UNIVERSIDAD NACIONAL AUTONÓMA DE NICARAGUA

UNAN-LEÓN

FACULTAD DE CIENCIAS JURÍDICAS Y SOCIALES

MONOGRAFÍA PARA OPTAR AL TÍTULO DE LICENCIADOS EN DERECHO.

DERECHO INFORMÁTICO DE LA UNIÓN EUROPEA COMO MODELO DE ANÁLISIS EN LA LEGISLACIÓN NICARAGÜENSE

AUTORES:

Br. KAROLA YESENIA NARVÁEZ MERCADO.

Br. KATHLEEN VANESSA OBANDO PARAJÓN.

Br. FREDDY MANUEL RIVAS TORRES.

TUTOR: PhD. DENIS IVÁN ROJAS LANUZA.

MAYO DE 2013

¡A LA LIBERTAD POR LA UNIVERSIDAD!

DERECHO INFORMÁTICO DE LA UNIÓN EUROPEA COMO MODELO DE ANÁLISIS EN LA LEGISLACIÓN NICARAGÜENSE

DEDICATORIA.

A:

Rosibel Torres: leona de tiempo completo.

Freddy Rivas: luchador, trabajador y pensador.

Danelia Aguilar: leonesa de corazón.

Rosa Tercero: la mera tayacana.

Kathleen Obando: más que novia, una amiga.

Mabel Rivas: donde quiera que esté.

Engels Aguilar: hasta chile.

Alfredo y Luis: quienes juntos son un 10.

Néstor, Omar, Elwin, Moisés, Jorge, María José, Karola: amigos que de algún modo aparecieron.

Pobres, humildes, campesinos y humillados: a ustedes.

FREDDY MANUEL RIVAS TORRES.

DEDICATORIA.

Antes que nada he de dar gracias a Jehová Dios y su hijo Jesús por ser quienes me han bendecido grandemente, por permitirme llegar hasta estos momentos y darme las fuerzas para continuar.

A mi Madre **Teresa Parajón**, quien es la margarita más bella y olorosa en mi jardín, por ser sencilla y enseñarme siempre que la humildad ante todo, por enseñarme buenos valores cotidianos y el amor a Dios.

A mi Padre **Jorge Obando,** porque ante todas las adversidades y dificultades siempre me ha demostrado su amor incondicional.

A mis dos Hermanitos, **Juan Obando y José Parajón**, quienes siempre han estado junto a mí aun en los momentos más difíciles.

A **Freddy Rivas,** quien es una Bendición de Dios en mi vida.

A la familia **Fernández - Domper**, quienes han demostrado su amor por mi familia y sobre todo por mi madre brindándonos su verdadera amistad.

A mis abuelitas y abuelito quienes juntos siempre me han demostrado su amor incondicional, a mis tíos y tías quienes siempre me han visto como su hija.

A mis primos, a mi chiquitín **Lawrent Sixto, Jana Rachel, Jahir, Sarela** y mi chiquitita **Lindsay** quien es un amor y a su hermanita también, a mis amigos y demás familiares, que no menciono por falta de tiempo pero que siempre están en mi corazón.

KATHLEEN VANESSA OBANDO PARAJÒN.

DEDICATORIA.

A **Dios**, por brindarme el aliento de vida, por cuidarme en todos y cada uno de los momentos de mí vida y por regalarme el don de la sabiduría.

A mi madre **Gladys Mercado**, pilar que me sostiene, por su amor, sacrificio, respaldo, por los valores morales y espirituales que me ha transmitido los cuales son de gran ayuda en mi vida.

A mi padre **Reynaldo Narváez**, por su cariño incondicional y por su enseñanza brindada la cual me ha guiado en el camino del bien.

A mis hermanos **Reynaldo** y **Roderick**, por todo su amor, apoyo, comprensión en los momentos de tristeza y alegría.

A mi abuelita **Anita**, madre luchadora que con sus ejemplos de perseverancia y fortaleza me ha demostrado que en la vida todo se puede lograr.

A mis tíos, tías, primos y primas, por todas las vivencias compartidas.

A mis compañeros de monografía, por luchar en este arduo trabajo.

Y por último pero no menos importante a mis amigos que han marcado mi vida con momentos inolvidables e irrepetibles; en especial a **Moisés Reyes,** por su compañía y por todos sus consejos manifestados.

KAROLA YESENIA NARVÁEZ MERCADO.

AGRADECIMIENTO.

A **Dios** nuestro Padre Celestial, principal guía en el camino de la vida y la verdad, por su amor y su infinita misericordia.

A nuestros **Padres**, por su apoyo incondicional, sus consejos, ánimos, por sus sacrificios, por darnos la formación que necesitamos para convertirnos en hombres y mujeres útiles a la sociedad.

A nuestro tutor **PhD. Denis Iván Rojas Lanuza**, por ser nuestro guía, por la dedicación que nos brindó, por su paciencia, por sus indicaciones, sus consejos y sabias correcciones las cuales fueron de suma importancia para consolidar nuestro trabajo.

ÍNDICE

INTRODUCCIÓN

El trabajo DERECHO INFORMÁTICO DE LA UNIÓN EUROPEA COMO MODELO DE ANÁLISIS EN LA LEGISLACIÓN NICARAGUENSE, es resultado del evidente vacío legislativo en cuanto a la regulación del derecho informático en Nicaragua, por lo cual utilizamos los instrumentos legislativos de la Unión Europea como un modelo de desarrollo en cuanto a esta materia, partiendo de la idea que el viejo continente tiene un gran avance en la tecnología regulada de manera supranacional, y que ha conllevado a su legislación comunitaria.

El intercambio de información personal y flujo trasnacional de datos personales a causa del surgimiento de nuevas vías de comunicación propias de un mundo globalizado, se genera de manera habitual y en forma masiva, en la dinámica de las ciencias jurídicas e impulsado por el desarrollo tecnológico que ha generado un cambio en toda la actividad jurídica, comercial y social a nivel mundial; por lo tanto debemos adoptarnos a los nuevos métodos que proporcionan las técnicas asociadas al ordenador, adecuarlas a la actividad jurídica y al desarrollo tecnológico, se hace perentorio entonces la acreditación de un marco legal que tutele esta novedosa rama.

Los primeros intentos por estudiar desde el punto de vista jurídico el fenómeno informático se gestaron en la década de los sesenta cuando iniciaban los primeros ordenadores, estos primeros pasos eran básicamente el intento de aplicar las instituciones jurídicas existentes al área de la informática, surge así pues prácticamente a mediados de la década de los 80, la necesidad de dedicar un estudio especializado del aspecto normativo del fenómeno informático; fue así como surgió el Derecho informático,

como una ciencia formal y especializada en todos los aspectos de la regulación jurídica de la informática, quedando la informática jurídica como una ciencia auxiliar del desarrollado y del bien estructurado Derecho Informático.

En Europa entre 1966 y 1969, con la denominación de "Cibernética y Derecho", se designaron las encuestas de estadística judicial que recurrieron al computador, los estudios de lógica formal aplicada al Derecho, los trabajos puramente computacionales que de alguna manera tuvieron que ver con normas jurídicas, como las investigaciones del Derecho que recurrieron a esquemas teóricos provenientes de la cibernética.

Ya por el año 1968 el destacado estudioso del tema Mario Lasono[1], propuso sustituir el término "*Jurimetría*" por el de "*Iuscibernética*".

El término "Derecho Informático" (*Rechtinformatik*en alemán) fue acuñado por el Prof. Dr. Wilhelm Steinmüller, académico de la Universidad de Regensburg de Alemania, en el año de1970. Sin embargo, no es un término unívoco, pues también se han buscado una serie de términos para el Derecho Informático tales como Derecho Telemático, Derecho de las Nuevas Tecnologías, Derecho de la Sociedad de la Información, Iuscibernética, Derecho Tecnológico, Derecho del Ciberespacio y Derecho de Internet.

