UNIVERSIDAD NACIONAL AUTÓNOMA DE NICARAGUA

UNAN-León

FACULTAD DE CIENCIAS JURÍDICAS Y SOCIALES

Monografía para optar al Título de:

Licenciatura en Derecho

# "LA CIBERDELINCUENCIA Y SU REGULACIÓN JURÍDICA EN CENTROAMÉRICA CON ÉNFASIS EN COSTA RICA, EL SALVADOR Y NICARAGUA".

AUTORES:

Br. Elisa de la Cruz Chavarría Pérez.

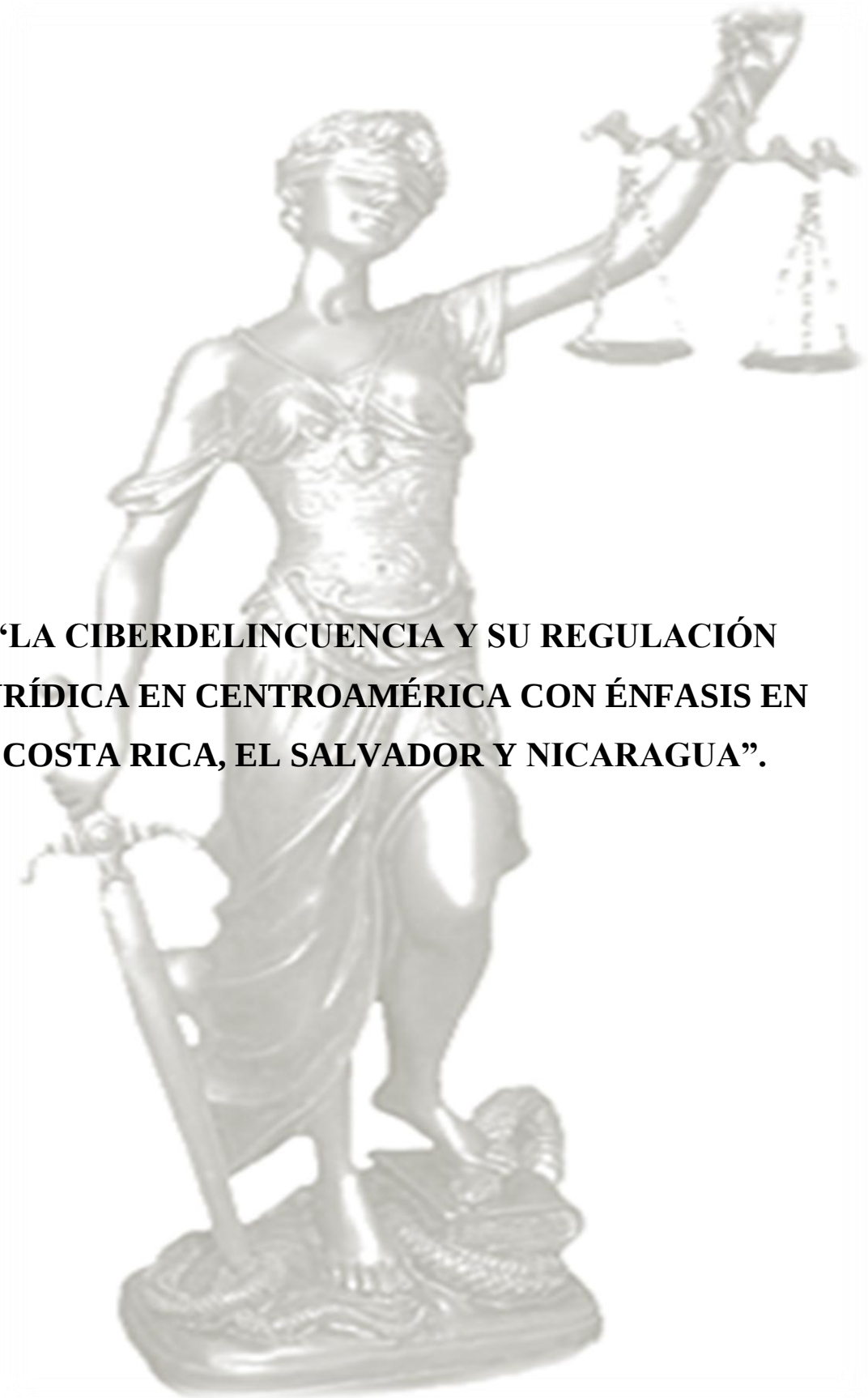
Br. Marcos Antonio Jirón Vargas.

Br. Freddy Alfonso Miranda González.

TUTOR: Dr. Denis Iván Rojas Lanuza.

León, Nicaragua, Agosto del 2016

"A LA LIBERTAD POR LA UNIVERSIDAD"



# “LA CIBERDELINCUENCIA Y SU REGULACIÓN JURÍDICA EN CENTROAMÉRICA CON ÉNFASIS EN COSTA RICA, EL SALVADOR Y NICARAGUA”.

## AGRADECIMIENTO

Primeramente le damos gracias a Dios por permitirnos llegar a este momento de nuestras vidas, donde hemos logrado culminar nuestra carrera, por los triunfos, experiencias y momentos difíciles que nos permitieron crecer y aprender cada día más.

A nuestros padres, a quienes les debemos todo en la vida, por su cariño, comprensión, paciencia, por el gran sacrificio que han hecho para poder estar donde hoy en día estamos y ser personas de bien en la vida y sobre todo por cultivar e inculcar el sabio don de la responsabilidad.

A esta prestigiosa Universidad porque sabemos que han preparado a grandes profesionales que han marcado el cambio en la humanidad y también a cada uno de los docentes que compartieron de sus enseñanzas.

A nuestro Tutor, por guiarnos en el camino de este último paso para la culminación de nuestra carrera, por la comprensión, apoyo y consejos brindados en este camino.

Culminamos con esta frase que significa mucho en nuestras vidas y que se quedará plasmada como tinta indeleble en la mente de todos los que la lean.

**“LA GRANDEZA DE UN HOMBRE SE DEJA PLASMADA CON HECHOS QUE DESAFÍAN AL TIEMPO”**

*César Coronado Castillo Ventura*

## *DEDICATORIA*

### *A DIOS*

*Por convertir mis crisis en oportunidades, las pruebas en enseñanzas y los problemas en bendiciones, pero sobre todo por ser la fuerza que me ayuda a mantenerme en pie y sin quien no soy nada.*

### *A mi madre Rosario de la Concepción Pérez Hernández.*

*La heroína que batalla día a día la constante guerra de la vida por formarme como una mujer de bien, a ti que fuiste mi médico sin trabajar en un hospital, a ti que fuiste mi maestra sin haber estudiado magisterio, a ti que sin ser abogada has sido mi mejor defensora, a ti que sin ser mago hiciste desaparecer mis lágrimas, a ti que sin pedirme nada me lo diste todo, a ti que más que ser mi madre supiste ser mi ángel.*

### *A mi Hija Azalia del Rosario Lanzas Chavarría.*

*A ti mi princesita de dulces juegos y travesuras que me impulsas a seguir adelante, contigo el fracaso no es una opción sino un reto constante a vencer, a ti mi angelito que con tu dulce sonrisa me enseñaste a correr tras el éxito con la misma fuerza con que tu corres por la pelota al jugar por la vida.*

### *A mis Amigos*

***Shiam José Ríos Alvarado, Edipcia Ninet Vanegas Bohórquez, José Gabriel Espinoza Blanco y Marcos Antonio Jirón*** *quienes no solo fueron un gran apoyo emocional durante el tiempo en que escribía esta tesis, sino también la fuerza que me alentó a continuar, aun cuando parecía que me iba a rendir.*

*A ustedes que me enseñaron que el éxito no se mide por lo que logras sino por los obstáculos que se superan.*

***A mis maestros***

***Denis David Reyes, Patricia Buitrago y Denis Iván Rojas Lanuza,*** *quienes nunca desistieron al enseñarme, quienes me enseñaron que la educación es la arma más poderosa para cambiar el mundo y que el éxito es la suma de esfuerzos repetidos día a día y que la educación no es la respuesta a la pregunta, sino el medio para encontrar respuesta a todas las preguntas.*

***A Gladys María Ruíz.***

*Quien más que maestra y amiga me enseño, que las metas son como las estrellas, no siempre podrás alcanzarlas pero siempre te servirán de guía.*

*A todos los que me apoyaron para escribir y concluir esta tesis.*

*Para ellos es esta dedicatoria de tesis, pues es a ellos a quienes se las debo por su apoyo incondicional.*

***ELISA DE LA CRUZ CHAVARRÍA PÉREZ.***

## *DEDICATORIA*

### *A DIOS*

*Porque su amor y misericordia no tiene fin, me permite sonreír ante todos mis logros que son el resultado de su ayuda, por convertir mis lágrimas en sonrisas, mis tristezas en alegrías, mis problemas en bendiciones y mis debilidades en mi fortaleza.*

### *Mis Padres*

***Maria Auxiliadora Vargas Laínez y Francisco Teodoro Jirón,*** *por haberme forjado como la persona que soy, a ustedes que me enseñaron que grande no es el que nunca falla sino el que nunca se dá por vencido. A ustedes que me enseñaron que lo unico imposible es aquello que no se intenta. Y que las mejores batallas no se ganan con espadas sino cuando doblas tus rodillas y te humillas ante Dios.*

### *A mi Familia*

*A ustedes, que son los pilares que me sostinen cuando creo que voy a desmoronarme, a cada uno de ustedes que me enseñaron que la familia es donde empieza la vida y el amor nunca termina.*

*A ustedes dedico este trabajo.*

***MARCOS ANTONIO JIRÓN VARGAS.***

## *DEDICATORIA*

***A Dios y la Virgen María.***

*Por darme la oportunidad de vivir, por fortalecer mi corazón e iluminar mi mente.*

***A la memoria de mi Padre Fredy Miranda y mi Hermano Jimmy Walter González.***

*Personas que en vida hicieron lo necesario para motivarme con mis estudios de niveles inferiores y a seguir con los estudios universitarios.*

***A mi madre Anselma González:***

*Por sus valiosos consejos de cómo se deben realizar las cosas en esta vida.*

***A mi Mamita Políta***

*Por la educación que me dio desde pequeño.*

***A mis hermanos, sobrinitos y tíos***

*Por el apoyo dado en todo momento y la motivación constante que me ha permitido ser una persona de bien.*

***A Lesbia Reyes***

*Por su amor y apoyo en todo tiempo, y su apremio constante, que me ha hecho lograr todas mis metas y proyectos.*

*A ustedes dedico este trabajo.*

***FREDDY ALFONSO MIRANDA GONZÁLEZ***

# ÍNDICE

## ABREVIATURAS UTILIZADAS

- **UCR:** Universidad de Costa Rica.
- **CRNET**: Red Nacional de Investigación de Costa Rica.
- **RED BITNET:** Because It's Time NETwor, (Red Porque ya es Hora).
- **RACSA:** Radiográfica Costarricense S.A.
- **ANTEL:** Asociación Nacional de Telecomunicaciones.
- **CONICIT:** El Consejo Nicaragüense de Ciencia y Tecnología.
- **UNI:** Universidad Nacional de Ingeniería.
- **INAA:** Instituto Nicaragüense de Acueducto y Alcantarillado.
- **INE:** El Instituto de Energía.
- **OCDE:** Organización para la Cooperación y el Desarrollo Económico.
- **IP: Internet Protocol (**Protocolo de Internet).
- **ONU:** Organización de Naciones Unidas.
- **FBI:** Federal Bureau of Investigation (Federal de Investigaciones).
- **OMPI:** Organización Mundial de la Propiedad Intelectual.
- **ISP:** Internet Service Providers (proveedores de servicios de interconexión informática).
- **DI:** Delitos Informáticos.
- **PI:** La propiedad intelectual.

# INTRODUCCIÓN

Las nuevas tecnologías están cambiando los comportamientos de la sociedad a una velocidad nunca antes vista en la Historia de la Humanidad. En esta nueva era, se producen nuevos hábitos y disfunciones en los individuos, que adquieren una nueva identidad social como usuarios capaces de acceder, crear, compartir, modificar información y conocimiento.

Hoy en día, el internet se ha convertido en un instrumento de comunicación, obtención de recursos e intercambios electrónicos, lo que conlleva importantes repercusiones en los distintos sectores sociales, económicos, jurídicos y culturales.

Al crecer el éxito comercial de esta herramienta informática, creció también la forma de vulnerar o trampear sus seguridades, llegando a ser cada vez más frágiles, pasando a ser de un elemento simplemente informativo de carácter social, a un ambiente de comercio y finanzas, en forma que casi todo intento de protección es rápidamente vulnerado, desde ahí comenzó el asunto más álgido, que ha causado tantos problemas a grandes compañías e incluso a gobiernos enteros.

La definición del Tema: **"La ciberdelincuencia y su regulación jurídica en Centroamérica con énfasis en Costa Rica, El Salvador y Nicaragua",** representa el interés de conocer a mayor profundidad el fenómeno social y jurídico que envuelve a la Ciberdelincuencia ya que hoy en día encontramos una serie de vacíos legales en nuestro ordenamiento jurídico, en cuanto a la disciplina del Derecho Informático; puesto que Nicaragua no

regula la ciberdelincuencia a través de una ley especial, que incorpore las nuevas conductas criminales que envuelven el fenómeno de la criminalidad informática, debido a que la informática se mueve más rápido que la legislación, existen diversas conductas criminales por vías informáticas que escapan de ser consideradas como delito; producto de esta situación los usuarios de internet que son víctimas de ciberataques quedan con cierta incertidumbre a la hora de buscar protección, creándose cierto estado de vulnerabilidad a los usuarios.

Así mismo la escasa publicación a nivel doctrinario y jurisprudencial en el área del Derecho informático, hizo que este trabajo estuviese motivado en abordar el tema de la criminalidad informática por ser un tema que no se encuentra regulado apropiadamente en Nicaragua a diferencia de El Salvador y Costa Rica que si previenen y sancionan este comportamiento delincuencial.

De lo anterior, surgen las siguientes preguntas de la investigación: ¿Qué particularidades envuelven al fenómeno de la ciberdelincuencia? ¿Cuáles son las principales causas que impiden la regulación de los ciberdelitos? ¿Qué instrumentos jurídicos están adoptando los países centroamericanos para combatir la ciberdelincuencia?

En base a lo desarrollado se han elaborado los siguientes objetivos: Como Objetivo General de esta investigación se planteó: Realizar un análisis general de la ciberdelincuencia y en especial en los países centroamericanos; así mismo para la consecución del presente trabajo se han planteado los siguientes Objetivos Específicos: Dar a conocer los conceptos básicos que envuelven al fenómeno de la ciberdelincuencia, comparar las legislaciones que

preceptúan los delitos informáticos, e identificar los retos que impiden la regulación del fenómeno de la ciberdelincuencia e indicar la incidencia de la cooperación internacional en esta materia.

En la elaboración de esta investigación utilizamos el método Comparativo/Inductivo-Deductivo. Comparativo pues fue menester hacer uso de los instrumentos legislativos de las Repúblicas de Costa Rica, El Salvador y Nicaragua, y otras legislaciones internacionales para comparar e interpretar este fenómeno Ciberdelincuencial. En cuanto al método Inductivo, tal como lo señala Carlos Manuel Villabella Armengol en su obra *La investigación y comunicación científica en la ciencia jurídica*, el método inductivo permite estudiar el fenómeno a partir de lo particular hacia lo general. Por su parte el proceso de Deducción, nos permitió estudiar este fenómeno social de lo general a lo particular; este método nos brindó la posibilidad de abordar el fenómeno de lo desconocido a partir de lo conocido.

Este trabajo podemos clasificarlo como una investigación documental o teórica, puesto que nos basamos en la recopilación de datos de fuentes documentales para la realización de esta investigación, se hizo necesario consultar: Las Constituciones Nacionales, Los Convenios Internacionales como lo fue el convenio de Budapest, el cual ha sido tomado como instrumento marco por otros países para la creación de sus normativas jurídicas internos; y finalmente los instrumentos jurídicos interno de Costa Rica, El Salvador y Nicaragua que regulan y sancionan el comportamiento ciberdelincuencial por medio de leyes especiales.

Asimismo, fue necesario citar las obras publicadas por juristas expertos en la materia, pudiendo mencionar a los autores Julio Téllez Valdés quien a través de su libro *El Derecho Informático*, nos brindó conocimientos especializados sobre el fenómeno ciberdelincuencial, de la misma manera nos auxiliamos de las obras jurídicas de Santiago Acurio Del Pino, Dotty Boen Oeklers y Santiago Muñoz Machado, entre otros; quienes con su aporte científico, complementaron este trabajo investigativo.

Finalmente, se obtuvieron datos de artículos, enciclopedias, notas de prensas y diccionarios; sin dejar de un lado el uso de medios digitales tales como: revistas, documentos y artículos periodísticos.

El presente trabajo investigativo se encuentra estructurado en tres capítulos:

En el primer capítulo denominada: Las Generalidades de la Ciberdelincuencia, se abordan los conceptos y nociones fundamentales que permitirá al lector ilustrarse en la idea que se quiere desarrollar en los capítulos subsiguientes.

El segundo capítulo titulado: Instrumentos Jurídicos Internacionales que combaten la Ciberdelincuencia en Centroamérica, contempla los diferentes cuerpos normativos que han implementado estos Estados para hacer frente al fenómeno de la criminalidad informática.

El tercer capítulo, nombrado: Principales Retos y Dificultades que afrontan los países Centroamericanos y la Cooperación Internacional como Paradigma de Solución para combatir la Ciberdelincuencia; acá se plasman las

contrariedades que afrontan los países de Costa Rica, El Salvador y Nicaragua, para lidiar con el fenómeno delitos informáticos. Igualmente se presentan la cooperación como una herramienta indispensable con que cuentan los Estados para poder hacer frente a la problemáticas que representa la ciberdelincuencia Principales Retos y Dificultades que afrontan los países Centroamericanos y La cooperación Internacional como Paradigma de Solución para combatir la Ciberdelincuencia.

# CAPÍTULO I: GENERALIDADES DE LA CIBERDELINCUENCIA

## 1.1 Evolución histórica de la ciberdelincuencia

Fue a finales de la década de 1960 e inicios de 1970 cuando el Departamento de Defensa de los Estados Unidos comenzó a desarrollar la primera red mundial que conectaba diversos ordenadores, veinte años más tarde se desarrollaron herramientas, hardware y software, principalmente; como servidores donde establecer páginas web, navegadores, entre otros instrumentos que permitieron al público tener acceso y utilizar internet.

El Internet, gran invento del siglo XX y símbolo de la época actual, ha facilitado las relaciones sociales, y en general toda comunicación e intercambio de información, pero aún más, ha alterado de manera decisiva e irreversible nuestro modo de vivir y acercarnos a los demás.

Muchas de las actividades que hace unos años realizábamos con normalidad, como comprar o charlar, han dado un vuelco completo con la aparición de internet. Además, han aparecido nuevas formas de ocio, trabajo, comercio, publicidad, relaciones con la administración, caracterizadas por la facilidad y la rapidez, en la realización de éstas a distancia.

El proceso de integración cultural, económica y social a nivel mundial, conocido popularmente como *globalización*[1], alcanza su punto álgido en nuestros días. Este fenómeno, surgido de las postrimerías de la guerra fría, arrastra tras de sí una innumerable cantidad de logros y desavenencias.

[1] Proceso por el que las economías y mercados, con el desarrollo de las tecnologías de la comunicación, adquieren una dimensión mundial, de modo que dependen cada vez más de los mercados externos y menos de la acción reguladora de los Gobiernos; según el Diccionario de la Real Academia Española. Disponible en: http://lema.rae.es/desen/?key=globalización. Consultado: El 15/05/2016.

