por la Revista Derecho y Negocios, San Salvador El Salvador*, (2017):23.

CAPÍTULO IV

DIFICULTADES EN INVESTIGACION DE LA CIBERCRIMINALIDAD Y SU ÁMBITO DE APLICACIÓN EN RELACION CON LA LEY ESPECIAL CONTRA DELITOS INFORMÁTICOS Y CONEXOS, POR LA FALTA DE CONVENIOS CON EMPRESAS DE SEGURIDAD INFORMÁTICA, EN LA REPUBLICA DE EL SALVADOR

En este capítulo se aborda La complejidad de las relaciones informáticas, el crecimiento exponencial del delito cibernético y las respuestas de los Estados Miembros, en la comunidad internacional y el sector privado ante este fenómeno, además se establece las dificultades de la investigación, las cuales radican en diferencia regulatoria tanto en la legislación nacional, como internacional, con el propósito de mejorar las buenas prácticas y la información actualizada en cuanto al fenómeno con organismos especializados en asistencia técnica y cooperación internacional como Oficina de las Naciones Unidas contra la Droga y el Delito.

4. Desarrollo de las tecnologías de la información y comunicación

Para entender de mejor manera la cibercriminalidad y los ciberdelitos, se tiene que contextualizar según la doctrina la práctica y la cronológica de La política criminal en cuanto a este fenómeno. En la actualidad obliga a enfrentarse a problemas concretos muy del actual tiempo, impensables hace apenas dos décadas, que exigen actualizar la legislación penal, quizás no es el más aconsejable en relación con la pausa que requiere toda reforma de la misma reflexionando sobre aspectos puntuales que sin duda no tienen la trascendencia de las grandes cuestiones de la política criminal, pero no

puede quedar sin opinión, en relación con los instrumentos tradicionales del Derecho Penal.[39]

4.1. Relación con el derecho penal

El concepto de la "teoría del caso" en el país, se asemeja en el ámbito jurídico prioritariamente, sus aplicaciones en el proceso penal, constituyendo por el sistema acusatorio una metodología para el análisis, la recopilación de la prueba y el planteamiento del caso, tanto en la etapa de investigación inicial de fiscalía y órgano policial, como en las distintas fases judiciales del proceso. La teoría del caso sirve para elaborar de forma metódica el plan de acción con el cual el abogado litigante debe preparar su caso para presentarlo ante los tribunales y ante su contraparte, con el propósito de lograr una decisión judicial definitivita, conveniente a los intereses de su representado, incluye la estrategia para desarrollar los componentes facticos, jurídicos y probatorios sobre los cuales se fundamenta el caso, además contiene las líneas de respuesta contra los planteamientos adversos de la contra parte para lo cual se definen objetivos concretos y se prevén soluciones jurídicas.[40]

De qué manera deben afrontarse novedosos modelos de delincuencia y plantearse incluso la necesidad de tutelar nuevos intereses sobre los que hasta ahora no se había reflexionado, sobre lo que debería debatirse aún más. Pues bien es incuestionable que el desarrollo de las nuevas tecnologías de la información y de la comunicación, así como la imparable consolidación de los contextos digitales en la sociedad actual y, sobre todo el desarrollo de

[39]Norberto J. de la Mata Barranco, *Derecho penal Informático*, 2ª Edición (Instituto Vasco de Criminología, España, 2007), 4.
[40]Saúl Ernesto Morales, E*l Ofrecimiento y valoración de la prueba en el Cogido Procesal Civil y Mercantil Salvadoreño,* ,2 ª edición, (Unidad Técnica Ejecutiva del Sector de Justicia, El Salvador 2016) ,15-17.

las redes de transmisión de datos, básicamente internet, situación que genera un auténtico cambio en los modos de relación administrativa, educativa, laboral o social, riesgos concretos para la garantía de determinados intereses, que corresponde salvaguardarlos.

Los ataques a los distintos sistemas de información y comunicación, ya sea para vulnerar los mismos, por razones varias, ya para lesionar bienes tradicionalmente tutelados por el derecho penal a través de ellos, es en todo caso algo consustancial en la actualidad al ámbito de informática.

El derecho penal, siempre como último eslabón de la cadena de tutelas jurídicas posibles, puede tener capacidad para dar cobertura preventiva y sancionadora a los intereses más importantes para una convivencia en que se hade tratar de maximizar la realidad de todos quienes participan de ella evitando en la medida de lo posible la realización de las conductas que más gravemente puedan afectarlos, estas conductas de riesgos y amenaza que acompañan el desarrollo de los contextos digitales- al margen de sensaciones inseguras, en acciones inexistente o exagerada-, que junto a razones econó-micas, pueden hacer desistir de implementación, solo cuando realmente vulnere intereses a los que presta o debe prestar atención el Derecho penal.[41] Es decir no se visualiza el riesgo ni el potencial preventivo y coercitivo que puede aportar la esfera penal frente a una sociedad digitalizada.

4.1.1. Evolución de la implementación de las tecnologías de la información y comunicación

En primer lugar, la ingente acumulación de datos de carácter personal de la ciudadanía por parte de los gobiernos, aun cuando no estaba masificado el

[41]Ibíd. 4-6.

uso de los ordenadores, hace que comiencen las preocupaciones en torno al carácter reservado. La acumulación y el uso que podría hacerse de tales datos.

Nace así el concepto de “privacy” y de derecho a la misma, que va más allá del tradicional de intimidad y que trata de referir el hecho de la acumulación en las bases de datos de carácter informático o no de información sobre los individuos y el uso que se hace de ella, así como la capacidad de decisión de cada ciudadano de que datos referentes a su persona deben ser compartidos o públicos y, en consecuencia, la salvaguarda que frente a dicha acumulación cabe proponer.

Ya en los años sesenta comienzan las primeras discusiones en torno a esta cuestión, sobre todo en materia civil y administrativa, planteándose el debate, en los años siguientes, también en términos penales, durante la década de los setenta, la proliferación del uso de los ordenadores en el empresarial supuso que la mayoría de las manifestaciones de la delincuencia vinculada a la información tuviera relación con la delincuencia económica, siendo las más comunes las referente a: fraudes, sabotajes informáticos a través de la manipulación de datos, espionaje empresarial, etc.

Hasta el punto de que en este periodo eran estas nuevas modalidades de delincuencia económica las que integraban el concepto de delito informático; o, al menos eran las principales manifestaciones. La generalización de los ordenadores personales en los años ochenta trajo consigo, al mismo tiempo, el surgimiento de la piratería de su software, dando comienzo a las primeras infracciones contra la propiedad intelectual, que se dispararía a finales de los años noventa, extendiéndose también, además del software, a productos como música o películas.

La expansión del internet en la década de los noventas llevo aparejado el surgimiento de un nuevo método para discutir contenidos ilegales o dañosos, tales como pornografía infantil, discursos racistas o xenofóbicos. Serán las conductas vinculadas a la difusión de contenidos ilícitos las que más pueden aprovecharse de la enorme implantación que tiene la red a nivel mundial, así como de sus características técnicas, que van a dificultar su descubrimiento, persecución y prueba.

En este periodo también se consolida la dependencia que los gobiernos y organismos internacionales tienen de los sistemas informáticos, tanto para su correcta organización como para el almacena-miento de datos importantes, lo que les pondrán en la mira para la comisión de delitos que atentaran contra la seguridad del Estado, del concepto genérico de "terrorismo a través de la red"[42].

En la actualidad retomando particularmente el término "pornografía Infantil" ya no es vinculante puesto que la noción de la "utilización de niñas, niños o adolescentes" para fines sexuales (ya sea en actuaciones u otros) tiene la ventaja de que el énfasis se pone en el hecho de que la niña, el niño o el adolescente está siendo sometido a una acción delictiva y no es responsable de lo que le sucede.

En ese sentido, como término, funciona de manera más neutral, pues evita estigmatizar o culpar la niña, el niño o el adolescente. Sin embargo, el término "pornográfico" en relación con éstos resulta inadecuado y debería ser sustituido por "sexual", siendo por tanto el término preferido "utilización de niños, niñas y adolescentes en los espectáculos sexuales"[43].

[42]Ibíd. 16-18.
[43]Guia de Luxemburgo, *Para la Orientaciones Terminológicas para la Protección de Niñas Niños y Adolescentes contra la Explotación y el Abuso sexual*, (Grupo de Trabajo Inter-institucional en Luxemburgo, 2016), 39.

Por otra parte, relacionado siempre con el fenómeno digital, no se puede dejar de mencionar el secuestro de datos a nivel global, ocurrido recientemente, tomando como ejemplo particularmente lo acontecido en Latinoamérica, el cual creció rápidamente especialmente en Brasil y México, países que reportaron el mayor número de víctimas de la región en el ciberataque global "entre los países más afectado estuvo México, que llego a ocupar el cuarto puesto del mundo en número de víctimas, y Brasil, el sexto", afirmo DmitryBestuzhev, director de Investigación para Latinoamérica del gabinete de seguridad informática KasperskyLab, al referirse al ataque "WannanCry".

El ataque comenzó el 12 de mayo de 2017, aprovechando una vulnerabilidad del sistema operativo de Microsoft Windows, afecto a cerca de 200.000 ordenadores en 150 países usando el secuestro de datos "ransomware", en que se encripta el contenido digital de la víctima y se mantiene como rehén hasta que se paga un rescate. El caso de "WannanCry" se exigió un pago en la moneda digital bitcoin para recuperar el accesoa los ordenadores y, según registros de Kaspersky, hasta el lunes 15 de mayo, 236 víctimas habían abonado al rescate. "Precisamente el problema es pagar. El `ransomware` crece por que la gente paga. Lamentablemente las empresas o los usuarios particulares han accedi-do a ello, lo que aumenta el riesgo por que motiva a los delincuentes", explico a Efe Sebastián Brenner, director de ingeniería para Latinoamérica y el Caribe de Symantec[44]

4.1.2. Conductas que afecta el desarrollo digital

Estas conductas de riesgo y amenaza que acompañan el desarrollo de los contextos digitales – al margen de sensaciones de inseguridad, en ocasiones inexistente o exagerada-, que, junto a razones económicas, pueden hacer

[44] La Prensa Gráfica, *Secuestro de datos golpea Latinoamérica*, (sección Economía. 2017). https://www.laprensagrafica.com/xestx_latinoamxrica_en_crisis-vf20191022mp4.html.

desistir de su implementación, con lo que puede debe ser el campo de intervención penal, generándose a menudo cierto clima de alarma social- solo a veces justificado- sobre la trascendencia de esas conductas.