Mas sin embargo para definir el derecho informático nos apegamos a la definición de, Julio Téllez Valdés quien lo determina así: "*El derecho informático es el conjunto de normas, principios e instituciones que*

[1] Filósofo del derecho y especialista en derecho informático por la Universidad Carlos III de Madrid.

regulan las relaciones jurídicas emergentes de la actividad informática. De igual manera el derecho informático puede definirse como: El conjunto de leyes, normas y principios aplicables a los hechos y actos derivados de la Informática"[2]

Para una mejor sistematización del Derecho Informático, su contenido es determinado por la protección jurídica de los datos personales, el flujo de datos transfronterizos e Internet, protección jurídica de los programas de computación, delitos informáticos, contratos informáticos y comercio electrónico. Es todo lo que hace referencia al Derecho Informático.

Se puede asegurar que la relación derecho-informática adquiere una importancia crucial ya que de un lado se ve la aparición de un fenómeno revolucionario llamado "la informática" que lleva dentro de su seno la energía para consolidar la liberación del hombre pero que al ser fenómeno nuevo y al no estar sujeto a reglas precisas podría ser sujeto de dominación, de ahí la importancia de su regulación.

Para la elaboración de este trabajo nos planteamos como objetivo general comparar los principales instrumentos jurídicos del Derecho Informático de la Unión Europea en relación con la legislación nicaragüense y como objetivos específicos brindar conocimientos básicos del Derecho Informático; estudiar el marco legal del comercio electrónico de la Unión Europea; y analizar la normativa referente a protección de datos y delitos informáticos entre ambas legislaciones.

En la actualidad a nivel internacional la difusión y desarrollo de esta materia en los llamados países industrializados tales como los Estados Unidos, Inglaterra, España, Francia, Alemania y Japón así como algunos países latinoamericanos como Argentina, Uruguay, México, Chile y

[2] TÉLLEZ VALDÉS, Julio. *Derecho Informático*. Tercera edición, Mc Graw-Hill Interamericana Editores S.A, México 2004. Pág. 24.

Venezuela ha sido impresionante. La mayoría de las facultades de Derecho de estos países han incluido en su plan de estudio esta materia, sin dejar a un lado las especialidades como maestrías e inclusive doctorados que se pueden cursar en algunas facultades de derecho como en Francia, por ejemplo. Esto debido al avance de las tecnologías que va en desarrollo. Razón de ello el Comité de Ministro del Consejo de Europa recomendó a los Estados (de la Unión Europea) la enseñanza, la investigación y formación en materia de "informática y derecho" y su "creciente importancia" que debe realizarse en el nivel académico. Como vemos en Europa y su latente progreso tecnológico es donde ha evolucionado más este derecho; motivo de nuestro trabajo, con todo lo antes expuesto nos surgen los siguientes cuestionamientos ¿En Nicaragua se puede implementar normas relativas de Derecho Informático tomando como base la legislación de la Unión Europea?; si se implementara estas normas del Derecho informático de la Unión Europea ¿Qué beneficios aportaría a nuestra legislación?; ¿Cuál es la situación de la legislación nicaragüense referente al Derecho informático?

En la elaboración de esta investigación partimos del método científico teórico documental que se define como aquella que trabaja con un dato ideal o especulativo contenido en objetos teóricos conceptuales, se auxilia de métodos teóricos.[3] De igual manera aplicaremos el método de Derecho comparado o de comparación jurídica, definido como aquel mediante el cual se cotejan o contrastan dos o más objetos jurídicos (sistemas de Derecho, normas, instituciones, procedimientos, etc.) a fin de descubrir

[3] VILLABELLA ARMENGOL, Carlos Manuel. *La investigación y comunicación científica en la ciencia jurídica.* Primera edición. Editorial Instituto de Ciencias Jurídicas de Puebla. Puebla, México. 2009. P.118.

sus relaciones, estimar sus diferencias y resaltar sus semejanzas, lo cual posibilita percibir los rasgos esenciales, hallar explicaciones y llegar a la esencia de las variables que se han determinado. Consultaremos fuentes documentales, teniendo como primarias La Constitución, Leyes, Directivas, Doctrinas de autores especializados en la materia y Jurisprudencia; como fuentes secundarias, revistas, artículos periodísticos y documentos electrónicos.

Para cumplir con nuestros objetivos dividimos el trabajo monográfico en tres capítulos; el Capítulo I denominado "Generalidades del Derecho Informático y su relación con otras ramas del Derecho", éste capítulo contendrá el origen del Derecho informático, nociones del Derecho informático, su clasificación, fuentes, importancia, contenido y las relaciones que tiene con las diferentes ramas el Derecho. En el Capítulo II referido al "Análisis comparativo del comercio electrónico dentro de la Unión Europea y Nicaragua" se estudiará su concepto, las directivas de la Unión Europea relacionada a este fenómeno, el estudio de la firma electrónica, la protección de tatos con relación a esta forma de comercio y la legislación nicaragüense. El Capítulo III contendrá "Los Delitos informáticos", se analizará su concepto, sus principales características, elementos y sujetos que participan en estos actos ilícitos, observando las normas de la Unión Europea y la forma en que están tipificados en Nicaragua.

CAPÍTULO I: GENERALIDADES DEL DERECHO INFORMÁTICO Y SU RELACIÓN CON OTRAS RAMAS DEL DERECHO.

1.1. Cibernética.

El nacimiento de la cibernética se estableció en el año 1942. Cinco años más tarde, Norbert Wiener uno de los principales fundadores de esta ciencia, propuso el nombre de cibernética, derivado de una palabra griega que puede traducirse como piloto, timonel o regulador.[4] Por tanto la cibernética es la ciencia que se ocupa de los sistemas de control y de comunicación en las personas y en las máquinas, estudiando y aprovechando todos sus aspectos y mecanismos comunes.[5]

1.2. Generalidades de la Computación.

Desde tiempos muy remotos el hombre, al verse en la necesidad de cuantificar sus pertenencias (animales, objetos de caza, pieles, etcétera), ha tenido que procesar datos. En un principio este procedimiento fue rudimentario ya que se utilizaba las manos y se almacenaba toda la información posible en su memoria. Esto impedía un flujo fácil de la información, porque al no existir representaciones fijas de los elementos que se tenían en un proceso determinado, las conclusiones a las que llegaba resultaban especuladoras. El hombre para contar estaba limitado al número de sus dedos; esto fue superado cuando empezó a utilizar otros medios como cuencas, granos y objetos similares.

4 ASIMOV, Isaac. Enciclopedia biográfica de ciencia y tecnología: la vida y la obra de 1197 grandes científicos desde la antigüedad hasta nuestros días. Alianza Editorial Mexicana. México. 1988. p. 906.

5 GUILLÉN BUSTAMANTE, Giovanny. *Cibernética*. Caracas, Venezuela, Especialista Certificado en Sistemas IBM AS/400. Publicado 13 de Enero de 2000.

Posteriormente, inventó un sistema numérico que le permitió realizar sus operaciones con mayor confiabilidad y rapidez, e ideó algunas herramientas que le ayudaron en su afán de cuantificar.