La globalización posee la facultad indudable de la homogeneización, progresivamente se unifican no sólo los mercados, sino también culturas, sociedades y su significación reside en la importancia de la globalización para explicar el fenómeno de evolución tecnológica.

### 1.1.1 Evolución de la Ciberdelincuencia en Costa Rica

El proceso de interconexión de Costa Rica a las grandes redes de investigación se inició en 1990 con el establecimiento en la Universidad de Costa Rica (en adelante *UCR)* del primer *nodo*[2], de *la Red BITNET*[3] en la región Centroamericana.

Tres años después, el 26 de enero de 1993, esta conexión costarricense se integró a la Red Internet. Paralelamente, con las conexiones pioneras de la UCR, se estableció la Red Nacional de Investigación de Costa Rica (en adelante *CRNET)*, una red digital que utiliza enlaces de fibra óptica para interconectar las instituciones académicas y de investigación más importantes del país, y proporcionan amplio acceso a la información y recursos computacionales del mundo.

[2] Término con el cual se identifica a cualquier computadora conectada a la Internet. En informática y en telecomunicación, de forma muy general, un nodo es un punto de intersección, conexión o unión de varios elementos que confluyen en el mismo lugar. Ahora bien, dentro de la informática la palabra nodo puede referirse a conceptos diferentes según el ámbito en el que nos movamos: En redes de computadoras cada una de las máquinas es un nodo, y si la red es Internet, cada servidor constituye también un nodo. En estructuras de datos dinámicas un nodo es un registro que contiene un dato de interés y al menos un puntero para referenciar (apuntar) a otro nodo. Si la estructura tiene sólo un puntero, la única estructura que se puede construir con él es una lista, si el nodo tiene más de un puntero ya se pueden construir estructuras más complejas como árboles o grafos. Disponible en: https://prezi.com/ibzhvl-qmtfe/definicion-de-nodo-protocolo-tcpip/. Consultado: El 18/05/2016.

[3] En sus siglas en ingles se conoce como: Because It's Time NETwor, (Red Porque ya es Hora). Antigua red internacional de computadores de centros de docentes que ofrecía correo electrónico y transferencia de archivos, usada principalmente para divulgar avances en investigaciones y noticias del ámbito académico, se conectaba a internet a través de una pasarela de correos electrónicos. Disponible en: http://www.alegsa.com.ar/Dic/bitnet.php. Consultado: El 19/04/2016.

Estos logros, no solo permiten la conexión instantánea de un gran número de personas con el resto del mundo, sino que introducen en el país por primera vez la tecnología inter redes a gran escala.

En 1994, Radiográfica Costarricense S.A. (*RACSA*), realizó las inversiones necesarias para responder a las necesidades del mercado en el acceso a este servicio para el sector comercial, que ofrece también servicios a particulares. A principios de julio 1995 entró en operación un dominio de Internet del sector gobierno que interconectó en su primera fase a 12 ministerios.

En cuanto al número de internautas, se afirma que en 1999, en Costa Rica la tasa de usuarios en Internet era de 2.7 usuarios por cada cien mil habitantes. En el 2001 esa tasa se duplicó lo que muestra una tendencia importante al aumento de personas conectadas a Internet. Desde su inicio de operación a la fecha, el crecimiento del servicio Internet en Costa Rica ha experimentado un crecimiento constante de más del 10% anual.

Años posteriores la población empieza a realizar una serie de denuncias referentes a delitos cometidos, valiéndose de tarjetas de crédito y cajeros automáticos, estas fueron interpuestas ante el Ministerio Público, el cual ante la inexistencia de tipos penales específicos intenta de manera poco exitosa, además contraria al principio *Nullum crimen, nulla poena sine previa lege (No hay crimen, no hay pena sin previa ley)* hacer pasar estos actos como estafas o hurtos. Tales denuncias van en aumento, costando el desembolso de altas sumas de dinero en protección por parte de los ciudadanos, bancos y empresas.

De lo anterior podemos decir que la utilización de programas *anti phising*[4] así como de software antivirus es una imperante necesidad, pues el tráfico en la red, ya sea, para fines de entretenimiento, sociales, negocios o académicos, es un riesgo que debe ser contrarrestado.

### 1.1.2 Evolución de la Ciberdelincuencia en El Salvador

Costa Rica fue el primer país centroamericano en conectarse a Internet, en 1993 y ante ello, unos meses más tarde El Salvador también daría un paso adelante para seguir dicho ejemplo.

En El Salvador existía una empresa estatal que era encargada de la telefonía, la cual era llamada ANTEL (Asociación Nacional de Telecomunicaciones). Esta institución era la encargada de mantener la telefonía en el país, sin embargo los recursos que se necesitaban hacían que las conexiones crecieran lentamente, es por ello que en la época de principios de los años noventa; en El Salvador era difícil conseguir un número telefónico o línea telefónica, incluso eran vendidas a precios altos y para solicitarlas tardaban años en ser aprobadas.

En marzo de 1995 ANTEL comenzó a ofrecer el servicio de correo electrónico al público con la terminación "@es.com.sv". Sin embargo el envío o recepción de los correos no eran instantáneos ya que el servidor de El Salvador se conectaba cada media noche con los servidores de UUNET para sincronizar los correos entre El Salvador y Estados Unidos, por lo que para enviar o recibir un correo electrónico podían pasar hasta 24 horas.

[4] Técnica utilizada principalmente para robar información sensible, como claves bancarias o datos de tarjetas de crédito.

Las primeras instituciones en conectarse a internet teniendo enlaces dedicados en una primera fase fueron: La Universidad de El Salvador, la Universidad Centro Americana, la Universidad Don Bosco y Conacyt. Esta última fue una de las primeras en tener estos enlaces dedicados a Internet.

En la segunda fase del proyecto se lograron conectar a algunas instituciones del gobierno.

En la actualidad durante los últimos años la demanda del internet, creció aceleradamente debido a la facilidad con la cual un usuario común puede conectarse a este servicio, especialmente desde los dispositivos móviles. Los teléfonos avanzados permitieron que las personas pudieran tener internet en cualquier parte del país.

A inicios de este año 2016 la comisión de seguridad pública de la Asamblea Legislativa, acordó proponer la iniciativa para empezar esta ley que combatiera la ciberdelincuencia, el origen de la iniciativa fue luego de registrarse antecedentes de ataques cibernéticos como el ocurrido en 2012, cuando se vulneró la seguridad de la página web del Órgano Legislativo y la página oficial de Sigfrido Reyes, ex diputado y ex presidente de la Asamblea Nacional de dicho Estado.

Y así muchos casos se han dado a los órganos constitucionales y salas de desarrollo, creando y dando la apertura para la ley que mencionamos anteriormente.

### 1.1.3 Evolución de la Ciberdelincuencia en Nicaragua

El l7 de febrero de 1983 se funda la Universidad Nacional de Ingeniería (en adelante UNI) como un centro de educación superior. Ese mismo año, antes que se declarara el bloqueo económico, Icaza & Asociados, introdujo al país las primeras computadoras Compaq XT, 8086 y 8088, después optó por traer Cannon; mientras que Canadá Business, traía los acer.

En 1984, luego que se fundara, Compaq lanzó las primeras computadoras 386. Ese mismo año *HP*[5] introduce al mercado mundial las primeras impresoras láser. Entre 1985 y 1986, sistemas de *IBM*[6] son instalados en el Banco Central, Instituto Nicaragüense de Acueducto y Alcantarillado (INAA), Casa Pellas y el Ingenio San Antonio.

La entrada de esos equipos era muy tímida debido al sistema imperante de la época. Estos equipos instalados en estas empresas e instituciones fueron sustituidos hasta 1992.

Para 1989, ya se tiene conciencia que la Informática es una realidad frente a los nuevos retos que impone el desarrollo y es exigido en la mayoría de las Universidades impartir la clase de Informática, teniendo trasfondo el Lenguaje de Programación BASIC. Con el cambio de gobierno, hay una transformación curricular en todas las carreras universitarias y se comienza a impartir y tomar en cuenta la computación como herramienta esencial para el desarrollo humano del profesional.

[5] Acrónimo de los Apellidos de sus creadores: Bill Hewlett y David Packard. Empresa Estadounidense de las mayores empresas de tecnologías de la información del mundo, fabricaban y comercializaban Hardware y Software, además de brindar servicios de asistencia relacionados con la informática.

[6] Reconocida empresa multinacional estadounidense de tecnología y consultoría, que fabrica y comercializa hardware y software para computadores; ofrece servicios de infraestructura para internet.

Se comenzaron a conectar varias universidades al nodo Nicarao y en fin el despegue tecnológico en Nicaragua es irreversible, pero los frutos son vistos hasta cinco años después, cuando egresan los primeros profesionales con nuevos pensum académicos, se fundan empresas que dan el servicio comercial de Internet, nacen empresas desarrolladoras de sistemas y se estrecha la competencia del mercado de computadora.

Desde el 2007 los ataques de hacker en Nicaragua son de miles y contundentes, especialistas informáticos de la UNI, reconocieron que los sistemas informáticos en Nicaragua son vulnerables a cualquier ataque directo que pueden hacer los *Hackers*[7].

En el 2011 se registra el primer ataque de hackers, realizados por quienes se hicieron llamar *anonymous*[8], el cual estuvo dirigido meramente hacia 10 Instituciones del gobierno de Nicaragua, entre ellas se encontraban: Ministerio de Hacienda y Crédito Público, Ministerio Defensa, El Instituto de Energía (INE), entre otros. Debido a eso, dichas Instituciones antes mencionadas, quedaron fuera de la red por varias horas.

Fue a partir de estos ataques que Nicaragua despertó su interés en proteger a sus ciudadanos de estas amenazas informáticas y poner límites a una delincuencia actualmente desbocada en este ámbito.

[7] Persona que utiliza su vasto conocimiento en informática para cometer delitos cibernéticos.
[8] El Hacking ético y los grupos hackitivistas anonymous y lulzsec. Anónimo o anónimos en español es un seudónimo utilizado mundialmente por diferentes grupos e individuos para realizar en su nombre acciones o publicaciones individuales o concertadas; es uno de los más famosos y revolucionarios grupos hackitivistas (Hacker + Activista = HACKITIVISMO) en el mundo, el cual cuenta con muchos usuarios en el mundo. Disponible en http://www.dsteamseguridad.com/archivos/hackconf/Anonympus_Remington.pdf. Consultado: El 22/04/2016.

El Anteproyecto de Ley sobre Delito Informáticas fue creado con el propósito de salvaguardar a los nicaragüenses de ser víctimas de los posibles ataques de los ciberdelincuentes.

### 1.2 Definiciones del comportamiento de la ciberdelincuencia

**A) Delitos informáticos:** Su primera definición fue propuesta por la *OCDE* (Organización para la Cooperación y el Desarrollo Económico), según esta constituye delitos informáticos las conductas antijurídicas, no éticas o no autorizadas que implican el procesamiento automático de datos y/o la transmisión de datos.

Por su parte el autor mexicano Julio Téllez Valdés señala que los delitos informáticos, *son actitudes contrarias a los intereses de las personas en que se tiene a las computadoras como instrumento o fin (concepto atípico) o las conductas típicas, antijurídicas y culpables en que se tiene a las computadoras como instrumento o fin (concepto típico).*[9]

**B) *Cibernética*[10]*:*** Tiene su origen en la voz griega kybernetes, "piloto" y *kybernes*[11]. Es la ciencia de la comunicación y el control.

**C) Cibercrimen:** Lo podríamos dividir en dos palabras: Ciber y Crimen. Según el diccionario de la Real Academia Española de la lengua, ciber se define como: "Prefijo utilizado ampliamente en la comunidad Internet para denominar conceptos relacionados con las redes

[9] TELLEZ VALDES, Julio 2004. Derecho Informático. Tercera edición. México: McGraw-Hill Interamericana pág. 163.
[10] Ibíd. pág. 3
[11] Concepto referido al arte de gobernar, alude a la función del cerebro con respecto a las máquinas. Disponible en: http://derechocarlosinformatica.blogspot.com/. Consultado: El 20/04/2016.

(cibercultura, ciberespacio, cibernauta, etc.). Su origen es la palabra griega kibernao, que significa pilotar una nave."

Según el diccionario de la Real Academia Española de la lengua, crimen se define como: "Delito grave". Acción indebida o reprensible.

**D) Cibercriminalidad:** Aquellos actos atentatorios de la confidencialidad, la integridad y la disponibilidad de los sistemas informáticos, de las redes y de los datos, así como el uso fraudulento de tales sistemas, redes y datos.

**E) Ciberdelitos:** Cualquier actividad delictiva en la que se utilizan como herramienta los ordenadores o que se lleva a cabo a través de la red.

**F) Sextorsión:** Es un término que designa un delito cada vez más común que consiste en la realización de un chantaje bajo la amenaza de publicar o enviar imágenes de las víctimas en actitud erótica, pornográfica o manteniendo relaciones sexuales.

**G) Phishing:** Técnica utilizada principalmente para robar información sensible. Consiste en obtener información tal como números de tarjetas de crédito, contraseñas, información de cuentas u otros datos personales por medio de engaños. Este tipo de fraude se recibe habitualmente a través de mensajes de correo electrónico o de ventanas. Consiste generalmente en la duplicación de páginas webs con el objetivo de engañar a los usuarios con el sitio suplantado, logrando la confianza de estos, razón por la cual la víctima de estos ataques no llega a sospechar aun cuando haya sufrido el perjuicio.

**H) Malware:** También llamado badware, software malicioso o software malintencionado es un tipo de *software*[12] que tiene como objetivo infiltrarse o dañar un ordenador sin el consentimiento de su propietario.

**I) Pirata informático:** Quien hace negocio con la reproducción, apropiación o distribución, con fines lucrativos, y a gran escala, de distintos medios y contenidos (software, videos, música) de los que no posee licencia o permiso de su autor, generalmente haciendo uso de un ordenador.

**J) *Hackers*:** Persona que utiliza su vasto conocimiento en informática para cometer delitos cibernéticos. Este término encuentra sus orígenes en 1959, cuando surgió un grupo de programadores con mucho talento que desarrollaron un conjunto de programas que eliminaban otros programas dentro de un mismo sistema operativo.

Hoy en día no solo están interesados en las vulneraciones de seguridad que pueda presentar un cierto sistema informático, sino también en conocer el porqué de las mismas.

**K) Sabotaje informático:** Implica que el *delincuente*[13] recupere o busca destruir el centro de cómputos en sí (las máquinas) o los programas o informaciones almacenadas en los ordenadores. Se presenta como uno

[12] Programas informáticos que hacen posible la realización de tareas específicas dentro de un computador. Es el conjunto de datos y programas que maneja el ordenador. Es la parte lógica o inmaterial de un sistema informático. Almacenados en forma de ceros y unos.

[13] Autor de una infracción, es decir, de cualquier acto previsto y castigado por la ley penal y que puede ser objeto de una investigación en este campo. Disponible en: http://www.enciclopedia-juridica.biz14.com/d/delincuente/delincuente.htm. Consultado: El 23/04/2016.

de los comportamientos más frecuentes y de mayor gravedad en el ámbito político.

**L) Piratería informática:** La piratería informática consiste en la violación ilegal del derecho de autor, son aquellas "mercaderías que lesionan el derecho de autor". La piratería es una de las modalidades de reproducción técnica (la otra es la reprografía-reproducción burda del original cuya apariencia dista mucho de la auténtica), que implica la elaboración de una copia semejante al original, con la intención de hacerla pasar por tal.

**M) Phreaking:** Es la metodología más antigua dentro de los denominados ciberdelitos, consiste en ingresar en las redes de telecomunicaciones para realizar llamadas telefónicas a larga distancia utilizando la cuenta ajena.

**N) *Black Hat Hacker*[14]*:*** Son aquellos a los que normalmente se les refiere como simple Hacker. Son identificados por no seguir ningún tipo de ética de comunidad, y por buscar a menudo el beneficio personal o económico. El Hacker negro se dedica a buscar la forma de colapsar servidores, entrar en zonas restringidas o tomar el control de sistemas y redes. Se siente orgulloso de demostrar sus habilidades y su grado de autorrealización es mayor cuanto mayor sea el impacto del perjuicio provocado.

[14] Del inglés, conocidos también como Hacker de sombrero negro; intervienen en los sistemas de una manera maliciosa. Disponible en: http://www.definicionabc.com/tecnologia/hacker-2.php. Consultado: El 23/05/2016.

**O)** ***White Hat Hacker[15]:*** Su mayor fechoría era la de dejar una tarjeta de visita informando al administrador del sistema las vulnerabilidades o fallos encontrados tras una incursión en su sistema, y/o realizando, en el peor de los casos, como únicas modificaciones, aquellas estrictamente necesarias para mantener su anonimato.

En ocasiones los Hacker Blancos, son sujetos que han formado parte de los Hacker Negros, y que han decidido cambiar sus propósitos maliciosos por el apoyo a los administradores de los sistemas de seguridad y a la lucha contra el Cibercrimen, utilizando los mismos conocimientos para luchar contra estos. Los términos Black Hat y White Hat provienen de las antiguas películas del Oeste donde los buenos llevaban sombrero blanco y los malos llevaban siempre el sombrero negro.

**P)** ***Grey Hat Hacker[16]:*** Sujetos cuya ética es ambigua, los cuales poseen conocimientos comparables a los de un Black Hat Hacker pero que sin embargo utilizan para encontrar vulnerabilidades o fallos de seguridad que posteriormente se ofrecen a solventar bajo un acuerdo económico.

**Q)** **Cracker:** Podrían incluirse dentro del grupo de los Hacker de sombrero Negro. Son considerados el grupo más agresivo y su único objetivo es,

[15] Conocidos como Hacker éticos o Hacker tradicionales; se especializan en buscar errores en sistemas informáticos, dándolos a conocer a las compañías desarrolladoras o contribuyendo a su perfeccionamiento. Disponible en http://www.definicionabc.com/tecnologia/hacker-2.php. Consultado: El 24/04/2016.

[16] Conocidos también como Hacker de sombrero Gris, es un hacker talentoso que a veces actúa ilegalmente, pero con buenas intenciones. Disponible en: https://es.wikipedia.org/wiki/Sombrero_gris. Consultado el 26/05/2016.

utilizando la expresión comúnmente usada por este colectivo, *reventar sistemas*[17] ya sean informáticos o electrónicos.

Los cracker son expertos programadores que utilizan sus conocimientos para modificar el comportamiento de sistemas y redes explotando cualquier vulnerabilidad encontrada, actuando de manera obsesiva e insaciable guiados por su afán destructivo y ególatra.

**R) Phreaker:** Colectivo enfocado mayormente al mundo de los sistemas telefónicos, incluyendo también la telefonía móvil y Voz sobre *IP*[18]. Conocen el funcionamiento de dichas tecnologías así como sus protocolos de comunicación y se dedican a alterar el comportamiento de dichos sistemas por placer y en ocasiones con fines económicos**.**

**S) Lammer**: Repudiados dentro del colectivo Hacker, son aquellos internautas que se dedican a recopilar información y ejecutar códigos maliciosos buscando el reconocimiento social como Hacker sin tener un conocimiento real del impacto de sus acciones, ni del funcionamiento del código ejecutado. En ocasiones son realmente molestos aunque sus acciones no suelen provocar grandes daños.