Se alude en este ámbito reiteradamente, a: -la precipitación en el acceso a los sistemas digitales que, de modo imprudente favorece la acusación de daños en los sistemas, un funcionamiento indebido de los mismos o incluso el acceso ilícito a ellos.

La pérdida de privacidad por la acumulación de datos tanto en poder del gestor de los distintos sistemas como aquellos a quienes se trasmite la información que se posee y la confusión a veces entre lo público y lo privado, cuando el sistema los cuales tienen una interconexión en distintos ámbitos de actuación individual y – los propios déficits del sistema que impiden garantizar tanto su salvaguarda como interna, ya en cuanto a la propia privacidad del contenido del sistema, ya en cuanto a la tutela de los derechos de gestión digital derivados o garantizados por él, su propio funcionamiento en si mismo considerando o el correcto desarrollo de los distintos entornos que permite el mismo para los fines que le son propios.

A partir de ellos, son múltiples las posibilidades de ataques a bienes jurídicos tradicionales como la intimidad, el patrimonio o la propiedad intelectual e industrial. Pocas dimensiones de vidas dejan de verse afectadas por los procesos digitales de tiramientos de datos, que incluso van a permitir la comisión fácil de los delitos más clásicos, por ejemplo el caso ingles de quien entra en los sistemas informáticos de un hospital para modificar el programa que organiza la distribución de medicamentos de los enfermos, que sin duda daría lugar a un delito, asesinato, al menos en grado de tentativa.[45]

[45]Mata, *Derecho penal Informático,* 6.

4.1.3. Aspecto que favorecen conductas ilícitas y su lesividad

Las posibilidades de expansión, intensidad y prolongación temporal de los efectos dañosos que se pretenden con las conductas que se sirven de los contextos digitales para llevarse a cabo –favorecidas por la absoluta digitalización de vida diaria-, tanto desde una perspectiva local , como personal, el anónimo que otorga la red, la facilidad con que puede cometerse y ocultarse esos ilícitos, las dificultades de prosecución y prueba que los caracterizan, con respuestas normales tardías por carencia de competencia-les, económicas, tecnológicas e incluso de capacitación para ello y la posibilidad de obtención de rápidos beneficios, no solo económicos, han favorecido el crecimiento cuantitativos como cualitativo de este tipo de conductas.

También, resulta reseñable la característica de la trans nacionalidad de muchas de estas conductas, frente a la territorialidad propia de otro tipo de ilícitos más tradicionales, lo que hace que tanto su persecución como sanción se complique aún más, desde un punto de vista práctico, pero también jurídico, pudiendo sugerir incluso lo que ya algunos autores han denominado “paraísos para los delitos informáticos”.

Las dificultades de detención, persecución, enjuiciamiento y prueba que caracterizan a los ataques vinculados con la informática – el interés que puede existir en que se tenga conocimiento de los mismos, ya sea en el caso de ataques a empresas privadas, para no perder la confianza de los clientes, ya en el de entidades públicas, por motivos de seguridad, el incrementadas por su carácter transnacional y el surgimiento de esos nuevos “paraísos delincuenciales” son una realidad. Es cierto que se están creando nuevas secciones especializadas en delincuencia informática en los cuerpos policía-

les que facilitaran la labor de seguimiento de los ilícitos, pero también lo es que unas veces el perjudicado no denuncia el hecho, al margen de las razones antes apuntadas, por no considerarlo suficientemente importante, y otras son las propias autoridades las que no le conceden prioridad por las dificultades técnicas que conlleva su tratamiento.[46]

4.2. Derecho informático y su relación con el delito informático

La delincuencia informática se encuadra de lo que se conoce como derecho informático. Este se define como "el conjunto de normas jurídicas que regulan la utilización de los bienes y servicios informáticos en la sociedad", incluyendo como objeto de estudio: 1º el régimen jurídico del software; 2º el derecho de las redes de transmisión de datos; 3º los documentos electrónicos; 4º los contratos electrónicos; 5º el régimen jurídico de la base de datos; 6º el derecho a la privacy; 7º los delitos informáticos; y 8ª otras conductas nacidas del uso de los ordenadores y las redes de transmisión de datos.

En lugar de crear una nueva rama del Derecho dedicada exclusivamente al estudio de estos aspectos, podría haberse abordado la regulación o estudio de cuanto concierne al ámbito de digitalización del empresarial, administrativo e incluso personal desde un análisis por cada una de las del ordenamiento jurídico ya existente, en las que habría que encajar la nueva realidad informática en función del aspecto concreto a analizar.

Así, de los contratos electrónicos se ocuparía el Derecho civil y mercantil, de las conductas ilícitas vinculadas a las nuevas tecnologías el derecho administrativo o penal, etc. Sin embargo la complejidad de las relaciones

[46]Ibíd.

informáticas, el crecimiento exponencial de las mismas o el hecho de que en el estudio de estas nuevas relaciones se transite de una rama del ordenamiento jurídico a la otra constantemente (administrativa, civil, laboral o penal) ha favorecido que por motivos pragmáticos desde algunos sectores se haya reclamado la consideración de esas nueva rama del ordenamiento jurídico que regularía todas las relaciones, cuales quiera vinculadas con la informática y que tendría como características, precisamente, el hecho de que en la disciplina confluya normas administrativas civiles, laborales y penales.

La primera dificultad a la hora de afrontar el análisis de los delitos informáticos es su propia definición. No resulta fácil considerar que debe entenderse por delito informático, que conductas pueden considerarse que debe entenderse por delito informático, que conductas pueden considerarse incluidas en este término mismo y que es, en consecuencia, lo que integra el Derecho Penal Informático; de hecho la dificultad de la doctrina por proponer un concepto unitario de delito informático y las importantes discrepancias en torno al mismo han llegado incluso a proporcionar que algunos autores admitan la imposibilidad de dar una definición del mismo y renuencia de ello.

La doctrina durante años, ha debatido, acerca de si se encuentran ante una categoría específica que pueda denominarse “delito informático”, parte del problema proviene, sin duda, de la vertiginosa velocidad con la que evolucionan las nuevas tecnologías y el consiguiente constante cambio y desarrollo, también extremadamente rápido, de las conductas delictivas vinculadas a las mismas.

Por ello puede tener interés, antes de exponer los distintos conceptos de delito o delitos informático o informáticos que sean indo impulsando las nuevas tecnologías y del modo en que, en consecuencia, ha ido apareciendo

el nuevo elenco de conductas lesivas de derechos vinculadas con a la información y la telemática.[47]

4.3. Delincuencia informática, criminalidad informática o delitos informáticos

En su resolución 65/230 la Asamblea General solicito a la Comisión de Prevención de Delito y Justicia Penal que, con arreglo a lo dispuesto en el párrafo 42 de la Declaración de Salvador sobre estrategias amplias ante problemas globales: los sistemas de prevención de delito y justicia penal y su desarrollo en un mundo en evolución, estableciera un grupo intergubernamental de expertos de composición abierta para realizar un estudio exhaustivo del problema del delito cibernético y las respuestas de los Estados Miembros, la comunidad internacional y el sector privado ante ese fenómeno, incluido el intercambio de información sobre legislación nacional, mejores prácticas, asistencia técnica y cooperación internacional, con miras a examinar opciones para fortalecer las actuales respuestas jurídicas o de otra índole ante el delito cibernéticos en los planos nacional e internacional y proponer otras nuevas . La Oficina de las Naciones Unidas contra la Droga y el Delito, recopilo información durante el periodo de febrero a julio de 2012.basandose en la información recopilada del grupo de expertos en cuanto a delitos cibernéticos.

4.3.1. Conectividad mundial y el delito cibernético

En ese sentido, en el año 2001 al menos 2,3000 millones de personas, equivalentes a más de un tercio de la población total del mundo, tuvo acceso a internet. Más del 60% de todos los usuarios están en los países en

[47]Ibíd. 15- 16.

desarrollo y el 45% de todos los usuarios de internet tienen menos de 25 años. Se estimó que para 2017 las suscripciones a la banda ancha móvil llagarían, aproximadamente al 70% de la población mundial.

Para 2020 el número de dispositivito interconectados pro la red (“internet de las cosas”) será seis veces mayor al número de personas de personas, lo que transformarála concepción actual del internet.

En el mundo híper conectado del futuro será difícil imaginar un “delito informático”, o quizás ningún delito, que no implique pruebas electrónicas relacionadas con la conectividad del protocolo internet. Las “definiciones” del delito cibernético dependen, en gran medida, de la intención con que se emplee esa expresión. Un número limitado de actos contra la confidencialidad, la inseguridad y la disponibilidad de datos o sistemas informáticos se hallan en la base del delito cibernético.

Sin embargo, los actos relacionados con la informática realizados en provecho propios o para obtener beneficios económicos o perjudicar a otros, por ejemplo los delitos relacionados con la identidad y los actos que guardan relación con contenidos informáticos (los cuales quedan comprendidos todos en el significado más amplio de la expresión “delito cibernético”) impiden llegar fácilmente a definiciones jurídicas de esas de esa expresión en un sentido general.

Es preciso llegar a determinadas definiciones respecto de los actos que se hallan en la base del delito cibernético. No obstante, la “definición” de ese delito no reviste tanta importancia a otros fines, como por ejemplo definir el alcance de las facultades especializadas de investigación y cooperación internacional, ya que en este caso es preferible centrarse en las pruebas

electrónicas de cualquier delito más en un concepto amplio y artificial del delito “delito cibernético.” [48]

4.3.2. Primeras definiciones en cuanto delito informático

Las definiciones que a lo largo de los últimos cuarenta años se han establecido el concepto de delito informático van necesariamente unidas a esa evolución que ha sufrido la implementación de las TIC en la sociedad y las propias conductas delictivas, o merecedoras de serlo, vinculadas con las nuevas tecnologías de la información y de la comunicación.