1.2.1. Concepto y estructura.

La computadora es una máquina automatizada de propósito general integrada por elementos de entrada (pantallas, disco, cintas, etc.), procesador central (CPU), dispositivos de almacenamiento, elementos de salida (pantalla impresora, etc.), a nivel estructural la computadora está integrada por el hardware (lo constituyen las partes mecánicas y electro magnéticas, es, la estructura física de la computadora) y el software (que es el que ejecuta los programas y actividades).[6]

1.3. Sociedad de la información.

La sociedad de la información implica el uso masivo de las tecnologías de la información y la comunicación para difundir el conocimiento y los intercambios en una sociedad. Así se identifica un nuevo ambiente donde la comunicación está inmersa. Lo propio de la sociedad de la información es la creación del conocimiento científico, la aplicación de dicho conocimiento, la tecnología y la difusión de la misma entre los actores económicos; todos los países deben tener una política nacional para ingresar a la sociedad de la información y su política científica tecnológica y de innovación productiva es el instrumento motor y articulador para lograrlo.[7] Se propone que la sociedad de la información sea incluyente y que se rija bajo ciertos principios éticos y jurídicos. Este fenómeno está

[6] TÉLLEZ VALDÉS, Julio. Ob. Cit. pág. 5.
[7] Ibídem, págs. 6 y sig.

impulsado por los nuevos medios disponibles para crear y difundir información mediante tecnologías digitales.[8]

1.4. Informática.

La informática es la ciencia que se dedica al tratamiento automático de la información mediante el uso del ordenador.

El término informática viene del vocablo francés *informatique* creado en 1962 por Philippe Dreyfus y se ha formado de la contracción de las palabras *information* y *automatique* que traducido al español significa información automática dando el neologismo informática.[9]

Según el criterio básico de la Real Academia Española, informática es el "*Conjunto de conocimientos científicos y técnicas que hacen posible el tratamiento automático de la información por medio de ordenadores*".[10]

1.4.1. Breve historia de la Informática.

El origen de las máquinas de calcular está dado por el ábaco chino, éste era una tablilla dividida en columnas en la cual la primera, contando desde la derecha, correspondía a las unidades, las siguientes a las decenas, y así sucesivamente. A través de sus movimientos se podía realizar operaciones de adición y sustracción.

Otro de los hechos importantes en la evolución de la informática lo situamos en el siglo XVII, donde el científico francés Blas Pascal inventó una máquina calculadora llamada después como la "pascalina". Ésta sólo

[8] KATZ, Jorge M. *Los caminos hacia una sociedad de la información en América Latina y el Caribe*. United Nations Publications. 2003. Pág. 9.

[9] *LA INFORMÁTICA, PRESENTE Y FUTURO EN LA SOCIEDAD.* Volumen 15 de Ciencias experimentales y tecnología. Librería-Editorial Dykinson. 2006. Pág. 23.

[10] DICCIONARIO DE LA REAL ACADEMIA ESPAÑOLA, [en línea] [Consultado el día 23 de noviembre del año 2012]. Disponible en: <http://lema.rae.es/drae/?val=informatica>

servía para hacer sumas y restas, pero este dispositivo sirvió como base para que el alemán Leibnitz, en el siglo XVIII, desarrollara una máquina que, además de realizar operaciones de adición y sustracción, podía efectuar operaciones de producto y cociente. Ya en el siglo XIX se comercializaron las primeras máquinas de calcular. En este siglo el matemático inglés Babbage desarrolló lo que se llamó "Máquina Analítica", la cual podía realizar cualquier operación matemática y hasta podía usar funciones auxiliares, sin embargo seguía teniendo la limitación de ser mecánica.

Con el desarrollo de la segunda guerra mundial se construye el primer ordenador, el cual fue llamado Mark I y su funcionamiento se basaba en interruptores mecánicos.

En 1951 son desarrollados el Univac I y el Univac II (se puede decir que es el punto de partida en el surgimiento de los verdaderos ordenadores, que serán de acceso común a la gente).[11]

En 1981 la empresa IBM construyó y sacó a la venta el primer ordenador personal, el cual ya tenía integrado un microchip llamado procesador (Intel).

1.4.2. Generaciones de la informática.

Primera Generación: se desarrolla entre 1940 y 1952. Es la época de los ordenadores que funcionaban a válvulas y el uso era exclusivo para el ámbito científico/militar. Para poder programarlos había que modificar directamente los valores de los circuitos de las máquinas.

[11] MINELLI, Alejandra; Et al. *Breve historia de la informática*. Publicado 22 de octubre de 2001.

Segunda Generación: va desde 1952 a 1964. Ésta surge cuando se sustituye la válvula por el transistor. En esta generación aparecen los primeros ordenadores comerciales, los cuales ya tenían una programación previa que serían los sistemas operativos. Éstos interpretaban instrucciones en lenguaje de programación (Cobol, Fortran), de esta manera, el programador escribía sus programas en esos lenguajes y el ordenador era capaz de traducirlo al lenguaje máquina.

Tercera Generación: se dio entre 1964 y 1971. En esta generación se comienzan a utilizar los circuitos integrados; esto permitió por un lado abaratar costos y por el otro aumentar la capacidad de procesamiento reduciendo el tamaño físico de las máquinas. Por otra parte, esta generación es importante porque se da un notable mejoramiento en los lenguajes de programación y además, surgen los programas utilitarios.

Cuarta Generación: se desarrolla entre los años 1971 y 1981. Esta fase de evolución se caracterizó por la integración de los componentes electrónicos, y esto dio lugar a la aparición del microprocesador, que es la integración de todos los elementos básicos del ordenador en un sólo circuito integrado.

Quinta Generación: va desde 1981 hasta nuestros días (aunque ciertos expertos consideran finalizada esta generación con la aparición de los procesadores Pentium). Esta quinta generación se caracteriza por el surgimiento de la PC, tal como se la conoce actualmente.[12]

[12] GARCIA CUEVAS, Roque. Principios básicos de Informática. Librería-Editorial Dykinson. 2007. P 5 y sigs.

1.5. Concepto de Derecho Informático.

Aunque es difícil de conceptualizar por el variado número de peculiaridades y muy a pesar de los opuestos puntos de vista que pudieran provocar, se puede decir que el Derecho Informático es una rama de las ciencias jurídicas que contempla la informática como instrumento (informática jurídica) y como objeto de estudio (Derecho de la informática).

Julio Téllez Valdés define el derecho informático como "*el conjunto de normas, principios e instituciones que regulan las relaciones jurídicas emergentes de la actividad informática. También el derecho informático puede especificarse como: El conjunto de leyes, normas y principios aplicables a los hechos y actos derivados de la Informática*".[13]

1.6. Clasificación del Derecho informático.

Es notorio que la clasificación de dicho Derecho Informático obedece a dos vertientes fundamentales las cuales son la Informática Jurídica y el Derecho de la Informática.[14]

1.6.1. Informática jurídica.

Según Julio Téllez Valdés la Informática Jurídica "*es la técnica interdisciplinaria que tiene por objeto el estudio e investigación de los conocimientos de la Informática general, aplicable a la recuperación de información jurídica, así como la elaboración y aprovechamiento de los instrumentos de análisis y tratamiento de información jurídica, necesaria para lograr dicha recuperación*".[15]

[13] TÉLLEZ VALDÉS, Julio. Ob. Cit. Pág. 7.
[14] Ibídem, pág. 8.
[15] Ibídem, pág. 24.

Es decir que esta ciencia estudia la utilización de aparatos o elementos físicos electrónicos, como la computadora en el Derecho; en otras palabras es la ayuda que presta al desarrollo y aplicación del Derecho.

Esta materia se sub-clasifica de la siguiente manera: la Informática Jurídica Documentaria (almacenamiento y recuperación de textos jurídicos); Informática jurídica de control y gestión, (desarrollo de actividades jurídicos-adjetivas), y sistemas expertos legales o informática jurídica meta documentaria (apoyo en la decisión, educación, investigación, redacción y previsión del derecho).

1.6.2. Derecho de la Informática.

El Derecho de la Informática, se define como el conjunto de leyes, normas y principios aplicables a los hechos y actos derivados de la informática. En el mismo sentido lo define Vittorio Frossini cuando dice que derecho de la informática es la normativa dirigida a reglamentar el uso y a reprimir el abuso del nuevo poder informático en posesión y comercio de la información.[16]

En esta materia configuran los delitos informáticos, el teletrabajo, protección de datos personales, comercio electrónico, sociedad de la información, biotecnología Derecho, seguridad de la información, documento electrónico y firma digital.