**T) Carders:** Este tipo de ciberdelincuentes se centran exclusivamente en el robo de identidad y en la consecución de fraudes mediante tarjetas de crédito en la Red. Podemos considerar a los Carders como la evolución

[17] Son programas destinados a la desprotección de programas comerciales para que puedan ser usados sin límites. Disponible en: https://www.vozcero.com/que-es-un-hacker/. Consultado el 03/05/2016.
[18] De la sigla en inglés Internet Protocol **o**, en nuestro idioma español, Protocolo de Internet. Se trata de un estándar que se emplea para el envío y recepción de información mediante una red que reúne paquetes conmutados. Disponible en: Diccionario informático. Consultado el 29/04/016.

natural de los tradicionales es carteristas. Una vez conseguida la información necesaria, pueden realizar transacciones y compras online encubriendo su identidad y cargando el coste a su víctima.

U) **Bucaneros:** Hacen el papel de comerciantes en la red. Se dedican a comprar y vender material ilegal obtenido por medio de otros, tales como identidades, tarjetas de control de acceso, software crackeado, etc.

### 1.2.1 Crímenes específicos

a) **El fraude informático:** Es inducir a otro a hacer o a restringirse en hacer alguna cosa de lo cual el criminal obtendrá un beneficio. Esto requiere que el criminal posea un alto nivel de técnica y por lo mismo es común en empleados de una empresa que conocen bien las redes de información de la misma y pueden ingresar a ella para alterar datos como generar información falsa que los beneficie, crear instrucciones y procesos no autorizados o dañar los sistemas.

b) **El hostigamiento o acoso:** Es un contenido que se dirige de manera específica a un individuo o grupo con comentarios vejatorios o insultantes a causa de su sexo, raza, religión, nacionalidad, orientación sexual, identidad etnocultural, etc.

Esto ocurre por lo general en canales de conversaciones, grupos o con el envío de correos electrónicos destinados en exclusiva a ofender. Todo comentario que sea denigrante u ofensivo es considerado como hostigamiento o acoso.

c) **Tráfico de drogas:** El narcotráfico se ha beneficiado especialmente de los avances del Internet y a través de éste promocionan y venden drogas ilegales a través de emails codificados y otros instrumentos tecnológicos.

Como el Internet facilita la comunicación de manera que la gente no se ve las caras, las mafias han ganado también su espacio en el mismo, haciendo que los posibles clientes se sientan más seguros con este tipo de contacto. Además, el Internet posee toda la información alternativa sobre cada droga, lo que hace que el cliente busque por sí mismo la información antes de cada compra.

### 1.3 Características del comportamiento de la ciberdelincuencia

a) **La indeterminación del ámbito geográfico:** La inexistencia de fronteras reales es una de las características intrínsecas de internet, que ofrece innumerables ventajas y como no podía ser de otro modo, inconvenientes para la persecución de actividades delictivas.

En primer lugar, para iniciar cualquier política criminal, hay que conocer cuál va ser el terreno de actuación. Dicho de otra manera, saber «dónde está Internet»; estamos ante uno de los grandes problemas que existen, dada la dificultad de responder con exactitud a dicha pregunta.

b) **La facilidad de comisión:** Cometer delitos informáticos es mucho más sencillo de lo que pudiera parecer. En primer lugar requieren escasos recursos por parte del delincuente (apenas un ordenador conectado a la

Red) y como se ha visto, pueden asimismo cometerse desde cualquier lugar del mundo.

Pero además puede ser extremadamente sencillo hacerlo, hasta el punto que una persona con escasos conocimientos de informática sería hipotéticamente capaz de lograrlo.

c) **Dinamismo y descontrol:** El asunto se complica aún más por la enorme capacidad de cambio y síntesis que posee Internet. En primer lugar, avanza a gran velocidad, y constantemente se transforma y cambia. Se ha dicho incluso que no cambia, sino que aún más fluye, padeciendo un «renacimiento constante». En segundo lugar, debido a su íntima transversalidad, cualquier cambio en Internet es susceptible de afectar a las demás ramas del ordenamiento jurídico. Ello hace necesario prestar especial atención a su regulación, puesto que no se trata de un tema trivial.

La cuestión de los delitos informáticos es abordada a un nivel muy inferior al mundial, bien nacionalmente o mediante Tratados multilaterales, siendo la máxima referencia actual el conocido como «Tratado de Budapest», que sin embargo no alcanza salvo a un limitado número de países.

De ahí que podamos afirmar que la regulación de las nuevas tecnologías y en especial de Internet va a estar siempre plagada de lagunas, que se van a rellenar lentamente.

**d) Crecimiento constante y desconocimiento:** En efecto, el uso de Internet se expande a ritmo frenético, cada día llega a más hogares y cada día más personas aprenden a utilizar las nuevas tecnologías. El aumento del número de usuarios de Internet acompañado de la escasa regulación, también provoca el incremento de las posibilidades de cometer delitos, más cuanto mayor sea la ignorancia informática de los nuevos consumidores de Internet.

Además, la precariedad normativa supone un problema añadido en los países en vías de desarrollo, se crean verdaderos paraísos cibernéticos, donde incluso los propios Estados fomentan el vacío legal para atraer explotaciones que en otros países serían ilícitas.

A su vez, el crecimiento constante no hace sino sumarse al problema anterior del exacerbado dinamismo de la Red, lo que dificulta la realización de políticas concretas, que se ven rápidamente superadas por los nuevos problemas que se presentan.

Todo ello, unido a la poca importancia que se presta a la educación en las nuevas tecnologías de la información, especialmente en los adultos, convierte a los ignaros informáticos en un blanco muy fácil para los delincuentes.

## 1.4 Clasificación de los ciberdelitos

### 1.4.1 Por la tipología de la comisión de delitos

La criminalidad informática incluye una amplia variedad de categorías de crímenes. Generalmente este puede ser dividido en dos grupos:

**a)** Crímenes que tienen como objetivo redes de computadoras, por ejemplo, con la instalación de códigos, gusanos y archivos maliciosos, Spam, ataques masivos a servidores de Internet y generación de virus.

**b)** Crímenes realizados por medio de ordenadores y de Internet, por ejemplo: Espionaje, fraude, robo, pornografía infantil y pedofilia, entre otros.

### 1.4.2 Por el Convenio sobre la Ciberdelincuencia del Consejo de Europa.

Con el fin de definir un marco de referencia en el campo de las tecnologías y los delitos para la Unión Europea, en Noviembre de 2001 se firmó en Budapest el "Convenio de Ciberdelincuencia del Consejo de Europa". En este convenio se propuso una clasificación de los delitos informáticos en cuatro grupos:

#### A) Delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos

**a) Acceso ilícito:** Acceso deliberado e ilegítimo a la totalidad o a una parte de un sistema informático.

**b) Interceptación ilícita:** Interceptación deliberada e ilegítima, por medios técnicos, de datos informáticos comunicados en transmisiones no públicas efectuadas a un sistema informático, desde un sistema

informático o dentro del mismo, incluidas las emisiones electromagnéticas procedentes de un sistema informático que contenga dichos datos.

c) **Interferencia en los datos:** La comisión deliberada e ilegítima de actos que dañen, borren, deterioren, alteren o supriman datos informáticos.

d) **Interferencia en los sistemas:** La obstaculización grave, deliberada e ilegítima del funcionamiento de un sistema informático mediante la introducción, transmisión, provocación de daños, borrado, deterioro, alteración o supresión de datos informáticos.

e) **Abuso de los dispositivos:** La producción, venta, obtención para su utilización, importación, difusión u otra forma de puesta a disposición de un dispositivo, incluido un programa informático, diseñado o adaptado principalmente para la comisión de cualquiera de los delitos previstos anteriormente o una contraseña, un código de acceso o datos informáticos similares, que permitan tener acceso a la totalidad o a una parte de un sistema informático

Algunos ejemplos de este grupo de delitos son: el robo de identidades, la conexión a redes no autorizadas y la utilización de spyware y de keylogger.

**B) Delitos informáticos**

a) **Falsificación informática:** La introducción, alteración, borrado o supresión de datos informáticos que dé lugar a datos no auténticos, con la intención de que sean tenidos en cuenta o utilizados a efectos legales

como si se tratara de datos auténticos, con independencia de que los datos sean o no directamente legibles e inteligibles.

**b) Fraude informático**: Los actos deliberados e ilegítimos que causen un perjuicio patrimonial a otra persona mediante cualquier introducción, alteración, borrado o supresión de datos informáticos, o mediante cualquier interferencia en el funcionamiento de un sistema informático, con la intención fraudulenta o delictiva de obtener ilegítimamente un beneficio económico para uno mismo o para otra persona.

El borrado fraudulento de datos o la corrupción de ficheros algunos ejemplos de delitos de este tipo.

**C) Delitos relacionados con el contenido**

**a) Delitos relacionados con la pornografía infantil**.

Se entenderá por pornografía infantil a: producción, oferta, puesta a disposición, difusión, adquisición y posesión de pornografía infantil con vistas a su difusión por medio de un sistema informático o medio de almacenamiento de datos que contenga la representación visual de un menor comportándose de una forma sexualmente explícita; una persona que parezca un menor comportándose de una forma sexualmente explícita; imágenes realistas que representen a un menor comportándose de una forma sexualmente explícita. Entendiéndose por menor, a toda persona menor de dieciocho años. [19]

[19] Convenio de Ciberdelincuencia del Consejo de Europa" Arto. 9, creado 23 Noviembre de 2001,

### D) Delitos relacionados con infracciones de la propiedad intelectual y de los derechos afines

Un ejemplo de este grupo de delitos es la copia y distribución de programas informáticos, o piratería informática.

Con el fin de criminalizar los actos de racismo y xenofobia cometidos mediante sistemas informáticos, en Enero de 2008 se promulgó el "Protocolo Adicional al Convenio de Ciberdelincuencia del Consejo de Europa" que incluye, entre otros aspectos, las medidas que se deben tomar en casos de:

**a)** Difusión de material xenófobo o racista.

**b)** Insultos o amenazas con motivación racista o xenófoba.

**c)** Negociación, minimización burda, aprobación o justificación del genocidio o de crímenes contra la humanidad.

El acceso ilícito, interceptación ilegal, la interferencia de datos, la interferencia del sistema, mal uso de los dispositivos, la falsificación informática, el fraude relacionado con la informática, los delitos relacionados con la pornografía infantil y los delitos relacionados con los derechos de autor y derechos conexos, todos estos están definidos por este Convenio.

Asimismo, se exponen cuestiones de derecho procesal como la preservación expeditiva de los datos almacenados, la preservación expeditiva y divulgación parcial de los datos de tráfico, la orden de producción, la búsqueda y la incautación de datos informáticos, la recogida en tiempo real del tráfico de datos y la interceptación de datos de contenido. Además, el Convenio contiene una disposición sobre un tipo específico de acceso

transfronterizo a los datos informáticos almacenados que no requieren asistencia mutua (con consentimiento o disponibles al público) y prevé la creación de una red de 24/7 para garantizar una asistencia rápida entre las Partes Colaboradoras.

El Convenio es el resultado de cuatro años de trabajo de expertos europeos e internacionales. Se complementa con un Protocolo Adicional que realiza cualquier publicación de la propaganda racista y xenófoba a través de redes informáticas como una ofensa criminal. En la actualidad, el terrorismo cibernético también se estudia en el marco del Convenio.

### 1.4.3 Por la Organización de Naciones Unidas

La ONU reconoce los siguientes tipos de delitos informáticos:

**A.- Fraudes cometidos mediante manipulación de computadoras**

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

b) **La manipulación de programas**. Es muy difícil de descubrir y a menudo pasa inadvertida debido a que el delincuente debe tener conocimientos técnicos concretos de informática. Este delito consiste en modificar los programas existentes en el sistema de computadoras o en insertar nuevos programas o nuevas rutinas. Un método común

utilizado por las personas que tienen conocimientos especializados en programación informática es el denominado Caballo de Troya, que consiste en insertar instrucciones de computadora de forma encubierta en un programa informático para que pueda realizar una función no autorizada al mismo tiempo que su función normal.

c) **Manipulación de los datos de salida**. Se efectúa fijando un objetivo al funcionamiento del sistema informático. El ejemplo más común es el fraude de que se hace objeto a los cajeros automáticos mediante la falsificación de instrucciones para la computadora en la fase de adquisición de datos. Tradicionalmente esos fraudes se hacían a base de tarjetas bancarias robadas, sin embargo, en la actualidad se usan ampliamente el equipo y programas de computadora especializados para codificar información electrónica falsificada en las bandas magnéticas de las tarjetas bancarias y de las tarjetas de crédito.

## B.- Fraude efectuado por manipulación informática que aprovecha las repeticiones automáticas de los procesos de cómputo

Es una técnica especializada que se denomina "técnica de salchichón" en la que "rodajas muy finas" apenas perceptibles, de transacciones financieras, se van sacando repetidamente de una cuenta y se transfieren a otra.

### C.- Falsificaciones informáticas

**a) Como objeto.** Cuando se alteran datos de los documentos almacenados en forma computarizada.

**b) Como instrumento.** Las computadoras pueden utilizarse también para efectuar falsificaciones de documentos de uso comercial. Cuando empezó a disponerse de fotocopiadoras computarizadas en color a base de rayos láser, surgió una nueva generación de falsificaciones o alteraciones fraudulentas. Estas fotocopiadoras pueden hacer copias de alta resolución, pueden modificar documentos e incluso pueden crear documentos falsos sin tener que recurrir a un original, y los documentos que producen son de tal calidad que sólo un experto puede diferenciarlos de los documentos auténticos.

## 1.5 Elementos de los Delitos Informáticos

En el derecho penal, la ejecución de la conducta punible supone la existencia de dos sujetos, un sujeto activo y otro pasivo. Estos, a su vez, pueden ser una o varias personas naturales o jurídicas. De esta manera, el bien jurídico protegido será en definitiva al elemento localizador de los sujetos y de su posición frente al delito.

El delito de daños informáticos se configura como un delito común, por lo que el sujeto del mismo puede ser cualquier persona física o jurídica, siempre que no sean los titulares de los datos, programas informáticos, documentos electrónicos o sistemas informáticos ya que rige la necesidad de ajenidad a los mismos.

### 1.5.1 El sujeto activo

El sujeto activo del delito, lo constituye la persona física que con su conducta produce el resultado lesivo para el pasivo, lesionando o poniendo en peligro el bien jurídicamente tutelado.

Ahora bien en los delitos informáticos y electrónicos las personas que cometen los Delitos Informáticos son aquellas que poseen ciertas características que no presentan el denominador común de los delincuentes, es aquel individuo que tiene dominio del hecho, los sujetos activos tienen habilidades para el manejo de los sistemas informáticos y generalmente por su situación laboral se encuentran en lugares estratégicos donde se maneja información de carácter sensible, o bien son hábiles en el uso de los sistemas informatizados, aun cuando, en muchos de los casos, no desarrollen actividades laborales que faciliten la comisión de este tipo de delitos.[20]

#### 1.5.1.1 El sujeto activo desde el punto de vista Criminológico

Según el criminológico norteamericano Edwin Sutherland, señala que el Sujeto Activo del delito es una persona de cierto status socioeconómico, su comisión no puede explicarse por pobreza ni por mala habitación, ni por carencia de recreación, ni por baja educación, ni por poca inteligencia, ni por inestabilidad emocional, pero con conocimiento en informáticos. Sin embargo, teniendo en cuenta las características ya mencionadas de las personas que cometen los delitos informáticos, estudiosos en la materia los han catalogado

[20] CHAVARRIA, Ana Rosa y otros. Delitos informáticos. Legislación y manejo de la información en la era del conocimiento, Pág. 5. Consultado: El 12/06/2016. Disponible en: www.ictparliament.org/sites/default/files/delitosinformaticos.pdf

como *Delitos de cuello blanco*[21]. Asimismo, podemos decir, que el sujeto activo de los delitos informáticos no se determina de acuerdo al bien jurídico protegido que se lesa, como sucede en los delitos convencionales, sino de acuerdo al sujeto activo que los comete.

El delincuente tecnológico comúnmente asume una actitud de reto con los sistemas a que se enfrenta, de modo tal que considera suficientemente justificado el lucro que obtiene, como recompensa a su pericia e inteligencia.

En la ponencia titulada "Incidencia de las Nuevas Tecnologías de la Información en el Derecho Penal", celebrado hace algún tiempo en Caracas, la Profesora Española Mariluz Gutiérrez Francés refería en lo siguiente:

El computador es un factor criminógeno de primera magnitud que aporta a la conducta criminal, unas veces, un nuevo objeto (la información misma, potenciada y revaluada por los nuevos sistemas de procesamiento de datos y los programas), y otras, un nuevo instrumento: ofreciendo un inmenso abanico de técnicas y estrategias que pueden ponerse al servicio del delito, enriqueciendo el repertorio criminal. Esta acertada distinción permite precisar cuando la tecnología es medio y cuando objeto del delito.

Cuando la información se convierte en objeto de apropiación y en blanco lucrativo del delincuente, se ven afectados valiosos bienes jurídicos como la intimidad, el orden socioeconómico, la fe pública y la seguridad del estado, entre otros.

[21]TELLEZ VALDES, Julio, Op. Cit. Pág. 164

### 1.5.1.2 El sujeto activo según sus Características

Las personas que pueden cometer Delitos informáticos son aquellas que poseen ciertas características que no presentan el denominador común de los delincuentes, esto es, los sujetos activos tienen habilidades para el manejo de los sistemas informáticos y generalmente por su situación laboral se encuentran en lugares estratégicos donde se maneja información de carácter sensible, o bien son hábiles en el uso de los sistemas informatizados, aun cuando, en muchos de los casos, no desarrollen actividades laborales que faciliten la comisión de este tipo de delitos. Estas características nos remiten a:

**a)** Operadores, que se pueden poner en relación con el Sistema para modificar, agregar, eliminar, sustituir información y/o programas, copiar archivos para venderlos a competidores.

**b)** Programadores, que pueden violar o inutilizar controles protectores del programa y/o sistema; dar información a terceros ajenos a la empresa, atacar el sistema operativo, sabotear programas, modificar archivos, acceder a información confidencial.

**c)** Analistas de sistemas, que pueden solucionarse con usuarios, programadores y/u operadores para revelarles la operación de un sistema completo.

**d)** Analistas de comunicaciones, que enseñan a otras personas la forma de violar la seguridad del sistema de comunicaciones de una empresa, con fines de fraude.

**e)** Supervisores, que pueden en razón de su oficio manipular los archivos de datos y los ingresos y salidas del sistema.

**f)** Personal técnico y de servicio, que por su libertad de acceso al centro de cómputo puede dañar el sistema operativo.

**g)** Ejecutivos de la computadora, que pueden actuar en situación de colusión con otras personas.

**h)** Auditores, que pueden actuar como los anteriores.

**i)** Bibliotecarios de preparación, que pueden vender la documentación.

**j)** Bibliotecarios de operaciones, que pueden destruir información mediante errores o pueden venderla a competidores.

**k)** Personal de limpieza, mantenimiento y custodia, que pueden vender el contenido de los costos de papeles, fotocopiar documentos, sabotear el sistema.