Como antes se decía las primeras conductas dañosas de ciertas entidades que aparecieron unidas a la proliferación de los ordenadores se centraban, principalmente, en el ámbito empresarial y consistían en conductas lesivas del patrimonio. Por este motivo, aunque generalmente sin olvidas los posibles problemas que la acumulación de datos de carácter personal podía conllevar, que serían tratados de modo independiente al del tratamiento de la delincuencia informática en general, las primeras definiciones de lo que debía entenderse por delito informático se limitaban al ámbito patrimonial. Incluso cuando ya se vislumbraba una proliferación de tipologías muy variadas de ilícitos vinculados con las nuevas tecnologías y la problemática que podía surgir de estas.

Una de las primeras definiciones de la doctrina fue la que realiza Parker, que describió los abusos informáticos como: cualquier accidente asociado con la tecnología de los ordenadores en el que la víctima sufrió o pudo haber sufrido un daño y el autor intencionalmente obtuvo o pudo haber obtenido un beneficio. Este autor no se limitó a describir las conductas relevantes para el

[48]UNODC, *Estudio Exhaustivo del problema del delito*, 1-2.

ámbito penal sino que reconoce que se está ante un amplio abanico de conductas en las que se incluyen además de conductas de naturaleza penal, otras de relevancia civil y meros incidentes sin trascendencia jurídica. A pesar de la vertiente patrimonial de su estudio, el autor también se preocupó por los ataques a la intimidad que, con la creación de las bases de datos, podían derivarse de la digitalización de datos de naturaleza privada.

En 1978, habiendo ya saltado a la prensa algunos de los primeros casos de delincuencia informática patrimonial. Un análisis de estos delitos considerando que en la definición del delito informático el acento debe ponerse en que los ordenadores pueden ser usados por el autor del delito no solo como instrumentos para cometer el mismo sino también como objetos del delitos, este autor incluyo los delitos de sabotaje informático y robo digitalizado de la información y programas de espionaje industrial. Asimismo, se aproximó a los problemas concretos que plantea esta delincuencia, entre los que destacaba la facilidad con la que pueden ser manipulados los ordenadores y su información, la dificultad de establecer medidas de seguridad de carácter técnico, sin que, al mismo tiempo, se bloqueen la fluidez de las transacciones realizadas.

En la doctrina española, considero que no habiendo una definición de delito informático plenamente satisfactoria, debía considerarse delito informático "toda acción dolosa que provoca un prejuicio a personas o entidades, sin que necesariamente conlleve un beneficio material pasa su autor, aun cuando no perjudique de forma directa o inmediata a la víctima y en cuya comisión intervienen necesariamente de forma activa dispositivos habituales utilizados en las actividades informáticas. Dejo fuera aquellas conductas que tienen como objeto del delito los dispositivos informáticos, por la relación meramente accidental que, en su opinión, tienen estas con la informática.

Otro de los autores españoles que se acercó temporalmente a la delincuencia informática de carácter patrimonial, aunque sin olvidar los problemas en relación con la privacy que puede provocar la acumulación de datos de carácter personal en ficheros fue el autor, que destaco la imposibilidad de agrupar todos los delitos vinculados con las nuevas tecnologías en un único concepto de delito. Por ello, sin intención de dar un cataloga exhaustivo, clasifica los "ilícitos informáticos" como un conjunto de delitos de carácter heterogéneo que puede derivarse en dos grandes grupos: por un lado, la amenazas a la intimidad personal y a la esfera privada derivadas de la ingente acumulación de datos; y por otro los delitos patrimoniales favorecidos en su comisión por las posibilidades que ofrecen las nuevas tecnologías.

Cabe destacar que tanto los autores, que escribieron sobre estas cuestiones en el año 1987 y 1986 respectivamente ya mencionaban entre el catálogo de los delitos informáticos los denominados como piratería de software, que empezaban a despuntar en esa década

La proliferación de conductas delictivas o ilícitas vinculadas a la informática fue complicada la definición de los delitos informáticos, no pudiendo ya limitarse está a conductas vinculadas estrictamente con el patrimonio o con la intimidad. Por ello en 1983 un comité de expertos convocados por la Organización para la Cooperación y el Desarrollo Económicos OCDE, definió de una manera vaga e imprecisa, los computer-relatedcrimes como "cualquier comportamiento no ético o no autorizado relacionado con el procesado automático de datos y/o transmisiones de datos".

Se trata de una primera aproximación a un posible concepto, adoptado en un principio por varios autores con el argumento de que una definición de esa amplitud permitirá el tratamiento de las mismas hipótesis de trabajo para distintas disciplinas y podría así usarse una misma definición en análisis

penales, económicos, sociológicos, etc. La definición puede servir como una primera aproximación conceptual que puede resultar útil para delimitar que conductas ilícitas o indeseables tienen alguna vinculación con la informática; sobre todo, porque en los primeros años en que comenzaron estos nuevos ataques los códigos penales se encontraban ante realidades no siempre abarcadas por ellos.

De hecho, aún son muchas las conductas, como el denominado hacking blanco, cuya caracterización como delictiva es discutible y discutida en los distintos ordenamientos penales, lo que dificulta más aun la propia conceptualización del delito informático. Y, así, la pretensión del concepto de la OCDE de abarcar conductas tanto penales como extrapenales ha restado virtualidad operativa al mismo y favorecido su progresivo abandono en sede penal.

En todo caso, autores a pesar de adoptar este concepto amplio de delito informático, terminan clasificando los ilícitos informáticos en dos grupos: los delitos patrimoniales vinculados con la informática y aquellos que tienen que ver con la acumulación de datos de carácter personal en los sistemas informáticos, mencionados, sin indagar demasiado en ellos, la problemática que podía surgir con la posible comisión de delitos contra intereses supra individuales, o de cualquier otro tipo, a través de ordenadores.

A pesar de que varios autores, apoyándose en la necesidad de un concepto amplio de delito informático, adoptaron un concepto similar al antes descrito, una parte de la doctrina no tardo en poner de relieve, por un lado, la excesiva amplitud del concepto y por otro lado la escases de valor que dicha definición aporta en términos estrictamente técnicos-penales, ya que, como antes se apuntaba, se pueden incluir en el mismo tanto conductas típicas

como conductas que no encajan en la definición que establezca cada código penal.

A finales de la década de los ochenta se trato de superar las definiciones arribas expuestas, puso de relieve que no se podía considerar la existencia de un significado general predicable del delito o abuso informático. No puede hablarse de un delito informático, sino de una pluralidad de ellos, en los que la única nota común es su vinculación de alguna manera con los ordena-dores.

No se trata de delitos en los que el instrumento mediante el que quizás la aportación más importante de este autor, en este contexto sea precisamente la idea de que la delincuencia informática o los delitos relacionados con la misma indican un aspecto de la criminalidad caracterizado por las especificidades aportadas por las funciones propias del ordenador de procesamiento y transmisión automatizados de datos y de confección y/o utilización de programas para ello.

Cualquier conducta que no tenga relación con esas funciones, aunque se trate de una conducta delictiva, o deba considerarse su sanción, no formara parte, a juicio de romero, de la delincuencia informática, careciendo de importancia a su juicio si en la comisión del hecho el ordenando es el objeto sobre el que recae la conducta o el medio para cometerla, e incluso considerando irrelevante para la definición de la delincuencia informática, aunque no para el estudio de la misma, que la conducta pudiera ser considerada delictiva o fuera merecedora de serlo.

Poco después también extensamente el autor se ocupó de los problemas de definición que planteaba el delito informático. Y, si bien el ámbito que

introdujo a la autora en el análisis del concepto delincuencia informática fue el del fraude informático, en su enfoque conceptual no se centró únicamente en la delincuencia informática patrimonial, poniendo de relieve, como ya otros muchos autores que los sistemas informáticos y todos sus componentes no solo pueden ser el medio a través del que se comenten los delitos en cuestión, si no que ellos mismos pueden ser objetó de un delito.

La autora destaco, mediante varios ejemplos, que prácticamente cualquier delito puede ser cometido utilizando sistemas informáticos y, por ello descarta de antemano que en la definición del delito informático queda incluir todos los delitos en los que de alguna manera pueda aparecer involucrado un ordenador, pues cualquier delito podría entonces en su opinión calificarse como informático.

Por otra parte, y en la línea ya avanzada por, la autora considera inadecuado el término “delito” porque tiene un significado muy específico en delitos informáticos pero que no tienen su encuadre en ninguna conducta tipificada penalmente, por eso acabara explicando que no puede hablarse de un único delito informático, sino de una pluralidad de ellos, en los que la única nota común es la vinculación de alguna manera con los ordenadores, en concreto con las funciones propias del ordenador de procesamiento y transmisión automatizados de datos y de confeccione y/o utilizados de programas para ello, sin que sin embargo, sea el bien jurídico el mismo en todos los delitos informáticos ni presenten sus formas de comisión siempre las mismas características. En este sentido señala expresamente que es mejor recurrir a fórmulas menos rígidas, como la de “delincuencia informática”, que reflejen el carácter criminológico de las conductas, para incluir así tanto las conductas tipificadas como las merecedoras de serlo.[49]

[49]Mata, *Derecho penal Informático,* 18- 22.

4.3.3. Ciberdelitos

Con la expansión mundial de internet, desde algunos sectores se ha insistido en que esta facilita la comisión de delitos, aunque su consolidación no haya implicado la aparición de nuevas conductas antisociales o licitas. Las clásicas figuras delictivas, ya presentes antes de su irrupción en la realidad diaria, simplemente se han encontrado con un nuevo canal o medio que facilita enormemente su comisión, aunque también su persecución y enjuiciamiento.

Ello, no obstante, la generalización del uso de redes de transmisión de datos, en realidad sobre todo de internet, ha favorecido la utilización de nuevos conceptos en los análisis de lo que puede considerarse es el Derecho Penal Informático, al menos en sentido, si no conceptual, si descriptivo. Así un sector de la doctrina empieza a prescindir incluso del término delito informático (o delincuencia informática, si se niega la existencia de aquel) para sustituirlo por otros como ciberdelito, ciberdelitos, cibercriminalidad, etc.