[16] ORÚE CRUZ. José. Manual de Derecho mercantil. 2da edición. Editorial HISPAMER. Managua, Nicaragua. 2008. Pág. 231.

1.7. Importancia y contenido del Derecho informático.

En nuestra sociedad, la informática está presente en todas las actividades sociales, económicas y políticas, por lo que su adecuada regulación permite que el Derecho esté acorde con la realidad en forma sistemática, coherente e integral. El Derecho Informático estudia la regulación de la actividad informática y como tal, su importancia es creciente y su aplicación cada vez más necesaria.

El Derecho Informático tiene como objeto y contenido propio de estudio la regulación del fenómeno informático en cuanto a la regulación del bien informacional; la protección jurídica de los datos personales; el flujo de datos transfronterizo e internet; la protección jurídica de los programas de computación; los contratos informáticos; los delitos informáticos; el comercio electrónico y el valor probatorio de los soportes informáticos.[17]

1.8. Relación del Derecho Informático con otras ramas del Derecho.

1.8.1. Derecho Constitucional.

El Derecho Informático tiene una fuerte relación con el Derecho Constitucional, en cuanto la forma y manejo de la estructura y órganos fundamentales del Estado, de igual forma abarca lo referente a la Privacidad como un Derecho humano inherente a la dignidad del hombre, como instrumento de protección a los Derechos humanos y garantías generales de las personas que utilizan la informática. En otras palabras guarda una estrecha relación con la protección de datos personales.

[17] Ibídem.

1.8.2 . Derecho Penal.

Existe una amena relación, porque el Derecho Penal regula las sanciones para determinados hechos que constituyen situaciones ilícitas provocando violación de normas, y en este caso el Derecho Informático regula todos los hechos ilícitos con respecto a informática por cualquier medio tecnológico.

En el aspecto penal, la informática ha dado lugar a la creación de nuevos delitos que implican el uso del computador y los sistemas informáticos, este es punto de partida de la relación entre derecho y la informática en el campo penal El Consejo de Europa y el XV Congreso Internacional de Derecho señalaron como delitos informáticos los siguientes:

1. Fraude en el campo de la informática
2. Falsificación en materia informática
3. Sabotaje informático y daños a datos computarizados o programas informáticos
4. Acceso no autorizado a sistemas informáticos
5. Intercepción sin autorización
6. Reproducción no autorizada de un programa informático no autorizado
7. Espionaje Informático
8. Uso no autorizado de una computadora
9. Tráfico de claves informáticas obtenidas por medio ilícito
10. Distribución de virus o programas delictivos.[18]

[18] BELTRÁN FUENTES, Fernando Patricio; BELTRÁN FUENTES, Soraya Viviana. Derecho Informático. [en línea]. Publicado: Miércoles, 27 de mayo de 2009. Disponible en: http://www.derechoecuador.com/index.php?option=com_content&task=view&id=4980. (Consultado el 1 de abril de 2013.)

1.8.3. Derecho Administrativo.

El Derecho Informático se relaciona con el Derecho Administrativo a través de la regulación de la actividad administrativa automatizada.

Además regula las cuestiones relativas a la contratación de bienes y servicios informáticos de las administraciones públicas y la transferencia electrónica de fondos.

1.8.4. Derecho Mercantil.

Esta relación se observa a través de los derechos intelectuales y de los derechos industriales. Se contempla en la búsqueda de un instrumento jurídico adecuado para la protección del software.[19]Además se relaciona con el comercio que se hace efectivo por medios informáticos, los cuales merecen su respectiva regulación. En el mismo sentido mercantil, específicamente con el derecho bancario guarda una relación en cuanto a la protección de la banca electrónica, entiéndase esta como las transacciones que surgen por medio del comercio electrónico, así como también las transacciones que se hacen por medio de las tarjetas de crédito o débito.

1.8.5. Derecho Civil.

Brinda al Derecho Informático las normas básicas para configurar su propia estrategia, en la regulación de las tradicionales relaciones civiles.

Por medio de la informática toda persona natural o jurídica puede celebrar un contrato por medio de la red. Los contratos informáticos pueden referirse tanto a bienes (hardware o software) como a servicios informáticos (tales como mantenimiento preventivo, correctivo o evolutivo;

[19] Ibídem.

desarrollo y hospedaje de sitios web, prestación de servicios de certificación digital, etc.[20]

1.8.6. Derecho Internacional Público y Privado.

La relación entre el derecho internacional público con la informática, es que gracias a los avances tecnológicos se pueden llevar a cabo diferentes relaciones entre las entidades del estado con las de otros países.

El flujo de datos transfronterizo hace alusión a la libre circulación de datos entre países fronterizos, cabe resaltar que estos datos deben contar como una seguridad para que en ningún momento agreda la soberanía de otros países.[21]

La relación entre el Derecho internacional privado con la informática, es que por medio de la red se pueden llevar a cabo diferentes relaciones o transacciones entre las diferentes entidades internacionales. El mercado informático, es un mecanismo que busca dar facilidad en las transacciones mercantiles por medio de los crecientes avances tecnológicos.[22]

[20] MOJICA, Germán. Informática jurídica: relación con el Derecho civil- Contratos informáticos. [en línea] Publicado 6 de Junio del 2009. [Consultado el día 16 de noviembre del año 2012].Disponible en: <http://informaticajuridicausco.blogspot.com/2009/06/relacion-con-el-derecho-civil-contratos.html>
[21] Ibídem.
[22] Ibídem.

CAPÍTULO II: ANÁLISIS COMPARATIVO DEL COMERCIO ELECTRÓNICO DENTRO DE LA UNIÓN EUROPEA Y NICARAGUA

2.1. Introducción al Comercio Electrónico.

Antes de abordar los aspectos relativos al comercio electrónico daremos una breve introducción sobre esta modalidad de comercio, la cual consideramos necesaria para su mayor comprensión. El paradigma a seguir es el europeo.

El origen del proceso de integración comunitaria europea ha sido la conformación de un "mercado único" para todo el ámbito territorial de Comunidad Europea (CE en adelante) que busca ser lo más parecido a un mercado interno posible, el comercio electrónico es parte del mercado único y de libre circulación de mercancías de la Unión Europea. En este sentido recordemos la jurisprudencia:

"*tiene por objeto la eliminación de todos los obstáculos a los intercambios comunitarios con el fin de fundir los mercados nacionales en un mercado único estableciendo condiciones lo más próximas posibles a un auténtico mercado interior*".[23]

Las reglas formales del funcionamiento del mercado único están inspiradas en los principios de una economía abierta y de libre competencia.[24]

"*el mercado interior implicará un espacio sin fronteras interiores, en el que la libre circulación de mercancías, personas, servicios y capitales*

[23] TJCE, Sentencia de 5 de mayo de 1982. (C15/81)
[24] TCE, Arto. 4.

estará garantizada de acuerdo con las disposiciones del presente tratado"[25]

Como se puede observar el comercio electrónico de la CE parte de su mismo mercado interno, con gran participación de los medios tecnológicos existentes, dándole prelación al internet sobre los demás métodos.

Frente a tal fenómeno los Estados han tomado sus medidas. Para que el comercio electrónico viva y surta sus efectos, no basta sólo con la tecnología, sino que también es necesario un marco legal que vaya de la mano, para que regule dicha actividad comercial, de tal forma se estaría aplicando la legendaria locución latina *Ubi Societas Ibi Ius (donde hay sociedad, hay derecho)*. Marco regulatorio que para muchos países no es ajeno, como los países del viejo continente, que a su vez son los pioneros en la regulación de dicha materia.