**l)** Usuarios, que pueden modificar, omitir o agregar información con fines fraudulentos.

*"Con el tiempo se ha podido comprobar que los autores de los delitos informáticos son muy diversos y que lo que los diferencia entre sí es la naturaleza de los cometidos. De esta forma, la persona que entra en un sistema informático sin intenciones delictivas es muy diferente del empleado de una institución financiera que desvía fondos de las cuentas de sus clientes".*[22]

[22] DEL PINO, Santiago Acurio. Delitos Informáticos: Generalidades. Consultado: El 18/06/2016. Profesor del Derecho Informático de la PUCE. Pàg.15. Disponible en: <http://www.oas.org/juridico/spanish/cyb_ecu_delitos_inform.pdf>

### 1.5.2 El sujeto pasivo

*"En primer término tenemos que distinguir que sujeto pasivo o víctima del delito es el ente sobre el cual recae la conducta de acción u omisión que realiza el sujeto activo, y en el caso de los "delitos informáticos" las víctimas pueden ser individuos, instituciones crediticias, gobiernos, etcétera que usan sistemas automatizados de información, generalmente conectados a otros".*[23]

*"El sujeto pasivo, es sumamente importante para el estudio de los delitos informáticos, ya que mediante él podemos conocer los diferentes ilícitos que cometen los delincuentes informáticos, con objeto de prever las acciones antes mencionadas debido a que muchos de los delitos son descubiertos casuísticamente por el desconocimiento del modus operandi de los sujetos activos".*[24]

Dado lo anterior, "ha sido imposible conocer la verdadera magnitud de los "delitos informáticos", ya que la mayor parte de los delitos no son descubierto o no son denunciados a las autoridades responsables" y si a esto se suma la falta de leyes que protejan a las víctimas de estos delitos; la falta de preparación por parte de las autoridades para comprender, investigar y dar tratamiento jurídico adecuado a esta problemática; el temor por parte de las empresas de denunciar este tipo de ilícitos por el desprestigio que esto pudiera ocasionar a su empresa y las consecuentes pérdidas económicas.

[23]CHAVARRIA, Ana Rosa y otros. , Op. Cit. Pág.7
[24] BOEN OEKLERS, Dotty. Comercio Electrónico. Serie business. Cengage Learning Editores, 2004. Pag. 124.

Por lo anterior, se reconoce que, para conseguir una prevención efectiva de la criminalidad informática se requiere, en primer lugar, un análisis objetivo de las necesidades de protección y de las fuentes de peligro. Una protección eficaz contra la criminalidad informática presupone ante todo que las víctimas potenciales conozcan las correspondientes técnicas de manipulación, así como sus formas de encubrimiento".

### 1.5.3 Bien Jurídico Protegido

*El objeto jurídico es el bien lesionado o puesto en peligro por la conducta del sujeto activo. Jamás debe dejar de existir, ya que constituye la razón de ser del delito, y no suele estar expresamente señalado en los tipos penales.*[25]

Sin duda alguna podemos afirmar que los bienes jurídicos protegidos en la criminalidad informática, serán los mismos que se protegen en la criminalidad tradicional, ya que estamos hablando de un mismo fenómeno pero con herramientas novedosas para delinquir, ya que se les ha agregado un elemento nuevo *La informática*[26] lo que facilita la comisión pero dificulta la persecución y sanción por parte del órgano jurisdiccional competente.

Los bienes jurídicos tutelados afectados pueden ser numerosos:

**a)** Las personas.

**b)** El honor de las personas.

**c)** La intimidad de las personas.

**d)** La propiedad (de hardware o software).

[25] DEL PINO, Santiago Acurio. Op. Cit. Pág. 20

[26] Es el conjunto de Conocimientos Científicos y Métodos que permiten analizar, mejorar e implementar actualizaciones a la comunicación, envío y recepción de información a través de los ordenadores. Disponible en: http://www.mastermagazine.info/termino/5368.php Consultado: El 18/06/2016.

**e)** Los Documentos, archivos, registros, bases de datos, y toda información concerniente al que hacer propio de la Entidad.

**f)** La fe pública.

A pesar de las discrepancias doctrinales ya comentadas en torno a la existencia o no de un concepto de "delito informático", cada vez son más las voces doctrinales que en el ámbito de la delincuencia informática sostienen la necesidad de creación de una nueva categoría jurídico penal que abarque las conductas vinculadas con el hecho informático, entendiendo que no estamos sólo 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 criterio a la hora de entender cómo debe explicarse este interés y cómo debe definirse el bien jurídico penal a que pretende hacerse referencia.

En fin, podemos decir que el bien jurídico protegido en general es la información, pero está considerada en diferentes formas, ya sea como un valor económico, como un valor intrínseco de la persona, por su fluidez y tráfico jurídico, y por último, por los sistemas que la procesan o automatizan; los mismos que se equiparan a los bienes jurídicos protegidos tradicionales.

# CAPÍTULO II: INSTRUMENTOS JURIDICOS INTERNACIONALES PARA LA PERSECUSION DE LA CIBERDELINCUENCIA

## 2.1 El Convenio de Budapest desde la perspectiva Internacional

Las instituciones europeas han sido pioneras en la regulación de la Sociedad de la Información. Muestra de ello es La Convención Sobre Delitos Informáticos o Convenio de Budapest creado el 23 de noviembre del 2001, en el seno del Consejo de Ministros de Europa. Este instrumento jurídico cuenta por el momento con cuarenta y siete firmas y treinta y cinco ratificaciones, habiendo entrado en vigor en un total de treinta y un Estados.

La Convención sobre Delitos Informáticos está considerada como la normativa internacional más completa hasta la fecha, ya que establece un marco global y coherente que abarca los diversos aspectos de la ciberdelincuencia. Su regulación constituye un importante referente en la protección internacional contra la delincuencia informática. El Convenio, en definitiva, se consagra como el instrumento más poderoso en la lucha contra el Cibercrimen a nivel mundial, al no ser un instrumento exclusivamente europeo.

Es el primer tratado internacional sobre delitos cometidos a través de Internet y otras redes informáticas, que trata en particular de las infracciones de derechos de autor, fraude informático, la pornografía infantil, los delitos de odio y violaciones de seguridad de red. También contiene una serie de competencias y procedimientos, tales como la búsqueda de las redes informáticas y la interceptación legal.

Dicho convenio no define el crimen para el que busca armonización, sino que se limita enumerar nueve categorías de ofensas y exhorta a las partes signatarias, de forma imperativa, a adoptar cuantas medidas legislativas o de otra naturaleza, fueran necesarias, para prever como infracción penal, conforme a su derecho interno, aquellas infracciones contempladas en el tratado.

Su principal objetivo, que figura en el preámbulo, es aplicar una política penal común encaminada a la protección de la sociedad contra el Cibercrimen, especialmente mediante la adopción de una legislación adecuada y el fomento de la cooperación internacional.

Las nueve categorías se refieren a ocho delitos contra la propiedad y a un delito que carece de esta connotación: acceso ilícito, interceptación ilícita, atentados contra la integridad de datos, atentados contra la integridad del sistema, abuso de equipos e instrumentos técnicos, falsedad informática, estafa informática, infracciones relativas a la pornografía infantil.

Esta Convención, cuya elaboración tomó más de cuatro años, tuvo como objetivos fundamentales los siguientes:

**a)** Armonizar las leyes penales sustantivas aplicables a las conductas delictivas que tienen como escenario el entorno informático.

**b)** Proveer reglas de procedimiento penal que brinden a las autoridades nacionales competentes las facultades necesarias para la investigación y persecución de tales conductas delictivas.

**c)** Establecer un régimen dinámico y efectivo de cooperación internacional.

La estructura normativa de este novedoso instrumento jurídico internacional consta de 4 capítulos:

El capítulo I define algunos conceptos básicos, tales como: Sistema de cómputo, datos informáticos, proveedor de servicios de interconexión o almacenamiento de datos informáticos e intercambio electrónico de datos.

El capítulo II establece las medidas que deben adoptar los *Estados signatarios*[27] dentro del marco de sus legislaciones penales sustantivas (sección 1) y adjetivas (sección 2).

Por último, el capítulo III recoge los principios generales de cooperación internacional, incluyendo aspectos tales como extradición, asistencia legal mutua e intercambio de información.

La sección 1 del Capítulo II está dividida, a su vez, en cinco títulos que establecen nuevas categorías penales sobre conductas asociadas con el almacenamiento, tratamiento y transmisión ilegítima e intencional de datos a través de sistemas de cómputos (*hardware*[28]) y programas informáticos (software).

El título 1 describe dentro de los "Delitos contra la Confidencialidad, Integridad y Disponibilidad de Datos y Sistemas de Cómputo" a los siguientes actos: "Acceso ilegal", que comprende la interceptación e interferencia ilegal

[27] Estado: Unidad política superior independiente y soberana. Disponible en: http://www.wordreference.com/definicion/Estado Signatario: de signar "firmar" adj. Dicho de una persona: Que firma. Disponible en: http://www.wordreference.com/es/en/frames.aspx?es=signatario. Consultado: El 28/06/2016. De lo anterior podemos decir que Estados signatarios son aquellas unidades políticas, independientes y soberanas que firman un convenio, tratado o acuerdo.

[28] Conjunto de componente físico de lo que está hecho el equipo, es decir, las partes que se pueden observar del computador.

de datos y sistemas de cómputo, conocido también como *hacking*[29] y el "uso inapropiado de programas informáticos y sistemas de cómputo", que contempla el sabotaje y daños ocasionados a equipos informáticos, comúnmente denominado *cracking*[30].

Por su parte, el título 2 contempla los "Delitos relacionados con Sistemas de Cómputo" y los "Delitos relacionados con el Contenido de los Datos Informáticos", entre los que destacan las siguientes conductas delictivas: Alteración, supresión y eliminación de datos informáticos y fraude informático (entendiéndose como tal, todo acto ilegítimo e intencional que ocasione la pérdida de patrimonio, cometido a través de la alteración, supresión, eliminación e interferencia de datos informáticos o sistemas de cómputo).

El título 3 establece los "Delitos relacionados con el contenido de los Datos Informáticos". Dentro de esta categoría se encuentran las siguientes formas de comportamiento antisocial: Producción, ofrecimiento, distribución y posesión de Pornografía Infantil. abarca todo material pornográfico que visualmente evidencie lo siguiente: (1) Un menor de edad envuelto en conducta sexual explícita, (2) Una persona que aparente ser menor de edad

[29] Es la búsqueda permanente de conocimientos en todo lo relacionado con sistemas informáticos, sus mecanismos de seguridad, las vulnerabilidades de los mismos, la forma de aprovechar estas vulnerabilidades y los mecanismos para protegerse de aquellos que saben hacerlo. Disponible en: http://www.duiops.net/hacking/hacking-cracking.htm. Consultado: El 23/06/2016.

[30] Tiene dos definiciones, según se hable de seguridad informática o de crackeo de programas. En el caso de seguridad informática es el permanente intento de violación de seguridad de los sistemas informáticos, con fines justificados o no. En el caso de crackeo de programas la definición es la de creador de cracks, literalmente romper, que son programitas destinados a la desprotección de programas comerciales para que puedan ser usados sin límite. Disponible en: http://www.duiops.net/hacking/hacking-cracking.htm. Consultado: El 23/06/2016.

envuelta en conducta sexual explícita, (3) Imágenes realistas que representen a un menor de edad envuelto en conducta sexual explícita.

El término menor de edad hace alusión a los menores de 18 años; no obstante, la Convención admite que los Estados firmantes reconozcan un límite de edad inferior, siempre y cuando no sea menor a los 16 años.

El título 4 regula los "Delitos relacionados con la Violación de los Derechos de Autor", reconociendo la necesidad de dar validez a los acuerdos internacionales sobre esta materia, entre otros, la Convención de Berna para la Protección de Trabajos Literarios y Artísticos, el Acuerdo de la OMC sobre Aspectos de Comercio Relacionados con la Propiedad Intelectual, y el Tratado sobre Derechos de Autor de la *OMPI*[31].

Por último, el título 5 establece un régimen de responsabilidad penal para las personas jurídicas que estén involucradas en alguna de las conductas descritas en los primeros cuatro títulos. Así, en su artículo 12, la Convención señala que *"Cada Estado parte deberá adoptar las medidas legislativas que sean necesarias para asegurar que las personas jurídicas sean responsables penalmente por las actividades delictivas establecidas de conformidad con esta Convención, cometidas en su beneficio por cualquier persona natural que actúe ya sea individualmente o como parte de un órgano interno de la misma"*[32].

[31] Organización Mundial de la Propiedad Intelectual, organismos especializados de las Naciones Unidas, que plasman normas internacionales de en aras de proteger la Propiedad Intelectual. Disponible en: http://www.wipo.int/about-wipo/es/. Consultado: El 28/06/2016.
[32] Convenio de Budapest, Artículo 12.

Por otra parte, la sección 2 del capítulo II contiene las condiciones y principios que han de orientar las normas de procedimiento en materia de delitos informáticos.

En tal sentido, el artículo 15 de la Convención dispone que los Estados firmantes deberán velar por la adecuada protección de los derechos humanos a la hora de la adopción y aplicación de las normas de procedimiento penal relacionadas con los delitos informáticos.

Adicionalmente, en esta misma sección están contempladas algunas medidas judiciales concretas, a saber: (1) Medidas cautelares tendientes a la preservación de la integridad y custodia de datos informáticos; (2) Medidas tendientes a obtener la divulgación total o parcial de datos informáticos; y (3) Órdenes de búsqueda y allanamiento de datos informáticos almacenados en sistemas de cómputo; (4) Órdenes para la recolección e interceptación de datos informáticos en tiempo real.

Estas medidas u órdenes, emitidas por autoridad competente, de conformidad con las disposiciones normativas internas que adopten los Estados signatarios, podrán ser dirigidas tanto a individuos como a proveedores de servicios de interconexión informática (ISP, Internet Service Providers) que estén domiciliados o establecidos, respectivamente, dentro del territorio nacional de cada Estado.

Finalmente, la sección 3 reconoce los distintos ámbitos de competencia en los que es viable ejercer la *acción penal*[33] sobre aquellos delitos descritos en la sección 1.

En este contexto, queda establecido, salvo reserva hecha por el Estado, que tendrán competencia las autoridades nacionales en cualquiera de las siguientes circunstancias: (1) Cuando el delito sea cometido dentro del territorio del Estado; (2) Cuando el delito sea cometido a bordo de un buque con la bandera del Estado; (3) Cuando el delito sea cometido a borde de una aeronave con la bandera del Estado; y (4) Cuando el delito sea cometido por alguno de sus nacionales, si éste es punible de acuerdo con las leyes del lugar en que fue cometido, o si fue perpetrado fuera de la jurisdicción territorial del Estado.

La Convención sobre Delitos Informáticos constituye sin duda el esfuerzo internacional más importante en contra de las actividades criminales cometidas a través de medios informáticos. La misma tiene lugar en momentos en que el Internet ha dejado de ser tan solo el vehículo más idóneo para la propagación y perfeccionamiento de actos criminales bajo condiciones de anonimidad, sino que además representa el entorno más frecuentemente utilizado para la financiación de este tipo de actividades. Hoy, a pocos días de su firma, como una muestra evidente de la aplicación efectiva de sus normas sobre cooperación internacional, la actividad conjunta de autoridades policiales en países como Inglaterra y España ha permitido desmantelar un

[33] Es aquella que se origina a partir de un delito y que supone la imposición de un castigo al responsable de acuerdo a lo establecido por la ley. De esta manera, la acción penal es el punto de partida del proceso judicial. Disponible en: http://definicion.de/accion-penal/#ixzz4CuIGNbBX. Consultado: El 28/06/2016.

número considerable de células criminales dedicadas a la producción y comercialización de pornografía infantil a través del Internet.

Corresponde ahora a los países la responsabilidad de reconocer la importancia de establecer sanciones y mecanismos de investigación adecuados, que sean lo suficientemente avanzados y dinámicos como para hacer frente a este tipo de actividades delincuenciales que afectan a la raíz misma de nuestra sociedad, una sociedad que ha llegado a ser denominada por algunos como sociedad de la información.

## 2.2 La regulación jurídica de Costa Rica

La legislación costarricense entorno al desarrollo de cuerpos jurídicos que regulan al delito informático se puede catalogar como innovadora. Los primeros tipos penales informáticos fueron regulados a partir del año 2001, cuando se crearon e incluyeron en el Código Penal los delitos de violación de comunicaciones electrónicas, fraude electrónico y alteración de datos y sabotaje informático, los cuales son modificados con la nueva ley, Ley 9048 "Reforma de varios artículos y modificación de la Sección VIII, denominada delitos informáticos y conexos, del Título VII del Código Penal" aprobada el 6 de noviembre del año 2012.

Con esta ley se brinda especial protección a la niñez del "Uso doloso e irresponsable de la tecnología de la información" ya que los tipos penales existentes eran abiertos e imprecisos. Así mismo con esta legislación, se crea un instrumento jurídico para abordar nuevas situaciones que surgen a partir de la ciberdelincuencia.

Con la creación de este instrumento jurídico, Costa Rica estableció reformas y modificaciones al Código Penal, por lo cual se establecen nuevos tipos penales como:

**a)** Suplantación de identidad.

**b)** Espionaje informático.

**c)** Instalación o propagación de programas informáticos maliciosos.

**d)** Suplantación de páginas electrónicas.

**e)** Facilitación del delito informático.

**f)** Narcotráfico y crimen organizado.

**g)** Difusión de información falsa.

Con lo anterior, podemos observar que se busca no sólo la protección de personas físicas, sino también la protección de personas jurídicas.

Otra novedad de esta ley es, que las penas son más altas para las personas que sean encargadas de administrar o dar soporte a un sistema o red informática, dado su conocimiento técnico y el acceso que poseen a la información. Así mismo esta nueva normativa agrava la sanción del delito de corrupción de menores si el ofensor utiliza redes sociales (cuatro a diez años de prisión)[34], crea tipos penales para castigar la suplantación de identidad, el espionaje electrónico, la propagación de malware, falsificación de sitios web (clonación con diferente URL) y el envío de Spam.

[34] Ley 9048 "Reforma de varios artículos y modificación de la Sección VIII, denominada delitos informáticos y conexos, del Título VII del Código Penal" Artículo 167. "Corrupción". Será sancionado con pena de prisión de tres a ocho años quien mantenga o promueva la corrupción de una persona menor de edad o incapaz, con fines eróticos, pornográficos u obscenos, en exhibiciones o espectáculos públicos o privados, aunque la persona menor de edad o incapaz lo consienta. La pena será de cuatro a diez años de prisión, si el actor, utilizando las redes sociales o cualquier otro medio informático o telemático, u otro medio de comunicación, busca encuentros de carácter sexual para sí, para otro o para grupos, con una persona menor de edad o incapaz; utiliza a estas personas para promover la corrupción o las obliga a realizar actos sexuales perversos, prematuros o excesivos, aunque la víctima consienta participar en ellos o verlos ejecutar."

A continuación detallamos las primicias estipuladas en la presente ley, enmarcándonos en los artículos del código penal costarricense que ha sido modificado a partir de este novedoso instrumento jurídico:

Así, mismo se crea el tipo penal violación de datos personales sancionado con prisión de tres a seis años. Más aun la pena será de cuatro a ocho años si el responsable es el encargado de soporte, revela datos de carácter público o estén contenidos en bases públicas, la información es de un menor de edad o revele datos sobre ideología, religión, creencias, salud, origen racial o preferencia sexual.

En el art 196 donde se nos habla sobre "Violación de correspondencia o comunicaciones**"** se unifica el tipo penal de violación de correspondencia y comunicaciones sancionando con prisión de tres a seis años a quien "con peligro o daño para la intimidad o privacidad de un tercero y sin su consentimiento" le intercepte o se apodere de comunicaciones dirigidas a otra persona. La pena se agrava de cuatro a ocho años si las conductas son realizadas por la persona encargada de la salvaguarda de las comunicaciones o soporte técnico.

En cuanto al Art. 214. Se aumenta la pena por el delito de extorsión de cuatro a ocho años, agravándola si se realiza por medios informáticos con pena de cinco a diez años.

Así mismo en el Art. 217. Ya no será "fraude informático" sino "estafa informática". Aumenta el mínimo y reduce el máximo de prisión dejándolo entre tres y seis años (anteriormente era de uno a diez años). Si la conducta es

cometida contra un sistema de información público, bancario o financiero la pena será de cinco a diez años de prisión.