El término “cibercrimen” se ha señalado que describe “el conjunto de conductas relativas al acceso, apropiación, intercambio y puesta a disposición de información en redes telemáticas, las cuales constituyen su entorno comisivo, perpetradas sin el consentimiento o autorización exigibles o utilizando información de contenido ilícito, pudiendo afectar a bienes jurídicos diversos de naturaleza individual o supra individual” se estaría ante una nueva generación de delitos, que en lugar de tener una vinculación con los sistemas informáticos, o mejor.

Además de tenerla se caracterizan por la vinculación que tienen con el uso de rede de transmisión de datos, siendo su relación con los sistemas informáticos secundaria respecto a la que tienen con las redes de transmisión de

datos. Es por eso esta vinculación con las redes de transmisión de datos lo que les otorgaría su carácter específico. En todo caso no puede negarse que todo lo que es cibernético o telemático es también, al mismo tiempo, informático, mientras que no ocurre lo mismo en sentido inverso, siendo por tanto muchos más omnicomprensiva esta última categoría.

A pesar de las discrepancias doctrinales en torno a la existencia o no de un concepto de "delito informático", cada vez son también más las voces doctrinales que en el ámbito de la delincuencia informática sostiene la necesidad de creación de una nueva categoría jurídico-penal que abarque las conductas vinculadas con el hecho informático, entendiendo que no se esta –o no en absoluto- ante la lesión de bienes jurídicos tradicionales, sino ante la lesión de un nuevo interés que merece ser objeto de atención también por el Derecho Penal.

Esta idea extendida cada vez más entre los nuevos autores no conlleva, sin embargo, una unidad de criterios a la hora de entender cómo debe explicarse este interés y como debe definirse el bien jurídico penal a que pretende hacerse referencia, las distintas posturas al respecto, no siempre tan divergentes, son básicamente: 1) seguridad informática, 2) integridad, confidencialidad y disponibilidad de los datos y sistemas informáticos, 3) intimidad informática entre otras.

4.3.4. Seguridad informática

La primera de las interpretaciones hace hincapié en la seguridad informática como bien jurídico colectivo a tutelar, objeto de ataque con las conductas vinculadas a la cuestión informática. Se trata de un bien, se dirá, cuya protección evita la lesión de una serie de bienes jurídicos de carácter individual, puestos en peligro con tales conductas atentatorias contra la

seguridad de las redes y sistemas informáticos, pero no siempre efectivamente dañosos. La extensión en el uso de redes y sistemas informáticos, se dirá, en otros términos, imprescindibles hoy para el desarrollo económico y social, para el correcto funcionamiento del ámbito tanto público como privado, hace que la protección de su seguridad sirva como medio para proteger otros bienes de carácter individual (patrimonio, intimidad, libertad sexual, honor, etc.) e, incluso, otros bienes de carácter supraindividual (orden público, la paz pública, seguridad del Estado).

Pero son esta expansión y dependencia social de las ITCs las que hacen que un ataque a ellas deba ser considerado en sí mismo como un ataque a un nuevo bien jurídico colectivo. Cuando se daña un sistema informático concreto, se señala, no solo se daña un bien jurídico individual, sino que se generan riesgos para toda la comunidad de usuarios.[50]

Como por ejemplo el citado caso de ransomware", ataque registrado de forma global el 12 de mayo de 2017, el cual aprovecho una vulnerabilidad del sistema operativo de Microsoft Windows, afectando a cerca de 200.000 ordenadores en 150 países usando el secuestro de dato, para obtener a cambio de su recuperación un valor económico a través de transacciones monetarias.

4.3.5. Integridad, confidencialidad y disponibilidad de los datos y sistemas informáticos

En un sentido bastante similar, otros autores tratan de la necesidad de proteger la integridad, confidencialidad y disponibilidad de los sistemas informáticos y de los datos contenidos en ellos. Se toma en consideración la

[50]Ibíd. 24- 25.

informatización de todos los datos, tanto pública como privada y la necesidad de poder confiar en su autenticidad y en su disponibilidad plena como garantía para un desarrollo económico y social acorde a los tiempos actuales. Esto es lo que garantiza la tutela de la incolumidad de los datos, de su libre disposición y de su mantenimiento en los términos en que los ha configurado su titular, bien jurídico también de carácter supraindividual que adelanta la intervención penal en cuanto al mismo tiempo es instrumental respecto de otros bienes jurídicos que pueden verse dañados o en peligro con el menoscabo de la accesibilidad, integridad o confidencialidad de determinados datos.

4.3.6. Intimidad informática y otras propuestas

La consideración del bien jurídico intimidad informática –habeas data o autodeterminación informática- se ha contemplado de un modo especial en la doctrina italiana –téngase en cuenta que en este ordenamiento se contempla el delito de acceso abusivo a un sistema informático, sin ulterior lesividad, ya desde el año 1993-, que entiende que lo que se ha de protegerse frente a esta clase de conductas vinculadas al hecho informático es, principalmente, el bien jurídico individual "intimidad e inviolabilidad informática". Como una nueva vertiente si se quiere de lo que es el domicilio físico de cada persona. Ello, sin prejuicio de que además se reconozca que la protección haya de ir encaminada a garantizar, también, la seguridad y la integridad de los sistemas informáticos, es decir, la seguridad informática.

En todo caso, y esto es lo importante frente a otro tipo de posturas, no se trata solo de reconocer el derecho de excluir a los demás de un determinado ámbito que el titular considera reservado y que ha de protegerse frente a intromisiones indeseadas, sino de un poder positivo de control sobre la

información personal que los demás pueden tener de cada uno y sobre el uso que puede hacer de misma. Por eso se considera necesario este nuevo concepto, entendiendo que lo que pretende abarcar no está sufrientemente garantizado ni por los tradicionales medios de tutela de la propiedad o la posesión de las cosas materiales, ni por la protección prestada al secreto, a la intimidad personal y domiciliaria o a otro tipo de bienes inmateriales.

Por lo tanto, se apunta como nuevo bien jurídico de carácter supra individual característico de los delitos informáticos la confianza en el funcionamiento de los sistemas informatizados. Como ya se ha mencionado en relación a las propuestas que aluden a la idea de la seguridad informática, los de los delitos vinculados con la informática no solo dañan en su comisión bienes jurídicos individuales y concretos; también pone en peligro la confianza de la sociedad en el buen funcionamiento de los sistemas informáticos y de las redes de transmisión de datos. La gravedad de este quebrantamiento de confianza radica, principalmente, en la propuesta de Corcoy, en la dependencia de la sociedad actual respecto de las T.I.C. para el desarrollo personal, económico y social de los individuos.

El autor afirma, por su parte, que la tecnología de internet es en sí misma un nuevo bien jurídico a proteger por el ordenamiento; un nuevo bien jurídico de primera magnitud, dirá otro autor que el derecho a la información como nuevo bien jurídico supraindividual, primordial y básico en su opinión _aunque matizando que no será el único que lesionen las conductas vinculadas con la informática-. Además, acude a la expresión “comunicación pacifica a través de las redes telemétricas, con independencia de las garantías y protección que puedan ofrecerse a bienes jurídicos como la intimidad y los datos de carácter personal”. Se ha destacado asimismo, por último, que mediante el delito informático se dañan bienes tanto personales

como patrimoniales sin reconocer con ello que se está ante conductas que atenten contra un especifico bien jurídico, se encuentra ante una categoría penal autónoma en la que el objeto de protección coincide no obstante con el de los tipos tradicionales que están siendo adoptados a las nuevas tecnologías.[51]

4.3.7. Panorama mundial del delito cibernético

Para muchos países, el aumento vertiginoso de la conectividad mundial ha llegado en medio de cambios económicos y demográficos, con crecientes disparidades en los ingresos, ajustes en los gastos del sector privado y menos liquidez financiera.

Los funcionarios encargados de hacer cumplir la ley que respondió al estudio consideraron que a nivel mundial habían aumentado los actos de delito cibernéticos a medida que tanto personas como los grupos delictivos organizados buscan nuevas posibilidades ilícitas para obtener ganancias y beneficios personales. Se estima que más del 80% de esos actos tienen su origen en alguna forma de actividad organizada, con mercados negros cibernéticos establecidos en un círculo de creación de programas informáticos maliciosos. Los delincuentes cibernéticos ya no necesitan pericias ni habilidades técnicas complejas. Especialmente en el contexto de los países en desarrollo han aparecido subculturas de jóvenes dedicados al fraude financiero relacionado con la informática, muchos de los cuales comenzaron a participar en dicho delito en sus últimos años de adolescencia.

Los actos delictivos cibernéticos son muy diversos a nivel mundial, desde actos motivados por intereses financieros y actos relacionados con el contenido informático hasta actos que atentan contra la confidencialidad, la

[51]Ibíd. 25- 27.

integridad y la accesibilidad de los sistemas informáticos. Sin embargo, los gobiernos y las empresas del sector privado perciben la amenaza y el riesgo relativo de manera diferente. En la actualidad la Estadística de delitos registrados por la policía no son una base sólida por hacer comparaciones entre países, aunque estas estadísticas suelen servir para formular políticas a nivel nacional. Dos tercios de los países consideran que su sistema de estadísticas policiales es insuficiente para registrar los delitos cibernéticos. Las tasas de delitos cibernéticos registrados por la policía se corresponden con los niveles de desarrollo del país y con la capacidad policial especializada más que con las delincuenciales existentes

4.4. Problemas de persecución de conductas lesivas en cuanto a la información y las actividades digitales en El Salvador

La era digital, según un informe del Instituto Centroamericano de Administración de Empresas (INCAE), está modificando la forma de producir y cambiando los patrones de consumo.

La tecnología está inmersa en las actividades diarias. un joven salvadoreño usa su teléfono, no solo para estar comunicado con sus familiares y amigos, sino como alarma para despertarse, pagar servicios básicos y comprar comida a domicilio para evitar salir del trabajo, especialmente, en las horas de mayor tráfico en las calles de San Salvador. Este salvadoreño usa, para comprar comida a domicilio, una llamada "Hugo", que también permite comprar bebidas, productos del supermercado y muy pronto servicio de transporte."Hugo lo que hace es acercarte diferentes servicios y productos que tú los puedes pedir desde la palma de tu mano y obtenerlos en tu casa y oficina en cuestión de minutos" sostiene el autor, director comercial de Hugo".