La Unión Europea, como lo señala Emilio Suñé: "*...tiene una participación muy activa en el desarrollo de un Derecho de la Informática transnacional...*".[26] En la CE se creó la Directiva de comercio electrónico relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular el comercio electrónico, en el mercado interior esta Directiva es la encargada de crear un marco regulatorio sobre comercio electrónico. En la Directiva se toma en cuenta que el desarrollo del comercio electrónico traerá consigo la creación de nuevas fuentes de trabajo; siendo la finalidad de esta Directiva garantizar un elevado nivel de integración jurídica comunitaria con el objetivo de establecer un auténtico espacio sin fronteras en ámbito de los servicios de la sociedad de la

[25] TECE, Arto. 130. Inc. 2.

[26] SUÑELLINÁS, Emilio. Tratado de Derecho Informático Volumen I, Introducción y protección de datos personales. Ed. Universidad Complutense de Madrid. Madrid. 2000.pág.7.

información; además la directiva pretende crear confianza entre los usuarios y empresas mediante un marco regulatorio.[27]

Dicho fenómeno debe ser regulado, en sus diferentes aspectos, firma electrónica, siendo esta figura la que asegura la autenticidad de un mensaje digital que puede ser por ejemplo un documento electrónico. Una firma digital da al destinatario seguridad de que el mensaje fue creado por el remitente; y protección de datos, que es la garantía o la facultad de control de la propia información frente a su tratamiento automatizado o no. Estos marcos regulatorios son necesarios para que la actividad electrónica comercial sea eficiente y eminentemente segura, dando a la vez confianza a los usuarios o compradores, a utilizar este medio para adquirir sus enseres por ejemplo.

Nicaragua por lo tanto está iniciando en este aspecto en comparación a estos países. Actualmente en Nicaragua están aprobando leyes con relación al tema, tales como la ley 729, ley de firma electrónica, publicada en la Gaceta, diario oficial del 30 de agosto del 2010, y la nueva ley 787, ley de protección de datos personales, aprobada el 21 de marzo del 2012.En el presente Nicaragua todavía no tiene una ley especial que regule el comercio electrónico, solo tenemos un anteproyecto presentado por el Consejo Nicaragüense de Ciencia y Tecnología (CONICYT en adelante) en el 2006 que no se ha vuelto a poner en agenda en la Asamblea Nacional, este último lo tomaremos como referencia documentaria para la elaboración de este capítulo, ya que compararemos las Directivas que comprende el

[27] Directiva 2000/31/CE del Parlamento Europeo y del Consejo del 8 de junio del 2000 relativa a determinados aspectos jurídicos de los servicios de la sociedad de la Información, en particular el comercio electrónico en el mercado interior (Directiva Sobre El Comercio Electrónico)**.** Publicada Diario Oficial n° L 178 de 17/07/2000 p. 0001 – 0016.

comercio electrónico, firma electrónica, protección de datos con la legislación nicaragüense.

Cabe observar que Nicaragua ratificó el Acuerdo de Asociación (AdA en adelante) con la Unión Europea, el cual se basa en tres pilares fundamentales: dialogo político, cooperación y comercio. En sentido más estricto el AdA UE-Centroamérica supone la creación de un área de libre comercio entre las dos regiones.
Este acuerdo no puede pasar desapercibido por la importancia que tiene en este ámbito, el cual lo abordaremos en este capítulo.

Cabe aclarar que las leyes de los diferentes estados que se citan en el presente capitulo, son para ejemplificar como las Directivas han sido traspuestas en el interior de cada estado.

2.2. Concepto de comercio electrónico.

Antes de dar un concepto de comercio electrónico, resulta apropiado analizar los distintos aspectos y características que hacen la esencia misma de la forma de comercio. Las particularidades del comercio electrónico están dadas, tanto por la forma en que los actores interactúan, como por la nueva dimensión que adquieren las funciones de tiempo y espacio. Aunque el comercio electrónico guarda ciertas analogías con el comercio tradicional, dentro de su contexto, los actores pasan a cumplir nuevo roles, operando en un nuevo ámbito y siguiendo los lineamientos de nuevos principios.

“En el comercio electrónico no existe contacto físico directo entre los actores, las operaciones se realizan por medios electrónicos de comunicación, (…) en sentido más estricto, solo se consideran operaciones

de comercio electrónico aquellas realizadas enteramente por medios digitales de comunicación".[28]

Un concepto más lo podemos tomar del anteproyecto de ley del comercio electrónico de Nicaragua, presentado por CONICYT en el 2006, el cual en su artículo 3 lo define: "*Es toda actividad comercial celebrada, sea o no contractual, por medio de mensajes de datos*."[29]

Una definición que nos brinda la Comisión de Comunidades Europeas[30] en el año de 1997 es que el "*comercio electrónico consiste en realizar electrónicamente transacciones comerciales; es cualquier actividad en la que las empresas y consumidores interactúan y hacen negocios entre sí o con las administraciones por medios electrónicos*"[31]desde esta óptica se destacan actividades diversas tales como el comercio electrónico de bienes y servicios como tal; la trasferencia electrónica de fondos, la compraventa de acciones, las subastas comerciales (electrónicas), la protección jurídica sobre las contrataciones entre ausentes y la protección del consumidor frente a este nuevo modelo de comercio.

2.3. Origen y evolución del comercio electrónico

El caso de la Unión Europea, respecto al origen y desarrollo del Comercio Electrónico o deja de ser interesante si se considera que en los países que la integran existe un auge en comercializar por la red. Sin embargo, sus antecedentes en cuanto al uso de Internet difieren en tiempos respecto al

[28] GARIBOLDI, Gerardo. Comercio electrónico: conceptos y reflexiones básicas. BID-INTAL. 1999. Pág. 3.
[29] CONICYT, Secretaria Ejecutiva. Anteproyecto de ley de comercio electrónico. Junio 2006.
[30] Dir. 2000/31/CE DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 8 de junio de 2000
[31] [COM (97) 157 final], Bruselas, 16-04-1997. Comunicación de la comisión de las comunidades europeas al consejo, al parlamento europeo al comité económico social y al comité de las regiones sobre iniciativa europea del comercio electrónico pp. 7-10.

origen que tuvo en los Estados Unidos. Los orígenes del comercio electrónico está íntimamente relacionado con el fenómeno del internet.

En cuanto a su regulación, en 1995 estuvo presente la temática de la sociedad de la información en la Conferencia Ministerial del G7 y fue también tema central en el Consejo de Ministros de 1997.[32] Para el año de 1994, la propia Comisión aprobó un plan de actuación para la UE, en cuyos puntos principales se destacaron cuatro importantes áreas en relación al tema que nos ocupa: Desarrollar un marco normativo y jurídico; Fomentar la aplicación de las tecnologías de la información y las comunicaciones; Vigilar y analizar las consecuencias sociológicas, sociales y culturales de la sociedad de la información; Promover la sociedad de la información y el Papel de la UE en la esfera internacional.

El 17 de julio del año 2000 (Diario Oficial No. L178 de 17/07/2000 P. 0001-0016), entró en vigor en la Unión Europea la "Directiva 2000/31/CE del Parlamento Europeo y del Consejo, de 8 de junio de 2000, relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular el comercio electrónico en el mercado interior (Directiva sobre el comercio electrónico) en cuyo artículo primero se describe su objetivo como "(…)*el garantizar la libre circulación de los servicios de la sociedad de la información entre los estados miembros de la Unión Europea* (…).[33] Dicha Directiva, a la que posteriormente se dedicará un espacio exclusivo para su explicación, presupone entre muchas otras cuestiones la necesidad de crear un marco jurídico que garantice la libre circulación de los servicios de la sociedad de la información entre

[32] BRIZ, Julián; LASO, Isidro. Internet y Comercio Electrónico. 2da edición. Ediciones Mundi-Prensa. Madrid, España. 200. Pág. 232.
[33] DAVARA RODRÍGUEZ, Miguel Ángel. Manual de Derecho Informático. Ed. Aranzadi. Madrid. 2001, p. 221.