Así mismo, en el Art 229 se regulan conductas criminales como el sabotaje informático que sanciona el art 229 del código penal costarricense en el cual se sanciona con pena de tres a seis años al que "destruya, altere, entorpezca o inutilice" información de medios digitales y agrava la pena cuando el daño produzca "peligro colectivo o daño social", realizado por el encargado de soporte o la información sea de carácter público.

En el Art 229 se establece que la Prisión será de uno a tres años al que destruya información digital ajena y sin permiso, y de tres a seis años de prisión si la información es irrecuperable. Y se crea un sexto inciso para el daño agravado cuando recae sobre medios informáticos

En cuanto al Art. 288. Se aumenta la pena de espionaje de cuatro a ocho años y extiende el tipo penal a la obtención de secretos que afecten la lucha contra el narcotráfico y crimen organizado. Además adiciona un párrafo agravando la sanción de cinco a diez años si el delito es cometido por medios informáticos.

Del mismo modo se contemplan los nuevos tipos penales, creados e incorporados en esta nueva ley que rolan del Artículo 230 al 236.

En el artículo 230 está contemplada la creación del tipo penal de suplantación de identidad en redes sociales, correos electrónicos, etc. Estos delitos están sancionados con una pena de tres a seis años de prisión. Pero si la

conducta es en perjuicio de un menor de edad o incapaz, en este caso la sanción será aumentada de cuatro a ocho años de prisión.

Así mismo en el artículo 231 se plasma el tipo penal "Espionaje informático", este delito informático tiene una sanción de tres a seis años al que se apodere o bloquee por medios informáticos información para el "tráfico económico" de la industria y el comercio.

Referente a la Instalación o propagación de programas informáticos maliciosos, contemplado en el artículo 232, se sanciona con prisión de uno a seis años a quien induzca a error a otra persona para que instale programa maliciosos, a quien instale programas con el fin de convertirlos en maliciosos como sitios de internet atacantes, quien distribuya programas para creación de software malicioso, a quien ofrezca, contrate o brinde servicios de denegación de servicios, envío de comunicaciones masivas no solicitadas o programas informáticos maliciosos.

En el caso que el programa malicioso afecte entidades bancarias, obtenga el control a distancia de un sistema para formar parte de una red zombi, busque beneficios patrimoniales, afecte sistemas informáticos de salud y pongan en peligro la salud o vida de las personas y tenga la capacidad de reproducirse sin la necesidad de intervención adicional por parte del usuario legítimo del sistema informático, este delito será sancionado con la pena de tres a nueve años

En cuanto al delito de Suplantación de páginas electrónicas, contenido en el artículo 233, se impone la sanción de uno a tres años a quien suplante sitios legítimos en internet, pero si en un dado caso, mediante el engaño se capture información, acá la pena será de tres a seis años de prisión.

En el artículo 234 los legisladores incorporan la figura de Facilitación del delito informático, este delito está sancionando con pena de uno a cuatro años de prisión a quien facilite los medios para la comisión del ilícito.

En el artículo 235, está contenida la regularización del delito Narcotráfico y crimen organizado. En este se duplica la pena cuando cualquiera de los delitos cometidos por medios informáticos afecte la lucha contra el narcotráfico o el crimen organizado.

Por último el artículo 236, hace mención sobre la Difusión de información falsa, esta se encuentra sancionada con pena de tres a seis años a quien utilice medios electrónicos para propagar información falsa que distorsione o cause perjuicio a la seguridad del sistema financiero o sus usuarios.

## 2.3 La regulación jurídica de El Salvador

El Salvador en materia de delitos informáticos está avanzando en cuanto a su cuerpo legislativo reglamentaria, puesto que el pasado 26 de Febrero del 2016 dio un paso importante en esta materia aprobando la Ley 260 ¨Ley Especial Contra los Delitos Informáticos y conexos¨.

Esta ley se inspira en el reconocimiento de la persona humana como el origen y el fin de la actividad del Estado, quien como garante de justicia, seguridad jurídica y bien común, debe brindar especial protección a sus ciudadanos, debido a la diversidad de actividades delincuenciales que pueden cometerse a través de las Tecnologías de la Información y la Comunicación cuyo daño representa severas repercusiones en materia de política, economía y el desarrollo tecnológico.

Dichos comportamientos criminales se encontraban anteriormente regulados de forma dispersa en diferentes instrumentos jurídicos tales como: Decreto Nº 1030 Código Penal, El Salvador, Decreto Nº 534, Ley de Acceso a la Información Pública y Decreto Nº 133, Ley de Firma Electrónica, entre otras. Las cuales no eran suficientes para brindar la protección necesaria y eficaz, generándose cierta impunidad para quienes cometen estos tipos de delitos; en consecuencia, resultó necesario la adopción de mecanismos suficientes para facilitar su detección, investigación y sanción de estos nuevos tipos de delitos.

La ley tiene por objeto *"proteger los bienes jurídicos de aquellas conductas delictivas cometidas por medio de las Tecnologías de la Información y la Comunicación, así como la prevención y sanción de los delitos cometidos en perjuicio de los datos almacenados, procesados o transferidos; los sistemas, su infraestructura o cualquiera de sus componentes, o los cometidos mediante el uso de dichas tecnologías que afecten intereses asociados a la identidad, intimidad e imagen de las personas*

*naturales o jurídicas en los términos aplicables y previstos en la presente Ley"*[35].

Así mismo se tutelan bienes jurídicos como: la información que garantice y proteja el ejercicio de derechos fundamentales como la intimidad, honor, integridad sexual, propiedad, propiedad intelectual, seguridad pública, entre otros;[36]

**A) La Intimidad:** *"Viene del latín intus que da idea de algo interior, algo recóndito, profundo del ser y por lo mismo oculto, escondido, de manera tal que podemos decir que se trata de un ámbito individual de existencia personal, en el cual el sujeto decide su forma de ser y estar, de verse él mismo, para gozar de su soledad o convivencia tranquila a fin de encontrarse en aptitud de reflexionar, analizar, pensar, crear, trabajar, amar, soñar, en fin, para sentirse anímicamente dueño de si y mantener su libertad como suprema aspiración humana"* [37].

**B) Honor:** *"El honor es la valoración que las personas hacen de la personalidad ético-social de un sujeto y comprende las representaciones que la persona tiene de sí misma, que se identifica con la buena reputación y la fama. El honor es el bien jurídico constituido por las proyecciones psíquicas del sentimiento de estimación que la persona tiene de sí misma, atendiendo a lo*

[35] Decreto Nº 260, Ley Especial Contra Los Delitos Informáticos y Conexos, Artículo 1.
[36] Ley especial contra los delitos informáticos y conexos, artículo 3 inciso b.
[37] Disponible en: http://bibliohistorico.juridicas.unam.mx/libros/5/2253/9.pdf, Consultado el 08/07/2016.

*que la colectividad en que actúa considera como sentimiento estimable"*[38].

**C) Integridad Sexual:** "*El concepto de integridad, que deriva del término de origen latino integritas, hace hincapié en la particularidad de íntegro y a la condición pura de las vírgenes. Algo íntegro es una cosa que posee todas sus partes intactas o, dicho de una persona, hace referencia a un individuo correcto, educado, atento, probo e intachable*[39]*. Y La sexualidad es el conjunto de las condiciones anatómicas, fisiológicas y psicológicas que caracterizan a cada sexo. El término también hace referencia al apetito sexual (como una propensión al placer carnal) y al conjunto de los fenómenos emocionales y conductuales vinculados al sexo"*[40].

Estos conceptos nos ayudan a comprender el término de integridad sexual, puesto que tal termino es muy abstracto, por lo que podemos decir que los Estados con dicho termino pretenden proteger a las personas de ataques que conlleven o impliquen actos sexuales en contra de su voluntad y proteger a los menores de edad que por su condición de madures sean fácilmente engañados para que realicen actos sexuales cuando su consentimiento no es igual al de un adulto.

[38] Disponible en: http://www.diccionariojuridico.mx/?pag=vertermino&id=856, Consultado: El 08/07/2016.
[39] Disponible en: http://definicion.de/integridad/#ixzz4EDfAimfO, Consultado: El 11/07/2016.
[40] Disponible en: http://definicion.de/sexualidad/#ixzz4EDfSj8yI, Consultado: El 11/07/2016.

**D) Propiedad:** "*Propiedad equivale en sentido gramatical a la cualidad de una cosa. Así se habla de propiedades físicas, o de propiedades de otro tipo. En el Derecho Civil lo que interesa al tratar de la Propiedad es la forma jurídica de las facultades o poderes del Hombre sobre las cosas, la relación de pertenencia o apropiación sobre las mismas"*[41].

**E) Propiedad Intelectual:** *La propiedad intelectual (P.I.) se relaciona con las creaciones de la mente: invenciones, obras literarias y artísticas, así como símbolos, nombres e imágenes utilizados en el comercio. La legislación protege la P.I., por ejemplo, mediante las patentes, el derecho de autor y las marcas, que permiten obtener reconocimiento o ganancias por las invenciones o creaciones. Al equilibrar el interés de los innovadores y el interés público, el sistema de P.I. procura fomentar un entorno propicio para que prosperen la creatividad y la innovación*[42]. y

**F) Seguridad Pública:** *La seguridad pública implica que los ciudadanos de una misma región puedan convivir en armonía, cada uno respetando los derechos individuales del otro. El Estado es el garante de la seguridad pública y el máximo responsable a la hora de evitar las alteraciones del orden social*[43].

[41]Disponible en: http://www.diccionariojuridico.mx/?pag=vertermino&id=856, Consultado: El 11/07/2016.
[42]Disponible en: file:///I:/%C2%BFQu%C3%A9%20es%20la%20propiedad%20intelectual.htm, Consultado: El 29/06/2016.
[43] Disponible en: http://definicion.de/seguridad-publica/#ixzz4EDcTY6vd, Consultado: El 11/07/2016.

En relación a los delitos informáticos de la ley 260, Ley especial contra los delitos informáticos y conexos, se regularon nuevas conductas criminales tales como:

El acceso indebido a sistemas informáticos, este tipo penal sanciona en su artículo 4, la conducta de aquellos individuos que intencionalmente y sin autorización o excedido la autorización que se les hubiere concedido, acceda, intercepte o utilice parcial o totalmente un sistema informático que utilice las Tecnologías de la Información o la Comunicación, y será sancionada con prisión de uno a cuatro años.

En el artículo 7, se hace referencia a los daños a sistemas informáticos, el cual sanciona a quien destruya, dañe, modifique, ejecute un programa o realice cualquier acto que altere el funcionamiento o inhabilite parcial o totalmente, un sistemas informático que utilice la tecnología de la información y la comunicación o cualquiera de los componentes que las conforman, sancionado estas conductas con prisión de tres a cinco años, y reduciendo la pena a las personas que cometan tal delito, actuando de forma culposa debido a la imprudencia, negligencia o inobservancia de las normas establecidas, reduciendo la pena de uno a tres años, aunque no ocurre lo mismo con las personas que realicen tal delito en contra de componentes de sistemas informáticos que utilicen tecnologías de información y comunicación, destinados a prestaciones públicas o financieras, o que contengan información personal, confidencial y patrimonial de personas naturales y jurídicas, en tal caso es una agravante imponiéndose una pena de tres a seis años.

Mientras tanto el artículo 8, señala que la posesión de equipos o prestación de servicios para la vulneración de la seguridad, es un tipo penal novedoso por cuanto sanciona la mera tenencia con fines de comercialización, de equipos, dispositivos, programas informáticos y códigos de acceso, utilizando las tecnologías de la información y la comunicación con el propósito de vulnerar y eliminar ilegítimamente la seguridad de cualquier sistema informático estableciendo una pena de tres a cinco años de prisión.

El acoso a través de tecnologías de la información y la comunicación establecida en el artículo 27, sanciona una conducta sexual indeseada por su receptor que implique frases, señas u otras conductas inequívocas de carácter sexual, utilizando tecnologías de la información y comunicación, imponiendo una pena de cuatro a seis años.

Al hablar de estafa informática, debemos remitirnos al artículo 9 el que contempla la tecnología como la herramienta mediante la cual se comete el delito, valiéndose de alguna operación informática o artificio tecnológico o por cualquier otra acción que incida en el procedimiento de los datos del sistema o que dé como resultado información falsa, incompleta o fraudulenta, con la cual procure u obtenga un beneficio patrimonial indebido para sí o para otro, sancionando esta conducta con prisión de dos a cinco años, y se le crea una agravante con pena de cinco a ocho años si el hechor actúa en perjuicio de propiedades del Estado, sistemas bancarios y entidades financieras o cuando el autor sea un empleado que debido a sus labores tenga acceso a dicho sistema.

Mientras tanto el fraude informático que regula el artículo 10, hace hincapié al uso indebido de la tecnología para poder insertar instrucciones falsas o fraudulentas que produzcan un resultado que permita obtener un provecho para sí o para un tercero en perjuicio ajeno, sancionándose tal conducta con pena de tres a seis años.

En el caso de utilización de datos personales lo encontramos en el artículo 24, donde se sanciona el mero uso sin autorización, de datos personales por medio de sistemas informáticos, violando sistemas de confidencialidad y seguridad de datos, insertando o modificando los datos en perjuicio de un tercero, sancionando tal conducta con pena de cuatro a seis años y la sanción aumentaría hasta una tercera parte del máximo de la pena si el autor revela a otro, información registrada en un archivo o en banco de datos personales cuyo secreto estuviere obligado a preservar.

En el caso de los delitos informáticos contra menores de edad o personas discapacitadas contenidos en el capítulo IV de dicha ley, se incluyen sanciones al que fabrique, transfiera, difunda, distribuya, alquile, venda, ofrezca, produzca, ejecute, exhiba o muestre material pornográfico con personas de la calidad antes mencionada, sancionando también a las personas que no adviertan de forma visible el contenido del material pornográfico o sexual, castigando tales conductas con penas que oscilan como mínimo 2 años y máximo 12 años de prisión, agravándose tales penas hasta en una tercera parte del máximo establecido de la pena y la inhabilitación del ejercicio de su profesión durante el tiempo que dure la condena, si cualquiera de las acciones descritas fueran realizadas por:

**a)** Ascendientes, descendientes, hermanos, adoptantes, adoptados, cónyuges, conviviente y familiares hasta el cuarto grado de consanguinidad y segundo de afinidad;

**b)** Funcionarios, empleados públicos y municipales, autoridad púbica y agente de autoridad;

**c)** La persona encargada de la tutela, protección o vigilancia de la víctima; y

**d)** Toda persona que prevaliéndose de la superioridad originada por relaciones de confianza, doméstica, educativa, de trabajo o cualquier otra relación.

En cuanto a la revelación indebida de datos e información de carácter personal según el artículo 26, se regula la conducta de personas que 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, vídeo, texto, audio u otros, sancionando esta conducta con pena de tres a cinco años, siempre que dicho delito no se haya cometido con ánimo de lucro, la comisión de otro delito o sea material sexual explícito en perjuicio de un tercero, porque la pena será de cuatro a ocho años y agravándose más esta pena si la conducta delictiva recae sobre datos confidenciales o sensibles definidos en la Ley de Acceso a la Información Publica poniendo como límite máximo los ocho años de la pena anterior, indicando que esta pena se puede aumentar hasta una tercera parte, tal

conducta también es conocida en legislaciones de materia de derecho comparado y derecho internacional como acciones de tipo revenge porn[44].

En el artículo 22 también se establecen sanciones con penas de tres a cinco años a quienes suplanten o se apodere de la identidad de una persona natural o jurídica a través de tecnologías de la información, y la pena se incrementa hasta los ocho años si esa conducta se: daña, extorsiona, defrauda, injuria o amenaza para ocasionar perjuicio u obtener beneficios para sí mismo o terceros.

Además las sanciones previstas en la presente Ley, serán aplicables sin perjuicio de otras responsabilidades penales, civiles o administrativas, como lo establece el artículo 35 de dicha ley.

En dicha ley, el poder legislativo trata de no dejar vacío alguno en el ámbito de aplicación de la misma, indicando en el artículo número 2 de la ley, que los hechos punibles realizados total o parcialmente dentro del territorio salvadoreño, también se aplicara si el hecho inició fuera de dicho territorio pero se consumó dentro de él o en los que se utilizó infraestructura tecnológica salvadoreña, por ejemplo redes informáticas o servidores.

También se aplicará en aquellos casos en que las víctimas sean ciudadanos salvadoreños o se afecten bienes jurídicos del Estado salvadoreño.

[44]El término “revenge porn” fue acuñado por primera vez en los Estados Unidos. Consiste en la publicación no autorizada de imágenes o videos privados, generalmente conteniendo imágenes íntimas, que una persona (la ex pareja) publica por venganza. De allí el termino Revenge porn.

## 2.4 La regulación jurídica de Nicaragua

Nicaragua en materia de regulación de Delitos informáticos no ha desarrollado una estrategia o política de seguridad cibernética nacional concreta, que brinde seguridad de forma eficaz a sus gobernados que hacen uso de esta nueva herramienta tecnológica, ya que los instrumentos jurídicos que regulan algunas de estas conductas se encuentran dispersos en distintas leyes entre las cuales podemos mencionar: Constitución Política de Nicaragua,

Ley 641 Código Penal de la Republica de Nicaragua y Ley 831 Ley que reforma la Ley número 49, Ley de amparo que contiene el recurso de Habeas Data. Lo que impiden que las víctimas de delitos informáticos sepan que instrumento jurídico debe invocarse cuando están frente a este tipo de hechos (Delitos Informáticos).

Si bien es cierto que Nicaragua no cuenta con un instrumento jurídico especializado que de tratamiento a la delincuencia informática, esto no quiere decir que algunos tipos penales o bien algunas conductas criminales no se prevengan o sancionen. Puesto que, como dijimos anteriormente si se previenen en diversos cuerpos normativos. Actualmente Nicaragua cuenta con una propuesta de Ley de Delitos informáticos, el cual es resultado del esfuerzo de nuestros legisladores por encaminar el derecho interno nicaragüense hacia la actualización y modernización de las leyes penales para poder combatir de forma efectiva la Cibercriminalidad, y evitar que estos hechos delictivos queden en la impunidad, y así poder hacer frente al problema de la Cibercriminalidad.

## CONSTITUCIÓN POLITICA

Nuestra Constitución Política Nicaragüense, es la norma suprema del ordenamiento jurídico, ninguna ley o norma jurídica de categoría inferior puede contradecir lo contemplado, en ella se brinda protección por parte del Estado frente a las diferentes situaciones jurídicas que puedan darse en el ámbito social.

En nuestra Carta Magna, se destaca la protección jurídica que brinda en el título IV referido a los deberes y garantías del pueblo nicaragüense, capítulo I de los derechos individuales. En los artículos 25 y 26 de nuestra constitución política se contempla la existencia de derechos individuales fundamentales que pueden resultar vulnerados con la comisión de los delitos informáticos, entre los cuales están: Derechos a la seguridad, Privacidad, Respeto a la Honra y la Reputación, como también el respeto a la libertad individual y a la seguridad.

Así mismo, se establece la protección a la privacidad e intimidad que debe gozar todas las personas del pueblo nicaragüense y al debido respeto que se debe mantener ante el domicilio, correspondencia y comunicaciones de cualquier ciudadano. También se hace mención acerca de que las personas deben conocer la información registradas por las autoridades y el porqué de ellas, el Estado debe proteger los datos contenidos en esas bases de información.

Es necesario mencionar la libertad de expresión que tienen los ciudadanos *"Nicaragüenses a expresar libremente su pensamiento en público o en privado, individual o colectivamente, en forma oral, escrita o por cualquier otro medio"*[45].

## CÓDIGO PENAL

Los códigos en general reconocen derechos propios de las personas, pero el código penal, no los declara, solo los defiende, es por ello que cuando hablamos de materia penal no hablamos de derechos, sino de delitos.