"La tecnología es el presente y el futuro y se cree que hay suficiente espacio de crecimiento para el mercado. Evalúa diferentes estudios que indican que para el 2020 entre el 60 y el 67% del consumo de comida de restaurantes en general va a ser a través del servicio de delivery" asegura el director administrativo de Hugo. El restaurante BuffaloWings cerró su servicio a domicilio y ahora hace sus entregas a través de la aplicación Hugo, La tecnología está modificando la forma de producir y los patrones de consumo, según INCAE.

Sin embargo, ingresar al mercado salvadoreño y que los restaurantes y clientes usaran la aplicación no fue fácil recuerda Cuéllar. "Lo común era para un restaurante recibir tus pedidos por teléfono, el introducir toda esta tecnología de que todo era digital, había un poco de resistencia, como 'no esto no se hace así', pero se han ido dando cuenta el gran beneficio que tiene esta plataforma.

Por lo tanto, esas condiciones ubican a Centroamérica en una posición difícil de competir con países que ya pueden beneficiarse de las tecnologías exponenciales existentes o aquellos que están haciendo cambios en sus modelos educativos para dotar a los estudiantes de habilidades digitales para la considerada revolución tecnológica.[52]

Como se puede ver en la anterior noticia, de fecha 27 de septiembre de 2017, la tecnología se ha vuelto una herramienta necesaria para simplificar la vida cotidiana, acelerar las relaciones sociales, y por su puesto dinamizar la economía, en un contexto globalizado. No obstante, la exponencial “digi-talización de la sociedad”.

[52]CNN En español *Tecnologías exponenciales: La cuarta revolución tecnológica*, (España, 2018). https://cnnespanol.cnn.com/2017/09/26/tecnologias-exponenciales-la-cuarta-revolucion-tecnologica/.

4.5. Problemas procesales en cuanto a la persecución de los delitos informáticos en El Salvador

El pasado 6 de febrero se aprueba bajo algún grado de confrontación en el seno de la Asamblea Legislativa el decreto 260 del 5 de febrero del 2016, mejor conocido como “Ley Especial contra los Delitos Informáticos y conexos” abreviado como LECDIC.

No cabe duda que, para algunos operadores del derecho, la ley posee “muchas incongruencias significativas,” su referencia al bien jurídico tutelado no es clara, su división capitular se presta al equivoco, su compendiosa parte especial la cual abarca 30 de 36 artículos, con frecuencia cae en una enunciación de delitos repetitiva, capaz de generar dificultades frente a las posibles fórmulas concursales cuando concurren múltiples tipos penales”.

La relación concursante entre LEDIC y Código Penal, no pasa desapercibida por este columnista, quien afirma que el principal obstáculo, más significativo, se encuentra en el campo procedimental u operativo, la normativa especial se encuentra bastante cargada en lo punitivo, pero ausente de s principales herramientas pasa perseguir aquello que señala.[53]

La Organización de los Estados Americanos (OEA) presentó el pasado 3 de junio de 2014, en el marco de la XLIV Asamblea General del organismo, el informe “Tendencias en la seguridad cibernética en América Latina y el Caribe”, elaborado en colaboración con la empresa Symantec, que ilustra y analiza los últimos acontecimientos en ciber seguridad y cibercrimen en la región.

[53]Oswaldo Feusier, “Comentarios a la ley especial contra los delitos informáticos y conexos”, *Revista Enfoque Jurídico,* (2017): 3. http://www.enfoquejuridico.info/wp/archivos/4741.

Adicionalmente, señaló que “América Latina y el Caribe es una de las regiones con mayor adopción de Internet, situación que podría generar mayores desafíos en materia de ciber seguridad. Las alianzas entre el sector público y el privado, como lo ha hecho en el caso de este reporte, son críticas para generar mayor conocimiento sobre los riesgos cibernéticos con el fin de proteger mejor a los ciudadanos, la infraestructura crítica y combatir el cibercrimen".

En el evento celebrado en Asunción, sede desde hoy y hasta el jueves de la Asamblea, el Secretario de Seguridad Multidimensional de la OEA, Adam Blackwell, destacó que la publicación “responde a la necesidad de los Estados Miembros de recibir información precisa y detallada sobre las amenazas cambiantes de ciber seguridad en el Hemisferio”.[54]

Existen dos ministerios que comparten la responsabilidad de la seguridad cibernética y la prevención del delito cibernético en El Salvador. El Ministerio de Justicia y Seguridad Pública es el líder designado para asuntos de seguridad cibernética, mientras que la responsabilidad de la investigación de cibercrímenes depende principalmente de la Unidad de Delitos Cibernéticos de la Policía Nacional Civil. Este organismo se encuentra actualmente en proceso de convertirse en una nueva Unidad de Delito cibernético. Se estableció un CIRT nacional, con la sigla SALCERT, y ya está en funcio-namiento.

Aunque aún no se ha establecido alguna política o estrategia nacional para la seguridad cibernética, ya se encuentra una en proceso de desarrollo. Actualmente, la Policía Nacional Civil está formalizando una asociación con

[54]Organización de Estados Americanos y Symantec *informe sobre seguridad cibernética en América Latina y el Caribe*, (El Salvador, 2016) http://www.oas.org/es/centro_noticias/comunicado_prensa.asp?sCodigo=C-225/14.

la Oficina de las Naciones Unidas contra la Droga y el Delito (UNODC) para recibir capacitación relacionada con el delito cibernético a fin de reforzar sus capacidades existentes, desarrolladas, hasta ahora, mediante cursos en línea autodidácticos e interacción informal con autoridades con autoridades homólogas de la región.

Se han implementado mecanismos jurídicos que permiten a la Policía Nacional Civil solicitar la cooperación de empresas privadas cuando se requiera información para combatir el delito cibernético. Sin embargo, en algunos casos la ley exige que estas solicitudes se realicen a través de la Oficina del Fiscal General, responsable de las investigaciones criminales. Actualmente, la Presidencia está evaluando la propuesta de una nueva legislación con el nombre de Ley Especial contra el Delito cibernético.

El gobierno emplea una estrategia para la recuperación de datos y la continuidad operacional de sus propias instituciones basada en el uso de dos sitios de almacenamiento remoto en tiempo real, un sitio primario y uno secundario, en los que almacena información de las bases de datos de red.

Cuando los datos están almacenados en la computadora de un usuario y no en uno de los dos sitios de almacenamiento remoto, se utiliza software forense para recuperarlos. Adentro de cada institución individual se utilizan firewalls para filtrar paquetes de información maliciosos, con el respaldo del sistema Advance Security de Oracle para seguridad de la base de datos. El acceso externo a través de una VPN (Red Privada Virtual) está protegido por contraseña. Asimismo, el gobierno manifiesta que se utilizan medidas de seguridad adicionales, no descritas en este documento, de forma rigurosa en todas sus instituciones. Los usuarios individuales reciben un manual de políticas de seguridad cibernética que les provee instrucciones explícitas

sobre el uso responsable y autorizado de sistemas de información administrados por el gobierno.

Las autoridades citan una serie de impedimentos para la mejora de la seguridad cibernética y combatir el delito cibernético en El Salvador. Los principales obstáculos son los límites de presupuesto y la falta de soporte de los ISP (proveedores de servicios de Internet) para brindar información acerca de los usuarios sospechosos de haber cometido un delito cibernético. De un modo similar, el gobierno no mantiene relaciones de cooperación con compañías establecidas fuera de El Salvador que proveen servicios de Internet relevantes, tales como proveedores de servicios de correo electrónico, redes sociales o dueños de sitios web.

Otras importantes deficiencias identificadas son la falta de un marco de trabajo legislativo integral para combatir el delito cibernético y la necesidad de más capacitación para investigadores y fiscales, además de la necesidad de brindar más oportunidades a los miembros de la Unidad de Delito Cibernético Emergente de participar en foros regionales e internacionales de desarrollo de capacidades. Finalmente, las autoridades resaltaron la falta de iniciativas de educación o concientización destinadas a informar mejor a los usuarios de Internet y TIC acerca de los riesgos y buenas prácticas para reducir sus vulnerabilidades.

Se ha informado una serie de actividades ilícitas a la Policía Nacional en los últimos años. Las autoridades comunicaron que se abrieron 72 casos de delito cibernético en 2013, que llevaron a 5 condenas. Además, desde la creación de la División de Delitos Cibernéticos en 2011, se documentaron otros 51 casos de pornografía infantil, 26 casos relacionados con amenazas o intimidación, 23 caso de diseminación ilegal de información y 15 casos de acoso sexual.

Por lo tanto, mientras que las leyes actuales no penalizan el hackeo como un delito de por sí (aunque en algunos casos se considera una forma de fraude de comunicaciones o violación de medidas de seguridad), las técnicas de hackeo se emplean para ganar acceso no autorizado a cuentas de correo electrónico y redes sociales, lo que sirve de base para cometer otras actividades ilícitas tales como extorsión, diseminación ilegal de información, etc.

Sin embargo, dado que las técnicas utilizadas para perpetrar estos últimos delitos no están penalizadas, no hay estadísticas disponibles que permitan evaluar un aumento de uso.

En un caso destacable, un depredador sexual estaba contactando víctimas jóvenes a través de redes sociales, ganándose su confianza y luego incitándolos a crear y compartir fotografías y videos sexualmente explícitos.

Se alertó a la Policía Nacional y se realizó una investigación que llevó a descubrir evidencia en la computadora del culpable. Luego, por primera vez en El Salvador, se enjuició al individuo y se lo condenó por depredación sexual de menores.

A futuro, las autoridades gubernamentales se concentrarán en la sanción de las Leyes Especiales contra Delitos Cibernéticos, la creación de una estrategia y política nacional en materia de seguridad cibernética, y el mayor desarrollo de la capacidad del personal responsable de la administración de incidentes e investigación de cibercrímenes, campañas de concientización y consolidación de las asociaciones internacionales.[55]

[55] Ibíd. 57 - 58

4.6 Definición conceptual de la informática forense y su práctica metodológica en relación con la evidencia digital

El análisis forense digital se corresponde con un conjunto de técnicas destinadas a extraer información valiosa de discos, sin alterar el estado de los mismos. Esto permite buscar datos que son conocidos previamente, tratando de encontrar un patrón o comportamiento determinado, o descubrir información que se encontraba oculta. En este post se introducirá el tema, así como la utilidad del mismo, ya sea dentro o fuera de una investigación.