Estados miembros y no armonizar el campo de la legislación penal en sí, asimismo, hace referencia a importantes temas como la protección de los consumidores, en cuanto a la publicidad, la información o la comunicación comercial que pueden ser tanto deseables como indeseables para los mismos. Resulta pertinente mencionar que la Directiva 2000/31/CE representa para la Unión Europea el inicio de la evolución jurídica en materia de comercio electrónico entre sus Estados miembros, de donde se desprende uno de los temas de mayor impacto en la materia, como lo es "la determinación del régimen jurídico aplicable al comercio electrónico intracomunitario".[34]

2.4. Aspectos legales del comercio electrónico.

Dentro del sistema de normas y de los actos jurídicos celebrados al amparo de la UE, destacan ciertos instrumentos legales de origen directamente institucional o comunitario, denominados así por ser derivados de la actividad "normativa" propia de la Unión, diferenciada de los actos derivados de las estructuras de cooperación que comparten con las acciones comunitarias su origen institucional que se producen en un marco jurídico con características diferentes a las de los Tratados comunitarios. De esta forma, dentro del sistema de normas de la Unión Europea destacan los Reglamentos, las Directivas y las Decisiones. Las denominadas Directivas, son instrumentos jurídicos reguladores emanados del derecho comunitario que tienen una obligatoriedad parcial "que deja en manos de las autoridades nacionales la elección de la "forma y los medios" de darle efectividad en el orden interno, es decir, requiere la intermediación estatal, carece por

[34] DE MIGUEL, Pedro. Directiva sobre comercio electrónico, determinación de la normativa aplicable a las actividades transfronterizas, en la *Revista de la Contratación Electrónica*. Ed. Editora de Publicaciones Científicas y Profesionales (EDICIP). Cádiz. 2001. p. 4.

definición de aplicabilidad directa (y, en consecuencia, de "efecto directo").[35]

Siendo la UE un espacio común en donde las fronteras geográficas han quedado marginadas y transformadas de su significado original, su espacio físico queda sin delimitación alguna ante el libre tránsito que los habitantes de la región tienen por el simple derecho de ser parte de esa comunidad. Así, el pertenecer a una región conformada por diferentes países pero legislada con normas comunes para todos los que la conforman unifica los criterios y permite a todos ejercer los mismos derechos y cumplir con un mismo tipo de obligaciones.

Ante el repentino auge que las tecnologías de información provocaron en la recién pasada década de los noventa, las legislaciones estatales se dieron a la tarea de regular la mayor parte de los temas en que dichas tecnologías estaban inmersas, por medio de normas que fueran adecuadas a la situación concreta que directamente requería de una regulación en su momento. Uno de los temas que vio rebasado su marco jurídico ante el desarrollo de la tecnología fue el del comercio electrónico.

Los motivos antes señalados fueron parte de las decisiones tomadas por la Unión Europea para emitir la Directiva 2000/31/CE del Parlamento Europeo y del Consejo, con fecha 8 de junio de 2000, relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular el comercio electrónico en el mercado interior. A este documento se le conoce popularmente como Directiva sobre el

[35] MANGAS MARTÍN, Araceli; LIÑÁN NOGUERAS, Diego; Instituciones y Derecho de la Unión Europea; Editorial Tecnos; Madrid, España; 6ta. edición, 2010; pp. 351.

comercio electrónico, fue publicada en Diario Oficial de las Comunidades Europeas (DOCE) L178 de 17 de julio de 2000, P. 0001-0016, y representa un documento valioso y vanguardista en la regulación de la materia del comercio electrónico.

En la parte introductoria de la Directiva 2000/31/CE, conocida como directiva del comercio electrónico, se indica que el desarrollo de los servicios de la sociedad de la información en la Comunidad Europea tiene una serie de obstáculos jurídicos que impiden un buen funcionamiento del mercado interior y hacen poco atractivo el ejercicio de la libertad de establecimiento y la libre circulación de servicios. Como vemos conviene en suprimir los obstáculos al coordinar ciertas legislaciones nacionales en la medida de lo necesario para el buen funcionamiento del mercado interior es por ello que el objetivo principal de la directiva en cuestión, se deriva del fin que tiene la Unión Europea en cuanto a "...*crear una unión cada vez más estrecha entre los Estados y los pueblos europeos, así como asegurar el progreso económico y social*..."[36] por consiguiente esta misma directiva en el considerando 1señala también que conforme al apartado 2 del artículo 14 del Tratado de la Unión Europea "... *el mercado interior supone un espacio sin fronteras interiores, en el que la libre circulación de mercancías y servicios y la libertad de establecimiento están garantizadas. El desarrollo de los servicios de la sociedad de la información en el espacio sin fronteras interiores es un medio esencial para eliminar las barreras que dividen a los pueblos europeos*".[37]El artículo 1, sobre Objetivo y ámbito de aplicación, de la Directiva 2000/31/CE, es claro al señalar que lo que pretende "*es contribuir al correcto funcionamiento del*

[36] Véase considerando 1 de la Directiva 2000/31/CE del Parlamento Europeo y del Consejo, de fecha 8 de junio de 2000.
[37] Ibídem.

mercado interior garantizando la libre circulación de los servicios de la sociedad de la información entre los Estados miembros".[38] Esta norma comunitaria, señala el mismo artículo 1 inciso 5 no se aplicará en materia de fiscalidad ni a cuestiones relacionadas con servicios de la sociedad de la información que estén incluidas en la Directiva 95/46/CE del Parlamento Europeo y del Consejo de 24 de octubre de 1995 relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y en la Directiva 97/66/CE del Parlamento Europeo y del Consejo de 15 de diciembre de 1997 relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las telecomunicaciones.

El artículo 2 de la citada Directiva define algunos conceptos claves para entender y considerar mejor sus alcances. El concepto "servicios de la sociedad de la información" se encuentra definido en la Directiva 98/48/CE del Parlamento Europeo y del Consejo de 20 de julio de 1998 que modifica la Directiva 98/34/CE del Parlamento Europeo y del Consejo de 22 de junio de 1998 por la que se establece un procedimiento de información en materia de las normas y reglamentaciones técnicas, en las actividades que por su naturaleza se necesita la intervención de los oficios notariales, en cuyo artículo 1, apartado 2, señala la palabra "servicio" como "*todo servicio de la sociedad de la información, es decir, todo servicio prestado normalmente a cambio de una remuneración, a distancia, por vía electrónica y a petición individual de un destinatario de servicios*".[39]

Por otra parte, sobre la información general exigida contemplada en el artículo 5 de la Directiva 2000/31/CE, indica que independientemente de

[38] Ibídem, Arto 1.
[39] Ibídem.

otros requisitos en materia de información contemplados en el Derecho comunitario, los Estados miembros garantizarán que el prestador de servicios permita tanto a los destinatarios del servicio como a las autoridades competentes acceder con facilidad, directa y permanentemente a datos como: el nombre del prestador de servicios, es decir quién es el proveedor de los servicios y la dirección geográfica en donde se encuentre establecido, en otras palabras el lugar donde la empresa ejerce sus operaciones, las señas que permitan localizar al prestador de servicios en donde se incluya su dirección de correo electrónico, con el objetivo para que exista mayor confianza entre el destinatario de los servicios y el proveedor de estos, mediante la comunicación. También deberán tenerse los datos relativos al registro mercantil u otro registro público del prestador de servicios (en el caso que este registrado), así como aquellos de la autoridad de supervisión si la actividad está sujeta a régimen de autorización. En el caso que sean servicios profesionales los que se ofrezcan, además de los requisitos anteriores, deberán presentar certificado de que es parte de un colegio profesional o institución similar, además de esa información deberán de presentar de manera clara y sin ambigüedades si están incluidos los impuestos y los gastos de envío.[40] En este último aspecto podemos hacer una comparación con la Ley 182, Ley De Protección Al Consumidor la cual manifiesta que "*Los precios de los bienes y servicios deberán incluir el valor de los mismos y toda clase de impuestos o cargas a que se encuentren afectos y que sean a cargo del consumidor….*"[41]

[40] Ibídem. Arto. 5.