El Código Penal de la República de Nicaragua, Ley No. 641 publicada en la Gaceta No. 232 del 03 de diciembre del 2007, es un conjunto de normas jurídicas que tipifican conductas mediante la aplicación de penas, en beneficio del orden jurídico, protección social y del bien común, debe regular todas y cada una de las acciones u omisiones que sean consideradas delictivas.

Nuestro Código Penal regula algunos delitos convencionales que también pueden cometerse a través del uso del internet como:

**Acoso Sexual**, el cual sanciona a "quien de forma reiterada o valiéndose de su posición de poder, autoridad o superioridad demande, solicite para sí o para un tercero, cualquier acto sexual a cambio de promesas, explícitas o quien implícitas, de un trato preferencial, o de amenazas relativas a la actual o futura situación de la víctima, será penado con prisión de uno a tres años"[46]

[45] Constitución Política de Nicaragua, Artículo 30.
[46] Ley No. 641, Código Penal Articulo 174, publicada en la Gaceta No. 232 del 03 de diciembre del 2007.

**Amenazas**: Este tipo penal sanciona a "*Quien amenace a otro con causarle a él, a su familia o a otras personas con las que esté íntimamente vinculado, un mal que constituya delito y que por su naturaleza parezca verosímil, será sancionado con pena de prisión de seis meses a un año.*"[47]

**Chantaje:** *"El que con amenazas de imputaciones contra el honor o el prestigio, violación o divulgación de secretos, con perjuicio en uno u otro caso para el ofendido, su familia o la entidad que represente o en que tenga interés, obligue a otro a hacer o no hacer algo, será sancionado con prisión de dos a cuatro años y de cien a doscientos días multa."* [48]

**Propalación:** "*Quien hallándose legítimamente en posesión de una comunicación, de documentos o grabaciones de carácter privado, los haga públicos sin la debida autorización, aunque le hayan sido dirigidos, será penado de sesenta a ciento ochenta días multa."* [49]

**Calumnia:** "*El que impute falsamente a otro la comisión o participación en un delito concreto, será sancionado con pena de cien a doscientos días multa. Si la calumnia se propagara con publicidad, será sancionado con pena de ciento veinte a trescientos días multa."* [50]

**Injuria:** "*Quien mediante expresión o acción, lesione la dignidad de otra persona menoscabando su fama, imagen, reputación, honor o atentando*

[47] Código Penal Artículo 184.
[48] Código Penal Artículo 185.
[49] Código Penal Articulo 195
[50] Código Penal Artículo 202.

*contra su propia estima, será sancionado con pena de cien a doscientos días multa."* [51]

**Estafa:** *"Quien con el propósito de obtener un provecho ilícito, para sí o para un tercero, mediante ardid o engaño, induzca o mantenga en error a otra persona para que realice una disposición total o parcial sobre el patrimonio propio o ajeno, siempre que el valor del perjuicio patrimonial exceda la suma equivalente a dos salarios mínimos mensuales del sector industrial, será penado con prisión de uno a cuatro años y de noventa a trescientos días multa".* [52]

**Exhibicionismo:** *"Quien se muestre desnudo o exhiba sus órganos genitales en lugares públicos, será sancionado de diez a treinta días multa, o trabajo en beneficio de la comunidad de diez a treinta jornadas de dos horas diarias."* [53]

Así mismo, nuestro Código Penal regula tan solo en seis artículos determinadas conductas ciberdelincuenciales propiamente dicha. Lo que representa un obstáculo para la persecución de tipos penales como: El Spam, phreaking y terrorismo virtual, entre otros, que no están previsto y consiguiente no se sancionan.

Los delitos de naturaleza informática que regula la ley 641 son:

En lo que se refiere al artículo 175, "Explotación sexual, pornografía y acto sexual con adolescentes mediante pago, se sanciona a quien induzca, facilite, promueva o utilice con fines sexuales o eróticos a personas menor de

[51] Código Penal Artículo 203.
[52] Código Penal Artículo 229.
[53] Código Penal Artículo 540.

dieciséis años o discapacitado, haciéndola presenciar o participar en un comportamiento o espectáculo público o privado, aunque la víctima consienta en presenciar ese comportamiento o participar en él, será penado de cinco a siete años de prisión y se impondrá de cuatro a seis años de prisión, cuando la víctima sea mayor de dieciséis y menor de dieciocho años de edad.

Así mismo se sanciona a quien promueva, financie, fabrique, reproduzca, publique, comercialice, importe, exporte, difunda, distribuya material para fines de explotación sexual, por cualquier medio sea directo, mecánico, digital, audio visual, o con soporte informático, electrónico o de otro tipo, la imagen, o la voz de persona menor de dieciocho años en actividad sexual o eróticas, reales o simuladas, explicitas e implícitas o la representación de sus genitales con fines sexuales, será sancionado con pena de prisión de cinco a siete años de prisión y de ciento cincuenta a quinientos días de multa.

En este artículo se aprecia la manera de como nuestros legisladores incluyen la novedosa modalidad de comisión de delitos informáticos, teniendo en cuenta dos elementos: la información como un bien jurídico tutelable y el internet como un medio de comisión de delito; siendo así que en dicho artículo se sanciona a quien distribuya material pornográfico a través de soporte informático o medios electrónico.

En cuanto al artículo 198, el acceso y uso no autorizado de información, se sanciona a quienes sin la debida autorización, utilice los registros informáticos de otro, o ingrese, por cualquier medio, a su banco de datos o archivos electrónicos, otorgando pena de prisión de uno a dos años, y de doscientos a quinientos días multa.

Así mismo en el artículo199, agravación por Abuso de Función o Cargo, este articulado a como el propio nombre lo expresa, se considera como un agravante el hecho que alguna autoridad, funcionario o empleado público que fuera de los casos autorizados por la ley y prevaliéndose de su cargo o función realice cualquiera de las conductas como: Apertura o interceptación ilegal de comunicaciones, Sustracción, desvío o destrucción de comunicaciones, Captación indebida de comunicaciones ajenas entre otra.

Serán castigados pena de tres a seis años de prisión e inhabilitación para ejercer el cargo o empleo público por el mismo período.

El artículo 245, hace referencia a la destrucción de registros informáticos, que penaliza con prisión de uno a dos años o de noventa a trescientos días multa a quienes destruyan, borren o de cualquier modo inutilice registros informáticos; esta acción se agrava cuando la información que se destruya trate sea necesaria para la prestación de un servicio público o se trate de un registro oficial. Elevándose la pena de tres a cinco años.

Por su parte el artículo 246, hace referencia al uso de programas destructivos, el cual es uno de los delitos de informáticos más frecuentes, que provocan grandes daño. Por tal razón se sanciona quien, con la intención de producir un daño, adquiera, distribuya o ponga en circulación programas o instrucciones informáticas destructivas, que puedan causar perjuicio a los registros, programas o a los equipos de computación, será penado con prisión de uno a tres años y de trescientos a quinientos días multa.

Por último el artículo 250, titulado: La protección de programas de computación, es uno de los tipos penales de naturaleza meramente informática, que sanciona de trescientos a quinientos días multa o prisión de uno a tres años e inhabilitación especial por el mismo período para ejercer cargo, profesión, oficio, industria o comercio relacionado con la conducta delictiva, a quienes contraviniendo la ley fabrique, distribuya o venda mecanismos o sistemas que permitan o faciliten la supresión no autorizada de dispositivos técnicos que se hayan utilizado para evitar la reproducción de programas de computación.

## HABEAS DATA

El hábeas data nace con el objeto de preservar derechos que, como consecuencia de constantes avances tecnológicos, están siendo violados a través de mecanismos que hasta la época del nacimiento de ésta nueva institución no podían ser garantizados. El hábeas data es una garantía novedosa dentro del sistema jurídico, tanto a nivel internacional como interno.

Nicaragua a través de la Ley 49 o Ley de Amparo incorpora el Recurso de Habeas Data, el cual regula el uso y acceso a la información basado en el Derecho que tienen los ciudadanos nicaragüense de saber por qué y con qué finalidad se tiene información personal; este es un derecho fundamental, inherente a la persona y que como tal los nicaragüenses tienen derecho, a su vida privada y la de su familia, a la inviolabilidad de su domicilio, su correspondencia y sus comunicaciones de todo tipo, al respeto de su honra y reputación.

Este recurso emerge como un mecanismo jurisdiccional de protección de los Derechos a la autodeterminación informativa consagrados en el artículo 26 numerales 1, 3 y 4 de la Constitución Política de la República de Nicaragua.

"Habeas Data garantiza el acceso de toda persona a la información que puede tener cualquier entidad pública sobre ella, así como el derecho a saber por qué y con qué finalidad tienen esa información"[54]. El mismo nace como imperativo frente a los problemas que se generan como consecuencia de los constantes avances tecnológicos.

Esta ley tutela los datos personales asentados en archivos, registros, bancos de datos, u otros medios técnicos, de naturaleza pública o privada, cuya publicidad constituya una invasión a la privacidad personal; el recurso de proceder a favor de toda persona para saber quién cuando, con qué fines y en qué circunstancias toma contacto con su datos personales y su publicidad indebida. "*en la ley dice que el recurso de habeas data cabe contra los responsables y cualquier otra persona que hubiere hecho uso indebido de ficheros de datos*"[55].

El órgano encargado para conocer y resolver el recurso de habeas data es la Sala de lo Constitucional de la Corte Suprema de Justicia.

[54] Ley 831, Ley de Reforma y Adiciones a la Ley 49, Ley de Amparo, Artículo 2, Publicada en la Gaceta Diario Oficial número 29, del 14 de febrero de 2013.
[55] Ley de Reforma y Adiciones a la Ley de Amparo, Artículo 5.

## LEY DE PROTECCIÓN DE DATOS PERSONALES

La Ley No. 787, fue Aprobada el 21 de Marzo del 2012 y publicada en La Gaceta del 29 de Marzo del 2012. Está inspirada en la obligación que tiene el Estado Nicaragüense de promover y garantizar el bien común, asumiendo la tarea de enfatizar el desarrollo humano protegiéndolo de todo tipo de explotación, discriminación y exclusión.

Basándose en los principios de: La libertad, la justicia y el respeto a la dignidad de la persona humana. Siendo que los nicaragüenses tienen derecho, a su vida privada y la de su familia, a la inviolabilidad de su domicilio, su correspondencia y sus comunicaciones de todo tipo, al respeto de su honra y reputación, así como a saber por qué y con qué finalidad se tiene información personal.

La Ley de Protección de Datos Personales cuenta con 56 artículos, divididos en IX capítulos.

El Capítulo I aborda generalidades, como objeto y ámbito de aplicación de la norma, entendiéndose que es la protección de datos personales, automatizados o no, de toda persona natural o jurídica, y el manejo de esta información en ficheros públicos o privados. También, encontramos algunos conceptos propios de la materia donde resaltan los siguientes:

A) **Autodeterminación Informativa**: Definiéndolo como el derecho que tiene toda persona a saber ¿quién?, ¿cuándo?, ¿con qué fines? y ¿en qué circunstancias? toman contacto con sus datos personales.

A nuestro criterio este concepto está muy reducido, pues la normativa lo ha limitado "a saber", cuando en realidad es un derecho fundamental derivado del derecho a la privacidad y por ende el individuo conserva la facultad de ejercer el control total y absoluto sobre su información personal.

**B) Bloqueo:** Entendiéndose como la identificación y conservación de datos personales una vez cumplida la finalidad para la cual fueron recabados, con el único propósito de determinar posibles responsabilidades en relación con su tratamiento, hasta el plazo de prescripción legal o contractual de éstas.

**C) El Consentimiento del titular:** Podemos entenderlo como Manifestación de voluntad, libre, inequívoca, específica e informada, mediante la cual el titular de los datos consiente el tratamiento de sus datos personales.

**D) Datos personales:** Se refiere a la información sobre una persona natural o jurídica que la identifica o la hace identificable.

**E) Datos personales informáticos:** Son aquellos datos personales tratados a través de medios electrónicos o automatizados.

**F) Datos personales sensibles:** Todos aquellos Concernientes a toda información que revele el origen racial, étnico, filiación política, credo religioso, filosófico o moral, sindical, relativo a su salud o vida sexual, antecedentes penales o faltas administrativas, económicos financieros;

así como información crediticia y financiera y cualquier otra información que pueda ser motivo de discriminación.

G) **Datos personales relativos a la salud:** Son los relativos a la salud física o mental de los pacientes que acudan a los mismos o que estén o hubieren estado bajo tratamiento de aquellos, respetando el secreto profesional.

H) **Datos personales comerciales:** Son datos sensibles de las Empresas las bases de datos de clientes, proveedores y recursos humanos, para fines de publicidad y cualquier otros datos que se consideren información comercial o empresarial reservada fundamentalmente para el libre ejercicio de sus actividades económicas.

I) **Disociación de datos:** Se refiere al mecanismo para el tratamiento de datos personales de manera que la información obtenida no pueda asociarse a persona determinada.

J) **Ficheros de datos:** Archivos, registros, bases o bancos de datos, públicos y privados, que contienen de manera organizada los datos personales, automatizados o no.

K) **Fuentes de acceso público:** Son aquellos ficheros cuya consulta puede ser realizada por cualquier persona, sin más exigencia que, el abono de una contraprestación.

**L) Responsable de ficheros de datos:** Es toda persona natural o jurídica, pública o privada, que conforme Ley decide sobre la finalidad y contenida del tratamiento de los datos personales.

**M) Tercero:** En materia de protección de datos, es considerado toda persona, pública o privada que realice a su arbitrio el tratamiento de datos personales, ya sea en ficheros de datos propios o a través de conexión con los mismos.

**N) Tratamiento de datos:** Son las operaciones y procedimientos sistemáticos, automatizados o no, que permiten la recopilación, registro, grabación, conservación, ordenación, almacenamiento, modificación, actualización, evaluación, bloqueo, destrucción, supresión, utilización y cancelación, así como la cesión de datos personales que resulten de comunicaciones, consultas, interconexiones y transferencias.

El titular de los datos deberá por sí o por medio de apoderado dar el consentimiento para la entrega de los datos. Siendo necesario otorgarlo por escrito o por otro medio idóneo, físico o electrónico. Se podrá revocar sin efecto retroactivo. No será necesario el consentimiento cuando: a) Exista orden judicial; b) Los datos personales se sometan a un procedimiento previo de disociación; c) Tenga el propósito de cumplir obligaciones derivadas de una relación jurídica entre el titular y el responsable; y d) Los datos se obtengan de fuentes de acceso público irrestricto y se trate de listados cuyos datos se limiten a nombre, documento nacional de identidad, y fecha de nacimiento.

El capítulo II habla de los responsables de los ficheros de datos. Abordando la obligación principal de informar al obtener los datos personales del titular.

Se estipula la obligación de informar previamente a los titulares de datos personales de forma expresa y clara, de los siguientes aspectos:

**a)** La finalidad para la que serán utilizados y quiénes pueden ser sus destinatarios o clase de destinatarios;

**b)** La existencia del fichero de datos electrónicos o de cualquier otro tipo, de que se trate y la identidad y domicilio de su responsable; que se le proponga;

**c)** Las consecuencias de proporcionar los datos personales, de la negativa a hacerlo o de la inexactitud de los mismos;

**d)** La garantía de ejercer por parte del titular el derecho de acceso, rectificación, modificación, supresión, complementación, inclusión, actualización y cancelación de los datos personales;

**e)** Cuando los datos procedan de fuentes accesibles al público y se utilicen para hacer envíos publicitarios o promocionales, en cada comunicación que se dirija al titular de los mismos se le informará del origen de los datos y de la identidad del responsable del tratamiento así como de los derechos que le asisten;

**f)** Que los datos sólo pueden ser utilizados para los fines que motivaron su tratamiento; y no podrán ser utilizados para otros fines;

**g)** Los datos inexactos, incompletos, o que estén en desacuerdo con la realidad de los que le corresponden a la persona, serán rectificados,

modificados, suprimidos, completados, incluidos, actualizados o cancelados según corresponda.

Con respecto a las medidas de seguridad y confidencialidad en el tratamiento de datos, al igual que en otras legislaciones, el responsable del fichero de datos debe adoptar las medidas técnicas y organizativas necesarias para garantizar la integridad, confidencialidad y seguridad de los datos personales, y evitar bajo su responsabilidad la adulteración, pérdida, consulta, tratamiento, revelación, transferencia o divulgación no autorizada, detectar desviaciones, intencionales o no, de información privada, ya sea que los riesgos provengan de la acción humana o del medio técnico utilizado.

En atención a la confidencialidad, las personas que intervengan en cualquier fase del tratamiento de datos personales están obligadas al secreto profesional respecto de los mismos. Subsistiendo aun después de finalizada su relación con el responsable del fichero de datos, pudiendo ser relevado del deber de secreto por resolución judicial y cuando medien razones fundadas relativas a la seguridad nacional, defensa nacional, seguridad pública o la salud pública.

Los datos personales se podrán ceder y transferir cuando, previo consentimiento del titular de los datos, al que se le deberá informar sobre la finalidad de la cesión e identificar al cesionario. El consentimiento para la cesión es revocable, mediante notificación por escrito o por cualquier otra vía que se le equipare, según las circunstancias, al responsable del fichero de datos. Este no podrá ser exigido cuando lo disponga una ley, se realice entre instituciones del Estado en el ejercicio de sus atribuciones, se trate de razones

de salud pública, de interés social, de seguridad nacional o se hubiere aplicado un procedimiento de disociación de datos, de modo que no se pueda atribuir a una persona determinada.

Para la cesión y transferencia de datos personales que se encuentren en ficheros de datos públicos o privados, se hará a solicitud de una persona legalmente autorizada, debiendo detallar el objeto y la finalidad que se persigue con dicha información, asegurando el responsable del fichero de datos cumplir con las medidas de seguridad y confidencialidad de los mismos.

Se debe verificar que el solicitante cumpla de igual manera con éstas medidas y sobre todo informar a la persona titular de los datos, la solicitud de transferencia y el propósito que se persigue, para su consentimiento; por ello se deben de tomar las previsiones necesarias para evitar que la información suministrada sea pasada a terceras personas. Toda esta transferencia de datos debe de contar con el aval de la Dirección de Protección de Datos Personales.

Los derechos del titular de datos, se encuentran contenidos en el capítulo III. Sobresaliendo el Derecho a solicitar información, pues el titular podrá en todo momento solicitar información a la Dirección de Protección de Datos Personales, relativa a la existencia de archivos de él en de ficheros de datos personales, sus finalidades y la identidad de sus responsables. El registro que se lleve al efecto será de consulta pública y gratuita. También podrán solicitar que se le permita rectificar, modificar, suprimir, complementar, incluir, actualizar o cancelar sus datos personales y se podrán abstener de proporcionar datos personales de carácter sensible, pero como explique

anteriormente, esto no se está cumpliendo a cabalidad, sobre todo en información financiera.

Con respecto a los ficheros y responsables de ficheros de datos personales, contemplados en el capítulo IV, es necesario aclarar que los responsables de estos deben inscribirse en el Registro de ficheros de datos que posee la Dirección de Protección de Datos Personales y esperar en el plazo de ley la resolución de su inscripción.

El registro de ficheros de datos debe recabar la siguiente información: a) Nombre y domicilio del responsable, entendiéndose como persona natural o jurídica con toda la descripción de la razón social, fecha de constitución, objeto y representante legal; b) Naturaleza de los datos personales contenidos en cada fichero de datos; c) Forma, tiempo y lugar de recolección y actualización de datos; d) Destino de los datos y personas naturales o jurídicas a las que pueden ser transmitidos; e) Modo de interrelacionar la información registrada; f) Medios utilizados para garantizar la seguridad de los datos, debiendo detallar nombre y domicilio de las personas que intervienen en la colecta y tratamiento de los datos; g) Tiempo de conservación de los datos; y h) Forma y procedimientos en que las personas pueden acceder a los ficheros de datos personales para realizar la rectificación, modificación, supresión, complementación, inclusión, actualización y cancelación de los mismos según concierna.