En el campo de la Informática Forense existen diversas etapas que definen la metodología a seguir en una investigación: identificación, preservación o adquisición, análisis y presentación de los resultados. Siguiendo el flujo lógico de actividades, primero se debe identificar las fuentes de datos a analizar y aquello que se desea encontrar, luego se debe adquirir las imágenes forenses de los discos o fuentes de información, posteriormente se realiza el análisis de lo adquirido para extraer información valiosa y finalmente se ordenan los resultados del análisis y se presentan, de tal modo que resulten útiles.

Hace unas semanas se analizó en este blog el proceso de adquisición, comparando medidas de rendimiento y facilidad de uso, para determinar qué herramienta de adquisición de imágenes forenses elegir. Es tiempo de pasar a la siguiente etapa: el análisis de la información adquirida.

Tener una copia exacta de un disco permite al investigador acceder al sistema de archivos e inspeccionar las cuentas de usuario existentes, los documentos asociados a un usuario, y los programas instalados, entre otras cosas. Sin embargo, mediante la utilización de herramientas y suites forenses, se puede buscar una gran variedad de información que es difícil de

encontrar por simple inspección. En primera instancia, se puede indexar el contenido del disco de acuerdo con ciertas palabras clave, pudiendo realizar luego búsquedas de esas palabras, visualizando los archivos donde se encuentran y su contenido. Por ejemplo, si se quiere encontrar evidencia de un fraude, se pueden buscar palabras como “fraude”, “robo” o “soborno”.

Además, es posible realizar una recuperación de archivos borrados o datos en partes especiales del disco, como espacios no asignados. En cuanto a las comunicaciones y actividades sociales, estas herramientas proveen características para acceder a correos electrónicos almacenados, así como recuperar correos eliminados, o ver historiales de chat y de navegación por Internet.

Por último, vale la pena mencionar que se puede recuperar información como el último usuario que inició sesión, o los dispositivos USB que fueron introducidos en el equipo, entre otros datos de sesión.

Para concluir, es importante mencionar que, si bien el proceso de análisis forense se aplica principalmente en investigaciones, en las cuales se desea encontrar evidencia que soporte una hipótesis, las herramientas disponibles son cada vez más accesibles para el usuario final.

Así, es posible utilizar herramientas para realizar algunas tareas específicas, como la recuperación de archivos eliminados, en forma sencilla. Para este proceso de análisis forense existen diversas suites con capacidades integradas de recuperación de archivos, visores de correos electrónicos, imágenes y documentos ofimáticos.

También pueden utilizarse herramientas específicas para cada tarea, las cuales pueden ser gratuitas o pagas. En un próximo post se aplicarán las

actividades descriptas a un determinado caso, para observar las posibilidades que existen en este tipo de análisis.[56]

Según el autor, ingeniero informático especialista en seguridad informática en Tiger Security El Salvador y ponente de la conferencia sobre "Delitos Cibernéticos", realizada en San Salvador, El Salvador, en la cual compartió su experiencia en la recolección de evidencia digital, haciendo énfasis en la recuperación de datos.

La informática forense busca recopilar analizar la información digital que sirva para una investigación científica, su preservación como evidencia en un proceso legal, afirmando que no toda evidencia es prueba. La Evidencia digital, busca como toda investigación, respuestas en cuanto a: ¿Quién?, ¿Qué? ¿Cómo?, ¿Cuándo? y ¿Dónde? Ocurrieron los hechos, los cuales no se procesan en 10 minutos, como en la televisión.

Este es un enfoque metodológico el cual involucra: 1) Identificación 2) recolección 3) análisis 4) presentación, los cuales en la práctica se desarrollan de la siguiente manera: 1) Identificación: Ubicar la fuente relevante, encajar requerimientos de investigación, con fuentes de datos relevantes 2) Recolección: Adquisición y preservación de data de información validadora documentar el proceso 3) Análisis: Extracción de evidencia de la data, examen de evidencia, validación cruzada (es el rastreó de la información de diferentes fuentes) recolección de datos 4) presentación: Reporte, demo de la lógica para los hallazgos, presentar documentación de procesos utilizados.

[56]Matías Porolli, *Especialista de Awareness &Research "¿En qué consiste el análisis forense de la información?*" (España, 2016), 5. https://www.welivesecurity.com/la-es/2013/08/12/en-que-consiste-analisis-forense-de-informacion/.

Es importante señalar que de la metodología expuesta por Orellana en la investigación puede darse el "meta peritaje" como una doble garantía o el derecho de respuesta de la contra parte. La metra peritaje es cuando existe un peritaje previo y yo contra parte verifico el primer peritaje y detecto un mal procedimiento.[57]

4.7 Dificultades técnicas en la Policía Nacional Civil

La División de Policía Técnica Científica, abreviada DPTC, es la única dependencia de la corporación policial, encargada no solo en el embalaje y cadena de custodia de la prueba científica como lo es la balística, y química, sino que también se encarga de incautar y sistematizar la prueba digital.

Recientemente se inauguró oficialmente la implementación y desarrollo del sistema de gestión de calidad, con el propósito de mejorar la utilización de la prueba científica en el proceso de investigación, en el marco del programa de la cooperación ABA-ROLI, en la que El Salvador, junto con otros países de la región, participa para el fortalecimiento de la capacidad forense en América Central.

Este programa representa un soporte importante para que esta división alcance un alto nivel de excelencia, mediante la implementación de un sistema de gestión de calidad, y que tiene entre sus objetivos la consolidación de la coordinación interinstitucional, de la capacidad de proteger y procesar la escena del delito y de asistir la reingeniería de los procesos de las áreas que producen la prueba científica.

A partir del mes de agosto los más de 200 empleados de la División científica, entre personal técnico, policial y profesional, formarán equipos de

[57]Guardiola, *Revista Derecho y Negocio,* 12.

trabajo para lograr resultados excelentes con la implementación del sistema de calidad y control de los procesos. El plan de trabajo ahora oficializado, contempla un período que concluyo en 2015, el cual incluye una serie de pasos como la identificación, documentación de procesos, que propiciarán la certificación con la norma internacional ISO 9001: 2008, y la respectiva acreditación de competencia técnica con la norma ISO 17025: 2005.[58]

Sin duda la tecnificación de dicha unidad es el primer paso para garantizar la autenticidad de la prueba forense, incluyendo la informática forense. Según lo manifestó Alberto Molina, perito y jefe de la sección de delitos tecnológicos de DPTC, se reciben de manera semanal entre 10 y 15 contenidos en cuanto archivos de video, los cuales son verificados en cuanto a su autenticidad, ya que la fuente suele ser una cámara de seguridad, archivos de videos de teléfonos y las cámaras de tránsito, entre otros. Trabajo que cada vez se vuelve más demandante por dicha sección, puesto que de ella se auxilia Fiscalía General de la República.[59]

4.8. Dificultades técnicas en Fiscalía General de la República

En el caso de Fiscalía General de la República, es notable la demanda a la cual siendo la institución que constitucionalmente es la encargada de la persecución del delito, es notoria su capacidad limitada frente a escenarios investigativos más complejos que los delitos comunes, tomando en cuenta que el ex alcalde de San Salvador, Nayib Bukele, atacó la semana pasada, en la entrevista “Diálogo con Ernesto López”, el proceso contra los cinco

[58] Ministerio de justicia de y seguridad pública, *Policía científica implementa sistema de gestión de calidad*, (El Salvador, 2016), 8. http://www. pnc.gob.sv/portal/page/portal/informativo/novedades/noticias/Polic%EDa%20cient%EDfica%20implementa%20sistema%20de%20gesti%F3n%20de%20calidad#.W2TodNVKjIV.

[59] Julio Alberto Portillo, *Conferencia Peritaje Informático Forense de Archivo de Video*, (Universidad de El Salvador, Facultad de Química y Farmacia, 2018), 1.

acusados de los ataques digitales a los sitios web de La Prensa Gráfica y El Diario de Hoy.

Para el funcionario, la base de la imputación parte de “un meme”. “Ese no debería llamarse el juicio del troll center, se debería llamar el juicio del meme, porque lo que se hizo es un juicio sobre un meme, un meme es una parodia, un chiste de algo que sale en Internet”, dijo Bukele sobre la vista pública que inicia este lunes y se tiene previsto que finalice el jueves. Bukele justificó que no existe legislación en el país que prohíba la creación de un meme o una parodia periodística.

En ese sentido, señaló que la Fiscalía ha dicho en varias ocasiones que carece de presupuesto para sus investigaciones, pero que lleva un año y medio tratando de meter a prisión con una condena de 16 años a los jóvenes, partiendo de un meme y sin tener pruebas. Según Bukele, él defiende a los imputados porque les están queriendo destruir la vida siendo inocentes, con el objetivo de salpicarlo mediáticamente.

“No han hecho nada, simplemente por afectarme políticamente”, justificó. Dijo que, aunque La Prensa Gráfica ha hecho publicaciones donde lo liga con los imputados en la red de ciberataques, la Fiscalía le notificó en dos ocasiones, en noviembre y diciembre de 2016, que no hay investigación abierta contra él. Además, puede leer: Juez caso ciberataques: hay una persona que no está procesada, pero daba órdenes, La semana pasada, Bukele demandó a La Prensa Gráfica ante el Tribunal de Sentencia de Santa Tecla por calumnia y difamación, a pesar que ya el Juzgado de Paz de Antiguo Cuscatlán había fallado en favor del rotativo.

Por la nueva demanda, la Sociedad Interamericana de Prensa (SIP) se pronunció. El presidente de esta, Matt Sanders, dijo que era inquietante que la

demanda constituya acto de intimidación contra los medios y pretenda una censura periodística. La semana pasada, Bukele demandó a La Prensa Gráfica ante el Tribunal de Sentencia de Santa Tecla por calumnia y difamación, a pesar que ya el Juzgado de Paz de Antiguo Cuscatlán había fallado en favor del rotativo.