[41] LEY 182, LEY DE DEFENSA DE LOS CONSUMIDORES. Arto. 15. Publicada en la Gaceta Diario Oficial No. 213 del 14 de noviembre de 1994.

En la Directiva hace mención sobre las comunicaciones comerciales, entendiendo esta como "*todas las formas de comunicación destinadas a proporcionar directa o indirectamente bienes, servicios o la imagen de una empresa, organización o persona con una actividad comercial, industrial, artesanal o de profesiones reguladas*".[42] O mejor conocidas como "*spam*". En su artículo 6 dice que será claramente identificable la persona física o jurídica en nombre de la cual se hagan dichas comunicaciones, las ofertas promocionales, como los descuentos, premios y regalos cuando estén claramente permitidos en el Estado deberán ser claramente identificables como tales y deberán presentarse de manera clara e inequívocas las condiciones que deban cumplirse para acceder a ellos.[43] Esto con el fin de aumentar la confianza del consumidor y garantizar unas prácticas comerciales leales, mientras que las comunicaciones comerciales por correo electrónico deben ser reconocidas claramente por el destinatario desde su recepción.

Por otro lado, la Directiva 2002/58/CE[44]prohíbe el envío de mensajes comerciales no solicitados (mensajes de texto o multimedia a terminales fijos o móviles) salvo que se haya obtenido previamente el consentimiento del abonado. En el mismo sentido se manifiesta la ley de servicios de la sociedad de la información y de comercio electrónico de España (LSSI en adelante) la cual prohíbe el envío de comunicaciones publicitarias o promocionales por correo electrónico y otro medio equivalente si previamente no se ha contado con el consentimiento expreso de los destinatarios, salvo que exista una relación contractual previa entre el emisor y el receptor de la comunicación y su envío concierna sobre

[42] DIRECTIVA 2000/31/CE. Ob. Cit. Arto. 2.
[43] LEY 182. Ob. Cit. Arto. 19, 20.
[44] DIRECTIVA 2002/58/CE Ob. Cit. Arto. 13.

productos o servicios de la empresa similares a los que inicialmente fueron objeto de contratación con el cliente. En todo caso, señala la LSSI, el prestador deberá ofrecer al destinatario la posibilidad de oponerse al tratamiento de sus datos con fines promocionales mediante un procedimiento sencillo y gratuito, tanto en el momento de recogida de los datos como en cada una de las comunicaciones comerciales que le dirija.[45]

Sobre la realización de un pedido, el artículo 11 de la Directiva determina las garantías que deben proporcionar los Estados miembros a los consumidores, exceptuando los casos cuando las partes no sean consumidores y así lo acuerden, los casos en que un destinatario de un servicio realice su pedido por vía electrónica, así el prestador de servicios debe acusar recibo del pedido del destinatario sin demora indebida y por vía electrónica, asimismo, señala que el prestador de servicios debe poner a disposición del destinatario del servicio los medios técnicos adecuados, eficaces y accesibles que le permitan identificar y corregir los errores de introducción de datos, antes de realizar el pedido, excepto si esto lo acuerdan las partes que no son consumidores.[46]

Un aspecto más a tratar es el alojamiento de datos el cual es regulado en artículo 14 de la Directiva el cual manifiesta que el prestador de servicios de almacenamiento de datos no puede ser responsable de los datos almacenados a petición del destinatario, siempre y cuando el prestador de servicios no tenga conocimiento efectivo que los datos albergados son ilícitos y si en caso que se diera el conocimiento y el prestador actúe con prontitud para retirar los datos o hacer que sea imposible acceder a ellos, esta artículo como vemos está enfocado específicamente a los servidores

[45] LEY 34/2002, Arto 21 de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico. Publicado en BOE núm. 166 el 12 de julio del 2002.
[46] DIRECTIVA 2000/31/CE del Parlamento Europeo y del Consejo, Ob. Cit. Arto. 11.

públicos que son muy famosos en la actualidad. En este sentido podemos recurrir a la Jurisprudencia "*debe interpretarse en el sentido de que se aplica al operador de un mercado electrónico cuando éste no desempeñe un papel activo que le permita adquirir conocimiento o control de los datos almacenados.*

Este operador desempeña tal papel cuando presta una asistencia consistente, en particular, en optimizar la presentación de las ofertas de venta en cuestión o en promover tales ofertas.

En el supuesto de que el operador del mercado electrónico no haya desempeñado un papel activo en el sentido descrito en el anterior párrafo y, en consecuencia, a su prestación del servicio le resulte de aplicación lo dispuesto en el artículo 14, apartado 1, de la Directiva 2000/31, ese operador no podrá, no obstante, en un asunto que puede concluir con una condena al pago de una indemnización por daños y perjuicios, acogerse a la exención de responsabilidad prevista en esa disposición cuando haya tenido conocimiento de hechos o circunstancias a partir de los cuales un operador económico diligente hubiera debido constatar el carácter ilícito de las ofertas de venta en cuestión y, en caso de adquirir tal conocimiento, no haya actuado con prontitud de conformidad con lo establecido en el apartado 1, letra b), de dicho artículo 14".[47]

En otro sentido cabe destacar que Nicaragua como ya lo hemos dicho, no tiene una ley especial que regule el comercio electrónico. El AdA con su aprobación creemos que aportará grandes beneficios para la implementación del comercio electrónico, tanto en la parte técnica, como la parte legal, hacemos esta observación basándonos en el artículo 56 del acuerdo el cual taxativamente expone "*que la cooperación incluye*

[47] TJUE, Sentencia del 12 de julio de 2011.

asistencia técnica y legal…"[48] para su mejor implementación.

2.5. Fundamentos del comercio electrónico

2.5.1. Contratación electrónica

"*… a medida que avanza la informática y penetra en la vida cotidiana de las personas, más atrás se queda el derecho vigente sin dar respuesta a la nueva realidad*"[49] esta cita refleja claramente la situación del derecho informático frente a este fenómeno, de igual manera refleja el ambiente actual de la contratación electrónica en Nicaragua, la cual en todo caso sería regulado por el Código Civil.

Tradicionalmente el intercambio comercial tanto en el ámbito nacional como en el ámbito internacional se ha realizado por medio de actos concretos que jurídicamente se denominan contratos. Estos documentos legales se utilizan también durante el intercambio comercial que se realiza a través de medios electrónicos y tanto la forma tradicional como la electrónica de los contratos, como formas de negociación, van a estar reguladas por las normas emanadas del Derecho Privado, específicamente del Derecho Civil y del Derecho Mercantil.

Será necesario hacer algunas definiciones que acerquen el concepto tradicional de contrato a la moderna noción de contratación electrónica y reconocer así las nuevas características que identifican este último concepto. Para ello se tomarán en cuenta algunas definiciones tomadas de la doctrina, concepto del código civil nuestro y de países europeos.

[48] ACUERDO, por el que se establece una Asociación entre la Unión Europea y sus Estados miembros, por un lado, y Centroamérica, por otro. Ob. Cit. Arto. 56.
[49] FERNÁNDEZ FERNÁNDEZ, Rodolfo. Contratación electrónica: la prestación del consentimiento en Internet. Ed. J.M. Bosch. Editor, Barcelona 2001. Pág. 17.