Él envío de publicidad y promociones, a través de medios electrónicos (sms, email, redes sociales) debe de ser normado, existiendo la posibilidad para el destinatario de expresar su negativa a recibir spot publicitarios y

promocionales de bienes y servicios o, en su caso, revocar su consentimiento de una forma clara y gratuita.

El órgano regulador de la analizada ley, es la Dirección de protección de datos personales, cuyas facultades se encuentran contenidas en el capítulo V. Está adscrita al Ministerio de Hacienda y Crédito Público, con una máxima autoridad administrativa, su función principal es el control, supervisión y protección del tratamiento de los datos personales contenidos en ficheros de datos de naturaleza pública y privada y sus funciones accesorias son:

**a)** Asesorar a las personas naturales y jurídicas que lo requieran acerca del contenido y alcance de la presente Ley. Facultad, que a mí criterio, hay que observarla detenidamente pues en un proceso administrativo puede verse afectada de parcialidad, por ser Juez y parte. Aunque la Dirección, se aleja de mí criterio, considero que en caso concreto sería oportuno un pronunciamiento de la máxima instancia que aclare esta situación.

**b)** Dictar las normas y disposiciones administrativas necesarias para la realización de su objeto en el ámbito de su competencia. Quedando siempre a salvo la vía administrativa para el agraviado que se considere que se está violentando algún derecho particular.

**c)** Dictar y vigilar que las normas sobre confidencialidad, integridad y seguridad de los datos personales se respeten y apliquen por los titulares de los ficheros de datos correspondientes.

**d)** Solicitar la información que requiera para el cumplimiento de su objeto a las entidades públicas y privadas titulares de los ficheros de datos,

garantizando en todo caso la seguridad, la integridad y confidencialidad de la información. Dicha forma se regula en el respectivo reglamento.

**e)** Imponer las sanciones administrativas que correspondan a los infractores, quedando a salvo el recurso vertical.

**f)** Formular y presentar las denuncias por violaciones a la ley, ante la autoridad correspondiente.

**g)** Verificar que los ficheros de datos personales tengan los requisitos necesarios para que proceda su inscripción en el registro correspondiente.

**h)** Acreditar a los inspectores para la supervisión y vigilancia de los responsables de los referidos ficheros.

**i)** Fomentar y promover modelos de autorregulación, siempre y cuando sea posible, como mecanismo adicional para garantizar el derecho a la autodeterminación informativa de toda persona, estos modelos buscan un valor añadido en su contenido con respecto a lo dispuesto en la ley y el reglamento.

**j)** Emitir su criterio técnico en todo proyecto de ley y reglamento que pudieran tener incidencia en la validez y garantía del derecho a la autodeterminación informativa.

**k)** Divulgar el contenido y extensión del derecho a la autodeterminación informativa a la población y al resto de los Poderes e instituciones del Estado; y

**l)** Cooperar con otras autoridades de protección de datos a nivel internacional para el cumplimiento de sus competencias y generar los mecanismos de cooperación bilateral y multilateral para asistirse entre sí y prestarse el debido auxilio mutuo cuando se requiera;

Con respecto a los Inspectores, la ley abordó un procedimiento que consiste en visitas, de verificación y control, mediante las cuales los inspectores, revisan los ficheros de datos con el objetivo de establecer el grado de cumplimiento de las normas regulatorias de esta actividad o de brindar a las autoridades de la Dirección de Protección de Datos Personales mayores elementos de juicio para la adopción de una resolución con afectación a terceros o no.

La ley las clasifica en infracciones leves y graves, entendiendo como leves: tratar datos personales sin el consentimiento expreso ya sea por escrito, por medios electrónicos, ópticos o por cualquier otra tecnología, o por signos inequívocos de su titular, cuanto la ley así lo exija; omitir la inclusión, complementación, rectificación, actualización, supresión o bloqueo, cancelación de oficio o a petición del titular, de los datos personales que se encuentran en ficheros de datos públicos y privados; incumplir las instrucciones dictadas por la Dirección; obtener datos personales a través de formularios u otros impresos, sin que figure en los mismos, en forma claramente legible, las advertencias que se utilizarán para crear ficheros; y remitir publicidad a través de medios electrónicos, a titulares que han manifestado expresamente su negativa a recibirla.

Como graves se entiende el tratamiento de datos personales por medios fraudulentos o que infrinjan la ley; impedir u obstaculizar el ejercicio del derecho a la autodeterminación informativa al titular de los datos personales, así como negar injustificadamente la información solicitada; violentar el secreto profesional; reincidir en las infracciones leves; mantener ficheros de datos, inmuebles, equipos o herramientas sin las condiciones mínimas de

seguridad, integridad y confidencialidad requeridas; y obstruir las inspecciones que realice la Dirección.

En materia administrativa operan el apercibimiento, suspensión de las operaciones relacionadas con el tratamiento de los datos personales y clausura o cancelación de los ficheros de datos personales de manera temporal o definitiva.

Es conveniente aclarar que siempre queda abierta la vía civil y penal para el titular de datos afectado por el actuar del responsable de ficheros de datos.

## ANTEPROYECTO
## DE LEY ESPECIAL SOBRE DELITOS INFORMÁTICOS

Actualmente Nicaragua cuenta con un anteproyecto de ley. Este proyecto jurídico tiene por objeto, prevenir y sancionar los delitos cometidos en contra de los sistemas informáticos integrados en equipos físicos o datos e información almacenada en archivos, registros, bases o bancos de datos automatizados. Este anteproyecto de ley tiene como ámbito de aplicación todo el territorio nacional a las personas naturales que utilizan equipos físicos con sistemas informáticos integrados.

Este proyecto de ley se estructura en tres capítulos; conteniendo el capítulo primero conceptos básicos como: Datos, Computador, Hardware, Información, Software, Sistema informático, Virus informático. Así mismo el capítulo segundo se refiere a los delitos y penas que se impondrán a quienes cometan estos delitos, en este capítulo se sancionan comportamientos criminales como: Acceso indebido de datos, Alteración de documentos, Daño

a datos o sistemas informáticos, Sabotaje informático, Fraude informático, Hurto informático, Espionaje informático, Difusión pornográfica de niños, niñas o adolescentes, Creación y distribución de virus informáticos y Violación de las comunicaciones.

En el capítulo tres de este proyecto de ley contiene las Disposiciones finales en las cuales se detallaría la vigencia de esta norma. De lo anterior podemos decir que el Estado de Nicaragua actualmente está trabajando para dar una respuesta jurídica ante el problema informático que envuelve a la sociedad nicaragüense, puesto que el Estado como garante debe garantizar las condiciones necesarias para el ejercicio de la mayor parte de los derechos fundamentales y libertades públicas del individuo.

A continuación presentamos una tabla de comparación entre los países de Costa Rica, El Salvador y Nicaragua, con respecto a las semejanzas y diferencias que hay entre estos estados, referente a la Regulación Jurídica en materia de ciberdelincuencia.

| Países | Regulación Jurídica en materia de ciberdelincuencia | Semejanzas | Diferencias |
|---|---|---|---|
| **Costa Rica** | ➢ Constitución política.<br>➢ Ley No. 4573 Código Penal.<br>➢ Ley No. 9048 de Delitos Informáticos que Reformas y modifica el Código Penal. | Los Estados consideran la ciberdelincuencia como un fenómeno social que involucra la vulneración de diversos bienes jurídicos. | Fue el pionero en regular la criminalidad informática a partir del año 2001. |
| **El Salvador** | ➢ Constitución política<br>➢ Ley No. 260 Ley de Delitos Informáticos | Estos Estados tomaron como instrumento Marco para la creación de su ordenamiento jurídico interno en relación a la criminalidad informática El Convenio de Budapest y en caso de Nicaragua para la creación del Anteproyecto de Ley de Delitos Informáticos. | La república de El Salvador a diferencia de Costa Rica presenta arduos dificultades en cuanto al ámbito de aplicación de la ley de delitos informáticos por no contar con el recurso técnicos y científicos. |

| | | | |
|---|---|---|---|
| **Nicaragua** | ➢ Constitución política.<br>➢ Ley No. Ley No. 641 código Penal.<br>➢ Ley NO 49, Ley de Amparo incorpora el Recurso de Habeas Data.<br>➢ Ley No. Ley No. 787, Ley de Protección de datos personales.<br>➢ Anteproyecto de Ley especial sobre Delitos Informáticos. | Actualmente estos Estados solo cuentan con el tratado de asistencia legal mutua en asuntos penales entre las Repúblicas de Costa Rica, El Salvador, Guatemala, Honduras, Nicaragua y Panamá, para hacer frente aquellos delitos que por su naturaleza transnacional escapan de sus jurisdicciones. | No cuenta con una norma jurídica especializada en Delitos Informáticos. |

# CAPÍTULO III: PRINCIPALES RETOS Y DIFICULTADES QUE AFRONTAN LOS PAÍSES PARA COMBATIR LA CIBERDELINCUENCIA Y LA COOPERACION INTERNACIONAL COMO PARADIGMA DE SOLUCIÓN

## 3.1 Principales Retos de la Comisión de los Ciberdelitos

El Internet es el espacio de la libertad. Un lugar exento de intervenciones públicas en el que los cibernautas disfrutan de un poder de acción ilimitado. Sobre todo para comunicar y expresarse, para desarrollar experiencias de investigación y culturales de cualquier tipo; esta libertad no solo es inmensa sino que tiene muy difícil limitación. Las propias tecnologías de la telecomunicación que se emplean en Internet están diseñadas, en ocasiones, de modo que hace imposible cualquier restricción de la libertad.

Desde otro punto de vista, podemos decir que Internet es un espacio inadecuado para preservar otros derechos fundamentales, lo cual esto viene a convertirse en problema.

En el ámbito de la delincuencia informática se presentan sin duda importantes complicaciones para el descubrimiento y la investigación de los hechos en y mediante el ordenador, de forma que puede en ocasiones no ser raro que muchos de los casos no lleguen nunca a detectarse. Según datos del *FBI*[56] solo se llegan a descubrir un 1% de los casos, de estos únicamente el 14 se ponen en conocimiento de las autoridades y, finalmente, tan solo un 3% de

[56] Conocido con sus siglas en inglés como Federal Bureau of Investigation o sus siglas en español como Federal de Investigaciones. El FBI es una agencia federal de investigación e inteligencia con jurisdicción sobre una gran variedad de delitos federales, incluyendo asuntos de seguridad nacional como terrorismo y espionaje, secuestro o extravío de menores, crimen organizado, corrupción pública, y delitos cibernéticos/informáticos. Disponible en: https://www.fbi.gov/espanol.

estos últimos acaba en una sentencia condenatoria. De forma que cada 22,000 autores de estos hechos, solamente 1 de todos ellos resultaría condenado por los tribunales.

## 3.2 El impacto económico y dificultades al estimar los daños que provocan los ciberdelitos

Diversos pronunciamientos de gobiernos, empresas líderes y organizaciones internacionales llevan a asegurar que la magnitud del ciberdelitos es realmente preocupante y a plantear escenarios de ataques cibernéticos, con consecuencias gravosas para la población.

Los daños causados a través de las manipulaciones informáticas trascienden los costos de la delincuencia tradicional o convencional. Se ha comprobado que los daños materiales ocasionados por las conductas que convienen incluir en la categoría *criminalidad económica*[57] alcanzan cifras astronómicas, haciendo imposible cualquier comparación entre los causados por los comportamientos integrantes de la denominada *delincuencia común*[58].

Sin embargo, intentar determinar este impacto es una labor compleja por diversos motivos y cualquier afirmación se basará necesariamente en una serie de supuestos justificados, ante la imposibilidad de acceder a datos concretos sobre la ocurrencia del incidente y sus características.

[57] Se caracteriza por generar un daño social considerable, ya que no solo afecta directamente a las instituciones democráticas, sino que socava el financiamiento estatal producto de la reducción de recursos disponibles para la implementación de políticas públicas.

[58] Es cometida por un individuo o cuando mucho por dos y que tienen por objeto la comisión de un delito que podría ser desde una falta menor hasta una grave, no son cometidos por bandas, no hay una gran planeación en los hechos delictivos y no se pretende operar permanentemente a gran escala. Disponible en: https://prezi.com/m/n2u9hf-c2m_b/delincuencia-comun/. Consultado: El 15/06/2016.

### A) Impacto Económico al estimar los daños que provocan los ciberdelitos

El costo más importante de la ciberdelincuencia reside en el daño que hace al rendimiento de la empresa y las economías nacionales, ya que afecta directamente el comercio, la competencia, la innovación y el crecimiento económico mundial.

La ciberdelincuencia afecta a cientos de millones de personas que sufren el robo de su información personal. Según el informe emitido por McAfee sobre las pérdidas netas y estimación del costo global de la ciberdelincuencia mantiene que en total se habrían robado más de 800 millones de registros individuales en 2013. Solo esto equivaldría a 160 000 millones de dólares al año. Las empresas denuncian constantemente ataques de hackers, lo que contribuye a que se extienda la sensación de que la ciberdelincuencia está fuera de control.

Las pérdidas en términos de propiedad intelectual que provoca la ciberdelincuencia son las más difíciles de cuantificar, sin embargo, también son la variable más importante para determinar los daños globales. Los robos de propiedad intelectual alteran las balanzas comerciales y afectan al empleo a nivel nacional. Los países en los que la creación de propiedad intelectual es más relevante o en los que los sectores muy ligados a la propiedad intelectual tienen gran peso en la economía son los más afectados por las pérdidas comerciales, de puestos de trabajo y de ingresos derivadas de la ciberdelincuencia.

Cuando los hackers se apoderan de la información de las tarjetas de crédito de millones de personas, este hecho recibe atención inmediata. Los delitos financieros suelen implicar un engaño, sin embargo, el fraude se puede llevar a cabo de distintas formas, según se dirija contra: consumidores, bancos u organismos públicos. En los delitos financieros más devastadores, los hackers penetran en las redes bancarias, y obtienen acceso a las cuentas para transferir fondos. Estos sofisticados atracos en los que se roban millones de dólares a los bancos son un fenómeno global.

El robo de información confidencial de una empresa —información de inversiones, datos de investigaciones y negociaciones comerciales secretas— puede rendir ganancias inmediatas. Según el informe emitido por McAfee[59] los daños a empresas individuales ascienden a millones de dólares. Y se estiman pérdidas que hacienden a los 1300 millones de dólares debido a fugas de propiedad intelectual que ha supuesto una desventaja para las empresas victimas frente a la competencia. Las actividades de los hackers en bancos centrales y ministerios de finanzas pueden reportar información económica de gran valor para averiguar las tendencias de los mercados o los tipos de interés.

La ciberdelincuencia prolifera en el área de los *mercados bursátiles*[60]. Si consiguen introducirse en las redes de una empresa o de sus abogados o

[59] Informe Pérdidas netas: estimación del costo global de la ciberdelincuencia Impacto económico de la ciberdelincuencia, julio 2014, disponible en: http://www.mcafee.com/mx/resources/reports/rp-economic-impact-cybercrime2-summary.pdf. Consultado: El 20/06/2016.

[60] Bursátil proviene del latín bursa que significa 'bolsa'. El mercado bursátil, por lo tanto, es un tipo particular de mercado, el cual está relacionado con las operaciones o transacciones que se realizan en las diferentes bolsas alrededor del mundo. En este mercado, dependiendo de la bolsa en cuestión, se realizan intercambios de productos o activos de naturaleza similar, por ejemplo, en las bolsas de valores se realizan operaciones con títulos valores como lo son las acciones, los bonos, los títulos de deuda pública, entre otros, pero también existen bolsas especializadas en otro tipo de productos o activos. Disponible en: http://www.banrepcultural.org/blaavirtual/ayudadetareas/economia/mercado_bursatil. Consultado: El 20/06/2016.

contables, los ciberdelincuentes pueden hacerse con información privilegiada sobre planes de fusiones y adquisiciones, informes de resultados trimestrales u otros datos que afecten a la cotización en bolsa de la empresa. Además, sería muy difícil detectar a los ciberdelincuentes que aprovechen esta información para operar en el mercado de valores.

Sin embargo, el factor más importante para determinar el costo de la ciberdelincuencia es el daño que causa a los resultados de las empresas y a las economías nacionales.

El costo de la recuperación tras sufrir un ciberfraude o una filtración de datos para las empresas individuales está aumentando. Además, aunque es cierto que los ciberdelincuentes no podrán rentabilizar la totalidad de la información que roben, el costo total de la recuperación es superior a las ganancias que obtendrán los ciberdelincuentes.

Para la sociedad, las consecuencias reales pasan por pagar la factura de la recuperación y para la empresa, incluyen los daños a la imagen de marca y otras pérdidas relacionadas con la reputación, así como el deterioro (o la pérdida) de las relaciones con los clientes.

La ciberdelincuencia genera grandes ganancias con un riesgo mínimo y a un costo (relativamente) bajo para los hackers. Sin embargo, en el caso de las víctimas ocurre justo lo contrario. Las empresas e individuos toman decisiones sobre cómo gestionar las posibles pérdidas derivadas de la ciberdelincuencia en función de los riesgos que están dispuestos a aceptar y el dinero que están dispuestos a gastar para mitigar dichos riesgos.

A medida que aumentan las actividades empresariales que se realizan online, se incrementa el número de consumidores que se conectan a Internet en todo el mundo y proliferan los dispositivos autónomos conectados a la Red, crecen las oportunidades para cometer ciberdelitos.

Las pérdidas a causa del robo de propiedad intelectual repuntarán si los países que la adquieren mejoran su capacidad para utilizar dicha información para fabricar sus propios productos. La ciberdelincuencia constituye un impuesto sobre la innovación y retrasa el ritmo de la innovación en el mundo, ya que reduce la tasa de rendimiento para innovadores e inversores.

### B) Dificultades económicas al estimar los daños que provocan los ciberdelitos

**a)** Ausencia de datos sobre la cantidad real de casos registrados.

**b)** Dificultades para establecer los costos indirectos y dimensionar la población afectada.

**c)** Bajo nivel de seguimiento y registro del tiempo y los recursos asignados al momento enfrentar un ataque.

**d)** Problemas para determinar sus consecuencias en el tiempo, todo lo cual dificulta la posibilidad de conocer el gasto total de remediación y compensación por las pérdidas registradas.

**e)** Escaso volumen de datos de casos de ataques o fallas reportados.

**f)** Son delitos difíciles de demostrar. Ya que, en muchos casos, es complicado encontrar las pruebas.

**g)** Son 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.

**h)** Los delitos informáticos tienden a proliferar y evolucionar. Porque complica aún más la identificación y persecución de los mismos.

## 3.3 El problema de las múltiples jurisdicciones y la responsabilidad penal en la comisión de los ciberdelitos

### a) El problema de las múltiples jurisdicciones

Nos referimos en concreto a la aplicación espacial de la ley penal. La gran libertad para cometer delitos con independencia absoluta del territorio, como se ha expuesto en el anterior apartado, origina grandes problemas. Recordemos, el sujeto activo puede cometer sin problemas un delito desde un Estado diferente al que se encuentra el sujeto pasivo, incluso sin saber dónde se halla éste último.

Esta nueva perspectiva, genera dudas a todos los niveles, tanto en relación al órgano estatal que va a conocer del asunto, como de la posibilidad de ejecutar la resolución recaída. Igualmente, un problema importante será la distinta regulación del Derecho sustantivo en los distintos Estados. Pudiera crearse un falso espejismo si pensamos que debido a que en la esfera penal jurisdicción y ley aplicable siempre coinciden, no existen dificultades en lo relativo a las reglas materiales que deben ser aplicadas.