Por la nueva demanda, la Sociedad Interamericana de Prensa (SIP) se pronunció. El presidente de esta, Matt Sanders, dijo que era inquietante que la demanda constituya acto de intimidación contra los medios y pretenda una censura periodística.[60]

4.9. Procuración de justicia en El Salvador en relación a los delitos informáticos

En el caso de poder jurisdiccional, no cambia el panorama, considerando lo expresado por el ex alcalde de San Salvador "Me da risa, a nadie le importa. A nadie le interesa lo de los troles", con esas frases el ex alcalde edil, Nayib Bukele restó importancia a la resolución del juzgado Segundo de Instrucción que envió a juicio a cinco personas por los ciberataques contra el periódico La Prensa Gráfica. Bukele dijo ayer durante el cambio de nombre de una calle en San Jacinto, que le "tiene sin cuidado los ataques políticos, venga de donde vengan" en contra de él. "El Ministerio Público debería estar trabajando contra la violencia. A nadie le interesa lo de los troles", repitió Bukele al final del evento en San Jacinto.

El juez determinó que los implicados seguirán procesados por violación de derechos de autor y derechos conexos, violación de distintivos comerciales,

[60]El Salvador. Com, *Bukele: "Lo que hizo es un juicio sobre un meme"*, (El Salvador, 2017) https://www.elsalvador.com/noticias/nacional/371839/bukele-lo-que-se-hizo-es-un-juicio-sobre-un-meme/.

falsedad material y agrupaciones ilícitas en perjuicio de La Prensa Gráfica, pero quedan exonerados de todos los delitos en el caso de El Diario de Hoy, pese a una apelación de la Fiscalía General de la República.

El tribunal decidió que Ricardo Ortiz Lara, José Navarro, Mayra Morán, Oscar Domínguez, Hugo Erazo y Sofía Medina; a quienes la Fiscalía acusa de ser los autores materiales de la clonación del sitio web del periódico pasen a juicio y sigan el proceso en libertad condicional bajo una nueva fianza. Juez Segundo de Instrucción de Santa Tecla concluyó que hay una persona que no está siendo procesada, pero que daba las órdenes en el caso de los ciber ataques a La Prensa Gráfica.

En los diferentes peritajes hechos por la Fiscalía General existen y se mencionan conversaciones entre el alcalde Bukele y algunos de los imputados que ayer pasaron a juicio, donde se les instruía sobre los ataques contra ambos periódicos.

Sobre ese punto, el abogado de La Prensa Gráfica, Arístides Perla señaló al final de la audiencia que “se ha dicho desde un principio que se requirió del contacto del señor Nayib Bukele para cometer este ciberataque y eso el juez lo ha dicho reiteradamente en su resolución, que hay unapersona arriba de los que están acá, que dirige esta organización”.

4.10. Investigación de delitos a través de las nuevas tecnologías y el potencial nacional y regional con empresas y especialistas en la materia

Es claro que ya para el año 2014, la Organización de Estados Americanos, en conjunto con la empresa especializada en seguridad informática, Symantec, señalaban que, específicamente en el país, la efectiva persecución de la cibercriminalidad enfrentaba como uno de sus principales obstáculos: (…) los

límites de presupuesto y la falta de soporte de los ISP (proveedores de servicios de Internet) para brindar información acerca de los usuarios sospechosos de haber cometido un delito cibernético.

De un modo similar, el gobierno no mantiene relaciones de cooperación con compañías establecidas fuera de El Salvador que proveen servicios de Internet relevantes, tales como proveedores de servicios de correo electrónico, redes sociales o dueños de sitios web (OEA, 2014: 57-58).

De alguna forma, el informe OEA-Symantec solo resaltó lo que algunos medios de comunicación ya habían señalado sobre esta materia, para el caso, en noviembre del 2011, el periódico digital La Página ya había publicado la nota "Policía y fiscalía enfrentan profundas debilidades ante "ciber delitos"", en la cual se entrevistaba al jefe de la unidad de Delitos Especializados de la PNC, quien destacaba como una importante dificultad operativa que: "La ley no obliga a las empresas servidoras de Internet a guardar un respaldo del registro de IP de todos los que se van conectando en el servicio web a los servidores de ellos".

Como se sabe, una de las principales dificultades de la persecución de la cibercriminalidad, consiste en la dificultad para identificar a su autor, que fácilmente puede ocultarse tras el anonimato y opacidad que ofrecen las modernas y universales redes informáticas, altamente complejas, e intervenidas por múltiples operadores privados (Flores Prada, 2012).[61]

Las conclusiones del informe destacan que actualmente en la región, "los usuarios están sufriendo el impacto de amenazas que son tendencia a nivel mundial, y de otras propias de cada región". "Como agravante de este

[61]Feusier, *Comentarios a la Ley Especial,* 5.

desafío” sigue el informe, “América Latina y el Caribe tienen la población de usuarios de Internet de más rápido crecimiento del mundo, con un aumento del 12 por ciento durante el último año”. Asimismo, identifica cinco principales tendencias que afectan a la región: el aumento en las violaciones de datos; los ataques dirigidos; las estafas en medios sociales; el uso de virus 'troyanos' bancarios y robos; y la atracción a los eventos de gran convocatoria, como por ejemplo el Mundial de fútbol, para los ciber delincuentes.

El informe incluye contribuciones de Microsoft, la Comunidad de Policías de América (AMERIPOL) y otras organizaciones como el Internet Corporationfor AssignedNames and Numbers (ICANN), theLatin American and Caribbean Internet AddressesRegistry (LACNIC), and the Anti-PhishingWorkingGroup (APWG), así como la sociedad civil y otros socios del sector privado.[62]

[62]OEA y Symantec *informe sobre seguridad cibernética,* 23.

CONCLUSIONES

En El Salvador con la finalización del conflicto armado, la integración a una economía neoliberal y la creación de nuevas instituciones como la Policía Nacional Civil, la cual constitucionalmente tiene la función de salvaguardar la seguridad pública como un ente coercitivo del Estado en el debido proceso, con enfoque de derechos humanos desde 1992. Siendo este su antecedente reciente adentro del aparataje estatal, su rol y actuación ante el fenómeno de la ciber criminalidad es más protagónico que Fiscalía General de la República y la Corte Suprema de Justicia, puesto que esta institución fue la primera en recibir el apoyo técnico de la Oficina Contra Delitos Especializados y Drogas, de Naciones Unidas, UNODC. Insumos y recursos integrados a la división científica de la PNC, con la conformación de la primera unidad especializada en la investigación, recolección, embalaje y presentación de la prueba digital, proveniente del Estado Salvadoreña, de la cual tanto el ministerio público como el órgano jurisdiccional se auxilia, llevando sus recursos tanto técnicos como humanos de por sí ya limitados a enfrentar dificultades para cubrir la demanda creciente frente a la saturación pericial.

Por otra parte, existe un problema de denuncia e impunidad en general, pero particularmente asociados al fenómeno digital en el sentido que es claro que en temas económicos las entidades privadas no denuncias o no realizan las investigaciones pertinentes frente a una situación como por ejemplo: desfalcos, clonaciones de tarjetas de créditos, y estafas vinculadas a la ciberdelincuencia, debido al tema de imagen, rentabilidad y confianza frente a sus clientes, específicamente las instituciones financiaras. Situación que dificulta el accionar de las autoridades. Circunstancias que son similares en

las instituciones públicas, puesto que al gobierno y en si al Estado no le conviene aceptar las deficiencias o vulnerabilidades a las que sus sistemas informáticos pueden estar expuestos, así como el robo y hurto de información confidencial o personal, tanto de sus funcionarios como empleados, así como el de sus usuarios.

Es indiscutible que, el desarrollo de las Tecnologías de la Información y Comunicación en un contexto globalizado, pese a las notorias ventajas e impactos positivos en la sociedad. Las conductas inaceptables como los daños directos o indirectos hacia las personas, son cada vez más incontrolables frente a la respuesta retardada de los Estados. Basta con mencionar el caso puntal de la explotación infantil o explotación en niñez y adolescencia, ya que si bien es cierto este problema tiene antecedentes históricos, su impacto y masificación tiene una vinculación directa con el desarrollo de las tecnologías, (poner lo que dice el informe de la ONUDC) esto ligado a las limitaciones o diferencias de los Estados en su marco normativo, siendo unos más flexibles que otros, frente al accionar no solo de las empresas transnacionales, si no que a la articulación cada vez más organizada de la red oscura en la internet, la cual no solo alienta o los depredadores sexuales, si no que generar un mercado negro digital el cual cada vez es más eficiente y rentable ya sea para las redes de narco trafico como las de tratas de personas, sin dejar de lado las estafas masivas por medios de secuestros de datos (poner lo del secuestro de datos), siendo cuestionable la inoperancia de las autoridades así como su limitación frente a un esquema globalizado que cruza las fronteras y la soberanía de cada país.

Abonado la falta de tratados internacionales o normativas regionales para evitar la distorsión frente a l tipificación de los delitos, siendo una barrera la falta de homogenización de las leyes secundarias, en razón que dichos

delitos por su naturaleza pueden ser transnacionales o cometidos desde el exterior.

Ante la notoria dificultad económica que presentan las instituciones Estado para solventar las necesidades de la ciudadanía, es necesario buscar mecanismos viables para enfrentar el fenómeno de la cibdercriminalidad en cuanto al trabajo investigativo, situación que más allá de pasar por un tema de presupuesto, es eminentemente técnico. Motivo por el cual tomando tal problemática se vuelve necesario no solo establecer convenios de cooperación con organismos internacionales como UNODC, sino que también con instituciones como la policía montada de Canadá, y empresas privadas que dedican su desarrollo tecnológico en cuanto a la seguridad informática de forma preventiva, como Symatec, sino que también puede ser aliados estratégicos en brindar herramientas técnicas para el embalaje incautación y sistematización de la prueba digital en un proceso penal.

Se concluye que se debe de establecer una política integral como eje fundamental fortaleciendo el aspecto coercitivo del Estado, en cuanto la investigación y peritaje del debido proceso, en el sentido de establecer acuerdos sostenibles con el sector privado, así como organismos especializados en soporte técnico que permitan garantizar la reproducción y seguridad de la prueba al momento de judicializar las conductas delictivas al fenómeno cibernético.