Lo cierto es que, más allá de esta circunstancia, encontramos gran cantidad de supuestos en que determinados actos son punibles con arreglo al Derecho Penal de un Estado, pero no en otros, dando lugar a obvias desigualdades y zonas de impunidad.

**b) El problema de la responsabilidad penal**

No nos referiremos aquí a las personas físicas que carecen de la responsabilidad penal de sus actos, sino a un tema particular que ha suscitado polémica en los últimos tiempos, la responsabilidad penal de las empresas en la comisión de delitos por Internet.

Es necesario decir, que el principio general del que se parte, en la mayoría de los países, es la irresponsabilidad de las personas jurídicas (formulado usualmente como societasdelinquere non potest). Teniendo esto en cuenta, se critican las posibles lagunas de *punibilidad*[61] que pueden aparecer ante la complejidad de determinar la *responsabilidad penal*[62].

Así, primero hay que lograr probar la actuación de la empresa, después quiénes fueron realmente los autores de la infracción, y finalmente el grado de responsabilidad de la actividad de los diferentes partícipes en el delito.

[61] Merecedor de Castigo. / Penado en la Ley. Diccionario Jurídico Cabanellas.
[62] La que se concreta en la aplicación de una pena, por acción u omisión dolosa o culposa del autor de una u otra. Diccionario Jurídico Cabanellas.

## 3.4 Cooperación internacional

La creciente densidad de tecnologías de la información y las comunicaciones también aumenta la frecuencia de ataques de la delincuencia informática, obligando a las naciones a establecer legislaciones que hagan frente a esta problemática. Se requiere de leyes nacionales adaptadas a la delincuencia cibernética para responder eficazmente a las peticiones externas de asistencia o para obtener asistencia de otros países.

Cuando se elabora legislación, la compatibilidad con las leyes de otras naciones es una meta esencial; la cooperación internacional es necesaria debido a la naturaleza internacional y transfronteriza de la delincuencia informática. Se necesitan mecanismos internacionales formales que respeten los derechos soberanos de los Estados y faciliten la cooperación internacional. Para que la asistencia judicial recíproca funcione con éxito, los delitos sustantivos y los poderes procesales de una jurisdicción deben ser compatibles con los de otras.

Los Estados tienen plena responsabilidad de reconocer que es de vital importancia la regularización de este fenómeno jurídico, a fin de establecer sanciones y mecanismos de investigación adecuados, que sean lo suficientemente avanzados y dinámicos como para hacer frente a este tipo de actividades delincuenciales.

Para eso tenemos que tener claro que las medidas que se tome en el ámbito ciberdelictual deben contar con carácter específico y global al que se enfrenta, pero sobre todo es necesaria una visión conjunta de los problemas.

La dimensión *supranacional*[63] juega un papel de real importancia en el tratamiento de los delitos informáticos. Es imperativa la ejecución de políticas conjuntas, generales, que integren a todos los Estados y sectores de la sociedad.

Desde nuestro punto de vista, podemos decir que no basta con establecer una correcta política de cooperación, lo ideal no son los Tratados bilaterales, sino los *Convenios Multilaterales*[64], ya que estos pueden involucrar al mayor número de países posible. De esta manera sería posible armonizar las políticas regionales en materia de cibercrímenes, logrando una regulación coherente, que no se contradiga y cuya utilización fuera posible a gran escala.

Las relaciones de los Estados, deben enmarcarse dentro de un plano de igualdad, equidad, reciprocidad, cooperación y respeto y autodeterminación de los pueblos.

La cooperación tendrá como fundamento los instrumentos internacionales aplicables a la materia, así como la legislación uniforme o recíproca y por supuesto el derecho interno de cada parte, lo anterior en aras a agilizar las investigaciones o los procedimientos relativos a delitos relacionados con sistemas y datos informáticos o bien para la obtención de pruebas electrónicas de la existencia de estos delitos.

[63] Adjetivo que sobrepasa los límites de lo nacional: autoridad supranacional; las ONG son organizaciones supranacionales. sistema político en el cual determinados Estados ceden parte de sus atribuciones de gobierno. Disponible en: http://www.oxforddictionaries.com/es/definicion/espanol/supranacional. Consultado: El 04/07/2016.

[64]Es un acuerdo internacional que involucran a un gran número de Estados, se suelen elaborar en el seno de las Organizaciones Internacionales sobre las que incide el ámbito material del tratado. Disponible en: http://www.um.es/aulademayores/docs-cmsweb/tema__general.pdf. Consultado: El 04/07/2016.

La cooperación internacional entre los Estados en materia penal, se rige a partir de los acuerdos bilaterales o multilaterales, suscritos en el tema por los diversos países y a falta de los mismos se enmarca dentro de los principios de voluntariedad y reciprocidad.

La asistencia judicial penal, reviste particular importancia pues a través de la misma se hace efectiva la obtención de pruebas que hayan podido recaudarse en país extranjero para la persecución de delitos y conductas ilícitas. La investigación de la delincuencia informática no es una tarea fácil, ya que la mayoría de los datos probatorios son intangibles y transitorios. Los investigadores de delitos cibernéticos buscan vestigios digitales, que suelen ser volátiles y de vida corta. También se plantean problemas legales en relación con las fronteras y las jurisdicciones. La investigación y el enjuiciamiento de delincuentes informáticos ponen de relieve la importancia de la Cooperación internacional.

Como hemos hecho hincapié, la posibilidad de infringir bienes jurídicos en distintas jurisdicciones provoca un abismo a la hora de llevar justicia en materia de delincuencia informática, por lo que establecer un frente común como el que propone el Convenio de Budapest en el artículo *23*[65] y siguientes, es la única manera de combatir estos nuevos tipos de delitos, así como aquella delincuencia a la que referimos como computacional, que si bien es tradicional adoptó el medio informático

[65] Las Partes cooperarán entre sí en la mayor medida posible, de conformidad con las disposiciones del presente capítulo, en aplicación de los instrumentos internacionales aplicables a la cooperación internacional en materia penal, de acuerdos basados en legislación uniforme o recíproca y de su derecho interno, para los fines de las investigaciones o los procedimientos relativos a los delitos relacionados con sistemas y datos informáticos o para la obtención de pruebas electrónicas de los delitos. Principios generales relativos a la cooperación internacional. Convenio de Budapest, Artículo 23.

como técnica para maximizar su alcance y con eso su carácter transgresor de fronteras políticas.

## CONCLUSIONES

**1)** A lo largo de este estudio, pudimos observar que los delitos informáticos son conductas que día a día se presentan con mayor frecuencia, afectando gravemente los Derechos constitucionales de las víctimas de los ciberataques.

**2)** El constante avance tecnológico y las nuevas formas de comisión de delitos en el mundo, no deben estar separadas de las correspondientes reformas y creaciones legales, se deben crear nuevas normas que abarquen y contemplen las posibles vulneraciones a los derechos constitucionales para que las personas puedan tener opciones y medios dónde acudir para denunciar y protegerse frente a cualquier delito.

**3)** La escasez de datos concretos sobre la cantidad de ataques potenciales o reales, y de sus costos asociados, hace difícil conocer su verdadera magnitud y la profundidad del impacto económico que generan los ciber ataques.

**4)** Costa Rica fue el primer país en Centroamérica que regulo la Ciberdelincuencia con la Ley 9048, la que fue aprobada el 6 de noviembre del año 2012. Dicha Ley vino a reformar 6 artículos que se encontraban estipulados en el Código Penal y a su vez incorporo nuevos tipos penales, así mismo agrava las penas para aquellos delitos cometidos a través de sistemas de informáticos.

**5)** Por su parte la Republica de El Salvador por medio de la leyse sancionan aquellas conductas delictivas cometidas por medio de las Tecnologías de la Información y la Comunicación, así mismo se previenen y sancionan de los delitos cometidos en perjuicio de los datos almacenados, procesados o transferidos. En cuanto a los tipos de penas esta ley no cambio mucho en comparación con las demás normativas dispersas puesto que estas legislaciones como el código penal, ley de acceso a la información pública y ley especial contra los delitos informáticos y conexos, entre otros, le sirvieron para establecer los conceptos y las penas de dichos delitos, en los que las penas al igual que esta ley, oscilan entre los 4 y 12 años mayormente aclarando que en los agravantes puede aumentar hasta una tercera parte de la pena máxima del delito que se impute.

**6)** Aunque una situación que todavía aqueja al Salvador es en cuanto a su método de aplicación o ejecución de esta ley en el ámbito de lo real, puesto que por la complejidad de este delito es muy difícil darle seguimiento a los ciberdelincuentes, por lo se debería de crear campañas para informar a las personas de estos tipos de delitos que cada día ocurren con más frecuencia.

**7)** Nicaragua a diferencia de la República de Costa Rica y El Salvador, regula la ciberdelincuencia por medio de diferentes leyes, dado que no cuenta con una norma legal concreta que de tratamiento especializado a la criminalidad informática, puesto que se sancionan estas conductas en

diferentes cuerpos normativos. Siendo así que nuestro código penal vigente sanciona la criminalidad propiamente dicha en tan solo seis artículos, mientras en otras leyes como Habeas Data y Ley de Protección de Datos proporcionan mecanismo para regular el uso de información de carácter personal. Es así pues que estos tres países a través de diferentes mecanismos intentan hacer frente al fenómeno d la ciberdelincuencia.

**8)** Estos esfuerzos serán insuficientes si no se procura crear un instrumento jurídico de carácter regional en Centroamérica que involucre a los países centroamericanos siendo que la ciberdelincuencia es un fenómeno trasnacional que casi siempre involucra la jurisdicción de los estados y si la mutua cooperación de los países será insuficientes la normas internas

# RECOMENDACIONES

El avance tecnológico ha rebasado al orden jurídico nacional por medio del uso del internet, la informática y las telecomunicaciones razón por la cual se exponen las siguientes propuestas:

## AL ESTADO

**1)** Desarrollar estrategias nacionales sobre ciberseguridad que contemplen campañas de concientización protección para la ciudadanía, mecanismos de coordinación con el sector privado y con otros países y se priorice la generación de un marco normativo adecuado para la penalización de delitos de esta naturaleza.

**2)** Para la implementación e investigación de estos tipos de delitos se debe mejorar la coordinación y el trabajo conjunto entre los organismos involucrados en la adopción de medidas de seguridad de la información como son Policías, Organismos judiciales entre otros.

**3)** Desarrollar contenidos y programas de formación de profesionales especialistas en seguridad de la información, que la aborden desde distintas visiones: técnica, legal y educación.

**4)** Desarrollar líneas de investigación que analicen las distintas perspectivas de los ciberataques.

**5)** Generar equipos tecnológicos dentro de las organizaciones que aborden la seguridad informática con un enfoque múltiple, que permita

comprender y resolver los problemas relacionados con la protección de la información desde diversas perspectivas.

## A LOS USUARIOS

**1)** Inducirlos a través de campañas de concientización a Adoptar una actitud responsable frente al uso de las tecnologías de información, capacitándose para minimizar los riesgos que las acompañan.

**2)** Denunciar los incidentes de seguridad ante las instancias que correspondan, permitiendo su seguimiento y contribuyendo así a su resolución.

**3)** Enseñar a los menores los peligros de las redes sociales y entrenarlos en una adecuada utilización de las tecnologías de la información.

## FUENTES DEL CONOCIMIENTO

**Primarias:**


- Constitución Política de la Republica de Costa Rica, Plublicada el 10 de Julio del 2011.
- Constitución de la República de El Salvador, Publicada el 12 de Junio del año 2014.
- Constitución Política de la República de Nicaragua / Managua, Nicaragua. Gaceta diario oficial N° 32. 18 de febrero del año 2014.
- Convenio sobre Cibercriminalidad Budapest. 23 de Noviembre de 2001.
- Ley Nº 4573.- Código Penal de la República de Costa Rica, reformado el 24 de Junio del año 2010.
- Decreto Nº 1030.- Código Penal de la Republica de el Salvador, 30 de abril 1997.
- Ley Nº 641, Código Penal De Nicaragua, Publicado el 9 de Mayo Del 2008.
- Ley Nº 9048 Reforma de Varios Artículos y Modificación de la Sección VIII, Denominada Delitos Informáticos y Conexos, del Título VII del Código Penal, de la República de Costa Rica, del 10 De julio Del 2012.
- Decreto Nº 260 Ley Especial Contra Los Delitos Informáticos y Conexos, de la República de El Salvador. Publicado el 26 de febrero del 2016.
- Ley Nº 49, Ley de amparo, Publicado el martes 4 noviembre de 2004.
- Ley Nº 831, Ley de reforma y adiciones a la ley Nº 49, ¨Ley de Amparo¨ Publicado el 30 de Enero del 2013.

- La Ley No. 787, Ley de Protección de Datos Personales**.** Aprobada el 21 de Marzo del 2012 y publicada en La Gaceta del 29 de Marzo del 2012.
- Anteproyecto de Ley especial sobre Delitos Informáticos.

**Secundarias:**

- RODRÍGUEZ MORULLO/Alonso Gallo/LASCURAÍN SÁNCHEZ, "Derecho Penal E Internet", Pág. 259.
- TELLEZ VALDÉS, Julio. 2004. *Derecho Informatico.* Tercera edición. México : McGraw-Hill Interamericana, 2004.
- DEL PINO, Santiago Acurio. Delitos Informáticos: Generalidades. Profesor Del Derecho Informático de la Puce. Pag.15.
- BOEN OEKLERS, Dotty. Comercio Electrónico. Serie Business. Cengage Learning Editores, 2004. Pág. 124.
- MUÑOZ MACHADO, Santiago. 2000. La Regulacion de la Red Poder Y Derecho En Internet. Madrid : Santillana de Ediciones, S.A., 2000, 2000.

**Terciarias:**

**<u>Enciclopedias</u>**

- Juridica, Enciclopedia. http://www.enciclopedia-juridica.biz14.com/d/delincuente/delincuente.htm. [En línea] [Citado el: 14 de Junio de 2016.]

**Tesis**

- Delincuencia Informática: Daños Informáticos del Artículo 264 del Código Penal Y Propuesta de Reforma Tesis Doctoral de: Jorge Alexandre González Hurtado Bajo La Dirección de: María Teresa Requejo Naveros Madrid, 2013 Pág. 227

**Boletín informático**

- V.05-82113 Undécimo Congreso de las Naciones Unidas Sobre Prevención del Delito y Justicia Penal, 18 a 25 de abril de 2005, Bangkok (Tailandia) Pág. 2 Disponible en: www.11uncongress.org véase también: www.unodc.org

**Notas de prensa**

- MORÁN, Otto. 2013. Preparan Ley Para Castigar Ciberdelitos. La Prensa. 21 de julio De 2013.
- CALDERÓN, Beatriz 2015. Diputados Acuerdan Aprobar Ley De Delitos Informáticos. La Prensa. 07 de julio de 2015.
- CUBIAS VILLALOBOS, Norma Cecilia. Nueva Ley Contra los Delitos Informáticos en EL Salvador. 2016. EL Salvador : Northclaimy, 2016.

**Revistas**

- ESTRADA, Alex Canedo La Informática Forense y los Delitos Informaticos. Corporacion Americana Universitaria. 2010. [ed.]. No.4, Costa Rica : CARUNIAMERICANA, Enero – Junio de 2010, Revista Pensamiento Americano, Vol. III, págs. Pag: 81-88. ISSN: 2027-2448.

- MIRÓ LLINARES, Fernando. La oportunidad criminal en el ciberespacio. Aplicación y desarrollo de la teoría de las actividades cotidianas para la prevención del Cibercrimen. Revista Electrónica de Ciencia Penal y Criminología (en línea). 2011, núm. 13-07, p. 07:1-07:55. ISSN 1695-0194 [RECPC 13-07 (2011), 29 Nov].
- BARINAS UBIÑAS, Désirée. El impacto de las tecnologías de la información y de la comunicación en el derecho a la vida privada. Las nuevas formas de ataque a la vida privada. *Revista Electrónica de Ciencia Penal y Criminología* (en línea). 2013, núm. 15-09, p. 09:1-09:60. ISSN 1695-0194 [RECPC 15-09 (2013), 17 Sep].
- MIRÓ LLINARES, Fernando. La respuesta penal al ciberfraude. Especial atención a la responsabilidad de los muleros del *phishing*. *Revista Electrónica de Ciencia Penal y Criminología* (en línea). 2013, núm. 15-12, p. 12:1-12:56. ISSN 1695-0194 [RECPC 15-12 (2013), 17 Sep].
- FUENTES OSORIO, Juan Luis. Lesiones producidas en un contexto de violencia doméstica o de género: una regulación laberíntica. *Revista Electrónica de Ciencia Penal y Criminología* (en línea). 2013, núm. 15-16, p. 16:1-16:57. ISSN 1695-0194 [RECPC 15-16 (2013), 25 Dic].
- FLORES PRADA, Ignacio. Prevención y solución de conflictos internacionales de jurisdicción en materia de ciberdelincuencia. *Revista Electrónica de Ciencia Penal y Criminología* (en línea). 2015, núm. 17-21, pp. 1-40. ISSN 1695-0194 [RECPC 17-21 (2015), 26 Dic].

## Sitios WEB


- http://lema.rae.es/desen/?key=globalización.
- http://www.alegsa.com.ar/dic/bitnet.php.
- http://www.dsteamseguridad.com/archivos/hackconf/anonympus_remington.pdf
- http://derechocarlosinformatica.blogspot.com/.
- http://www.microsoft.com/latam/seguridad/hogar/spam/phishing.mspx.
- http://www.enciclopediajuridica.biz14.com/d/delincuente/delincuente.htm
- http://www.definicionabc.com/tecnologia/hacker-2.php.
- http://web.mit.edu/rhel-doc/4/RH-DOCS/rhel-sg-es-4/ch-risk.html.
- https://www.vozcero.com/que-es-un-hacker/.
- http://es.thefreedictionary.com/para%c3%adsoa.
- http://www.wordreference.com/definicion/cibern%c3%a9tico.
- http://www.irdaoc.com/irdaoc/documentos/pidat_ii_2010/group_4_analisis_del_proceso_de_delitos_informaticos.pdf
- http://www.ictparliament.org/sites/default/files/delitosinformaticos.pdf
- http://www.delitosinformaticos.info/delitos_informaticos/tipos_delitos.html
- http://www.abogadorojaspozo.com/ciberdelincuencia-problemas-para-combatirla/
- http://www.wordreference.com/definicion/estado
- http://www.wordreference.com/es/en/frames.aspx?es=signatario
- http://definicion.de/accion-penal/#ixzz4cuignbbx
- http://www.wipo.int/about-wipo/es/

- http://www.mcafee.com/mx/resources/reports/rp-economic-impact-cybercrime2-summary.pdf
- http://www.mcafee.com/mx/resources/reports/rp-economic-impact-cybercrime2-summary.pdf
- http://www.comjib.org/sites/default/files/ciberdelito_convenio%20y%20adhesiones.pdf
- http://ticoblogger.com/2012/07/11/delitos-informaticos-costa-rica/
- http://www.comjib.org/sica/inicio-sica
- http://es.thefreedictionary.com/para%c3%adso
- http://www.wordreference.com/definicion/cibern%c3%a9tico
- https://www.ucr.ac.cr/noticias/2012/08/21/expertos-creen-que-ley-de-delitos-informaticos.html
- http://conventions.coe.int/treaty/en/treaties/html/185-spa.htm.
- http://www.mastermagazine.info/termino/5368.php
- https://prezi.com/ibzhvl-qmtfe/definicion.