RECOMENDACIONES

Las ventajas obtenidas, en cuanto a que El Salvador cuenta desde el año 2016, con su propia Ley Especial de Delitos Informáticos y Conexos a pesar de no contar con instrumento regional, las expectativas de dicha ley en cuanto a la parte sustantiva si reúnen los estándares mínimos, pese a la tema de delitos concursarle, el cual puede ser el punto de partida para solicitar las reformas necesarias como la ampliación de su tipificación en cuanto a los delitos económicos como en la restructuración del tema procesal, partiendo de la experiencia de la Policía Nacional Civil, sobre la cual en la práctica no debería de recaer toda la responsabilidad procesal que hoy en la práctica así se maneja, incluyendo en el cuerpo normativo el rol protagónico de la Fiscalía General de la República.

En relación con lo anterior se considera recomendable la restructuración de Fiscalía General de la República y Policía Nacional Civil en razón del fenómeno, gozando de flexibilidad a la hora de poder nombrar peritos especializados en informática forense, puesto que en las etapas preliminares de la investigación es donde mejor resultados se obtienen al momento de presentar la evidencia digital-.

El Salvador debe proponer una respuesta efectiva frente a su desventaja con países industrializados, en la búsqueda de acuerdos técnicos no solo en la persecución del delito si no en la prevención de los mismos tomando como una apuesta principal establecer convenios de cooperación no solo con organismos internacionales como lo son UNODC, así como la cooperación conjunta de empresas transnacionales que brindan soporte en seguridad informática tomando como una apuesta principal la modernización de las instituciones públicas, así como los controles en cuanto al tráfico de

información de su población que cada vez digitaliza su cotidianidad, llegando a acuerdos regionales con los proveedores de Tecnologías de la Información y Comunicación, como ya se hizo en el pasado con el tema de la piratería, esto con la finalidad de establecer alianzas estratégicas con el sector privado en beneficio de la ciudadanía, que a su vez garantizaría que el derecho a información y acceso a las TIC de forma segura partiendo de la tutela colectiva a la individualidad de la persona.

.

BIBLIOGRAFIA

LIBROS

Alvarado, Rolando y Ronald Morales, *Cibercrimen*, IUS Ediciones, España, 2012.

Lidón, José María *Cuadernos Penales, delitos e informática: Algunos Aspectos*, Universidad de Deusto, Bilbao, 2007.

Mata Barranco, Norberto J. *Derecho penal Informático*, Instituto Vasco de Criminología, España, 2007.

Morales, Saúl Ernesto *El Ofrecimiento y valoración de la prueba en el Cogido Procesal Civil y Mercantil Salvadoreño,* Unidad Técnica Ejecutiva del Sector de Justicia, El Salvador 2016.

Nava Garces, Alberto *Delitos Informáticos*, Editorial Porrúa, México, 2007.

Portillo, Julio Alberto *Conferencia Peritaje Informático Forense de Archivo de Video*, Universidad de El Salvador, Facultad de Química y Farmacia, 2018.

TESIS

Cuestas, Rosa María Elena y Marta Alicia Moreno, *"Avance Tecnológico de las Computadoras en El Salvador y su importancia en el desarrollo del país"*, tesis de grado Universidad Centroamericana Jose Simeón Cañas, San Salvador, El Salvador, 1979.

Montaño Álvareza, Alejandro Armando “La problemática jurídica en la regulación de los delitos informáticos”, tesis de grado, Facultad de Derecho, Universidad Nacional Autónoma de México, 2008.

LEYES

Código penal de El Salvador D.L. No. 1030, de fecha 26 de abril de 1997, D.O. No. 105, Tomo 335, del 10 de junio 1997.

Código penal de el salvador D.L. No. 1030, de fecha 26 de abril de 1997, D.O. No. 105, Tomo 335, del 10 de junio 1997.

Código procesal penal alemán, 15 de mayo de 1871, reforma 31 de enero de 1998.

Código procesal penal, D.L. No. 733, de fecha 22 de octubre de 2008, D.O. No. 20, Tomo 382, de fecha 30 de enero de 2009.

Constitución de la República De El Salvador, D.C. 38, del 15 de diciembre de 1983, D.O. No 234, Tomo 281, del 16 de diciembre de 1983.

Ley especial contra delitos informáticos y conexos D.L. No. 260, de fecha 4 de febrero de 2016, D.O. No. 40, Tomo 410, del 26 de febrero 2016.

Ley general de telecomunicaciones, D.L. No. 142, de fecha 6 de noviembre de 1997, D.O. No. 218, Tomo 337, de fecha 21 de noviembre de 1997.

ley sobre la firma electrónica, D.L. No. 133, de fecha 1 de octubre de 2015, D.O. No. 196, Tomo 409, de fecha 26 de octubre de 2015.

JURISPRUDENCIA

Sala de lo Contencioso Administrativo, *Sentencia declarativa pronunciada por el Registrador de la Propiedad Intelectual y Director Ejecutivo Centro Nacional de Registro, referencia 64-2006.* (El Salvador, Corte Suprema de Justicia, 2003).

INSTITUCIONAL

Guia de Luxemburgo, *Para la Orientaciones Terminológicas para la Protección de Niñas Niños y Adolescentes contra la Explotación y el Abuso sexual*, (Grupo de Trabajo Interinstitucional en Luxemburgo, 2016).

Policía Nacional Civil *Portafolio de servicios Institucionales*, 2°edición (División policía técnica y científica, El Salvador, 2016) 5.

UNODC, United Nations Office on Drugs and Crime, *Estudio Exhaustivo del Problema del Delito Cibernético y las respuestas de los Estados miembros, la comunidad internacional y el sector privado ante ese fenómeno*, (Estados Unidos, 2013).

REVISTAS

Cassou Ruiz, Jorge Esteban, “Delitos Informáticos en México”, *Revista del Instituto de la Judicatura Federal, No. 28, México*, (2015): 216.

Guardiola Salmerón, Miriam y Mario Orellana, Conferencia “Delitos Cibernéticos” *promovida por la Revista Derecho y Negocios, San Salvador El Salvador*, (2017):23.

SITIOS WEB

Agencia Estatal *Boletín Oficial del Estado*, (España, 2016). https://boe.es/buscar/act.php?id=BOE-A-1999-23750

Boe.es *Boletín Oficial del Estado* (España, 2016), 5. https://www.boe.es/buscar/act.php?id=BOE-A-2002-13758

Boe.es *Ley de Servicios de la Sociedad de la Información y Comercio Electrónico* (España, 2016), 2. https://www.boe.es/buscar/act.php?id=BOE-A-2002-13758,

Campus Usal, *Reglamento de medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal*, (España, 2016), Artículo 1. https://www.boe.es/buscar/doc.php?id=BOE-A-1999-13967.

CNN En español *Tecnologías exponenciales: La cuarta revolución tecnológica*, (España, 2018). https://cnnespanol.cnn.com/2017/09/26/tecnolo gias-exponenciales-la-cuarta-revolucion-tecnologica/

Computer Forensic *definición de delito informático* (El Salvador, recovery labs 2019), 23. http://www.delitosinformaticos.info/delitos_informaticos/definicion.html

Division Computer Forensic *Delitos Informáticos*, (España, 2016), https://delitosinformaticos.info/delitos_informaticos/legislacion.html

El Salvador. Com, *Bukele: "Lo que hizo es un juicio sobre un meme"*, (El Salvador, 2017) https://www.elsalvador.com/noticias/nacional/371839/bukele-lo-que-se-hizo-es-un-juicio-sobre-un-meme/.

Feusier, Oswaldo “Comentarios a la ley especial contra los delitos informáticos y conexos”, *Revista Enfoque Jurídico,* (2017): 3. http://www.enfoquejuridico.info/wp/archivos/4741.

José Rivas *Historia de la Computadora en El Salvador,* (El Salvador, blog Hitos salvadoreños en temas de informática, energía, comunicaciones, 2017), 2. http://histsv.blogspot.com/2016/04/historia-de-la-computacion-en-el_23.ht ml,

La Prensa Gráfica, *Secuestro de datos golpea Latinoamérica*, (sección Economía. 2017). https://www.laprensagrafica.com/xestx_latinoamxrica_en_crisis-vf20191022mp4.html.

Lito Ibarra, *¿Cómo está El Salvador en tecnologías de información y comunicaciones (TIC)? ,* (El Salvador, Blog de Tecnología La Prensa Gráfica, 2011), http://blogs.laprensagrafica.com/litoibarra/?p=1646.

Matías Porolli, *Especialista de Awareness&Research “¿En qué consiste el análisis forense de la información?*” (España, 2016) 5.https://www.welivesecurity.com/la-es/2013/08/12/en-que-consiste-analisis-forense-de-informacion/

Miguel Estrada Garavilla, *Los Delitos Informáticos tratamiento Internacional,* (El Salvador, 2016) https://la-razon.com/la_gaceta_juridica/delitosinformaticos-Tratamiento-internacional_0_2450155056.html.

Ministerio de justicia de y seguridad pública, *Policía científica implementa sistema de gestión de calidad*, (El Salvador, 2016), 8 http://www. pnc.gob .sv/portal/page/portal/informativo/novedades/noticias/Polic%EDa%20cient%EDfica%20implementa%20sistema%20de%20gesti%F3n%20de%20calidad#.W2TodNVKjIV

Noticia jurídica, Ley *Orgánica de Protección de Datos de Carácter Personal* (España, 1999). http://noticias.juridicas.com/base_datos/Admin/lo15-1999.html

ONU *Orientaciones terminológicas para la protección de niñas niños y adolescentes contra la explotación y el abuso infantil,* (España, 2017). http://srsg.violenceagainstchildren.org/sites/default/files/documents/docs/Terminology%20guidelines_SPA.pdf

Organización de Estados Americanos y Symantec *informe sobre seguridad cibernética en América Latina y el Caribe*, (El Salvador, 2016) http://www.oas.org/es/centro_noticias/comunicado_prensa.asp?sCodigo=C-225/14

The Franco Journal, *ciber-delincuencia y el Convenio de Budapest* (Budapest, 2017) https://thefrancojournal.com/2015/06/24/laciberdelincuencia-y-el-conve nio-de-budapest/.

Universidad de Navarra, Concepto Jurídico Indeterminado, (España, 2016) 2. https://dadun.unav.edu/.../1/CONCEPTO%20JURÍDICO%20INDETERMINADO