En relación a la definición utilizada en el Código Civil define contrato "*acuerdo de dos o más personas para constituir, regular o aclarar entre las mismas un vínculo jurídico*"[50], en tanto el artículo 1254, del código civil español, define la palabra contrato "*el contrato existe desde que una o varias personas consienten en obligarse, respecto de otra u otras, a dar alguna cosa o prestar algún servicio*."[51]Brenes Córdoba los sintetiza diciendo "… *convenio de dos o más personas para constituir una obligación*"[52]

Como vemos el contrato es el generador de las obligaciones en el acto de creación, transmisión y extinción de los derechos reales, pero al tratarse de los medios electrónicos aunque éstos no sean el instrumento tradicional sí puede darse el consentimiento a través de ellos y por ende generar las obligaciones jurídicas. La particularidad del contrato electrónico en contraste con el contrato tradicional radica en el uso de los medios electrónicos para la formación de la voluntad, es decir, el elemento diferenciador es el medio electrónico en sí, informático o telemático.

Al respecto se puede tomar en consideración lo que platea el Código Civil nuestro, acerca de la forma de mostrar el consentimiento el cual manifiesta"… *la manifestación puede ser hecha de palabras, por telégrafo, teléfono, por escrito por hechos de que necesariamente se deduzca*"[53] Brenes Córdoba en este sentido dice "*los contratos que se celebran en esa*

[50] MORALES, Carlos A. Et. Al. Código Civil de la República de Nicaragua, tomo II. Versión comentada. Arto. 2435. 3ra edición. Casa Editorial Carlos Heuberger. Managua, Nicaragua. 1933.
[51] REAL DECRETO, Ley Código Civil. Arto. 1254. Publicada en Boletín Oficial del Estado, núm. 206 de 25 de julio de 1889. España.
[52] BRENES CORDOBA, Alberto. Tratado de los contratos. 6ta ed. Editorial Juricentro. San José, Costa Rica. 2009. Pág. 39
[53] CÓDIGO CIVIL DE LA REPUBLICA DE NICARAGUA, tomo II. Ob. Cit. Arto 2448.

forma estatuye el código de obligaciones suizo[54] *en su artículo 4º, que "se reputan hechos entre presentes si las partes o sus mandatarios han estado personalmente en comunicación" regla perfectamente aceptable como doctrina general y que no discuerda con lo estatuido en el artículo 1008 del código civil nuestro."*[55]Cabe aclarar que el artículo 2448 de nuestro código civil fue extraído de código civil de Costa Rica. En el mismo sentido podemos agregar que la ley de Servicios de la Sociedad de la Información española en su artículo 27 inciso 3, perteneciente al Título IV, sobre Contratación Electrónica, que indica: *"Sin perjuicio de lo dispuesto en la legislación específica, las ofertas o propuestas de contratación realizadas por vía electrónica serán válidas durante el periodo que fije el oferente o, en su defecto, durante todo el tiempo que permanezcan accesibles a los destinatarios del servicio."*[56]

La Directiva 2000/31/CE del Parlamento Europeo y del Consejo aunque no menciona literal y directamente sobre lo que es un contrato electrónico, sí promueve el uso de los mismos en su artículo 9 inciso 1 que indica "*los Estados miembros garantizaran en particular que el régimen jurídico aplicable al proceso contractual no entorpezca lo utilización real de los contratos por vía electrónica, ni conduzca a privar efecto y validez jurídica a este tipo de contratos en razón de su celebración por vía electrónica*"[57], Para este caso, no todos los contratos pueden ser considerados ya que la propia Directiva en el mismo artículo 9 excluye algunos de ellos, tales como los contratos inmobiliarios, aquellos contratos que requieran de la

[54] Cabe aclarar que Suiza lo tomamos como referencia doctrinal, acuñada por el señor Brenes Córdoba, en ningún caso lo tomamos como análisis comparativo, ya que Suiza no forma parte de la Unión Europea.
[55] BRENES CORDOBA, Alberto. Ob. Cit. Pág. 57.
[56] LEY DE SERVICIOS DE LA SOCIEDAD DE LA INFORMACIÓN Y DE COMERCIO ELECTRÓNICO (LSSI), Ob. Cit. Arto. 27. Inc. 3.
[57] DIRECTIVA 2000/31/CE. Ob. Cit. Arto. 9.

intervención de tribunales, autoridades públicas o profesionales que ejerzan funciones públicas como los notarios, los contratos en materia de familia o de sucesiones.[58]

En artículo 10 de la directiva expresa de la información exigida para que se celebre el contrato siendo estos "los *pasos técnicos que deben darse para celebrar el contrato; si el prestador de servicios va registrar o no el contrato y si esta va ser accesible; los medios técnicos para identificar y corregir los errores de introducción de datos antes de efectuar el pedido; las leguas ofrecidas para la celebración del contrato. Además el prestador de servicios deberá indicar los códigos de conducta a los cuales se apega y deberá facilitar la manera de consultarlos electrónicamente, para mayor confianza con los usuarios"*.[59]

Respecto a la naturaleza jurídica del contrato electrónico celebrado a través de Internet, algunos autores lo consideran como un contrato a distancia, sin embargo, es evidente que en general todo negocio jurídico electrónico se perfecciona a distancia, éste tiene ciertas modalidades, características y condicionantes totalmente novedosas que lo hacen particular y diferente al tradicional contrato a distancia, cuyas modalidades peculiares tienen relación con la expresión del consentimiento, la producción de sus efectos, los medios de comunicación, entre otros rasgos que destacan su diferencia. Sin embargo, aunque en su naturaleza jurídica al contrato electrónico se le considere como un contrato a distancia y sean referidos ambos como sinónimos, *a priori* podría no ser así porque desde un punto de vista estrictamente jurídico el contrato electrónico puede considerarse como una subespecie del contrato a distancia.

[58] Ibídem.
[59] Ibídem.

Si se considera a la contratación electrónica como una contratación a distancia, en el caso de la primera estarán los aspectos típicos de la segunda si se contrata en tiempo real, aunque no concurran voz e imagen, no obstante de que las partes contratantes se encuentren conectadas simultáneamente a un mismo sitio de la red y expresando sus declaraciones de voluntad en línea.[60] En la misma perspectiva podríamos dar un concepto de contrato a distancia definido en el artículo 2 de la Directiva 97/7/CE del Parlamento Europeo y del Consejo de 20 de mayo de 1997, relativa a la protección de los consumidores en materia de contratos a distancia, como "*todo contrato entre un proveedor y un consumidor sobre bienes o servicios celebrado en el marco de un sistema de ventas o de prestación de servicios a distancia organizado por el proveedor que, para dicho contrato, utiliza exclusivamente una o más técnicas de comunicación a distancia hasta la celebración del contrato, incluida la celebración del propio contrato*".[61]

2.5.2. Firma electrónica

La seguridad en internet consiste en implementar mecanismos para que cuando se reciba un mensaje se realice una transacción por medios electrónicos, se asegure la integridad del contenido y la identidad del remitente y del receptor. Las contraseñas y palabras claves ya no son un mecanismo suficientemente fiable y seguro, ya que estas pueden ser interceptadas durante su transmisión. En este sentido conviene implementar un método más seguro a la hora de hacer una transacción por medio

[60] MORENO NAVARRETE, Miguel Ángel. DERECHO-e Derecho del Comercio Electrónico. Ed. Marcial Pons. Madrid. 2002. Pág. 35.

[61] DIRECTIVA 97/7/CE del Parlamento Europeo y del Consejo, de 20 de mayo de 1997, relativa a la protección de los consumidores en materia de contratos a distancia. Publicada Diario Oficial n° L 144 de 04/06/1997 pp. 0019 – 0027. Arto. 2.

electrónico, es ahí donde la firma electrónica aparece para dar mayor seguridad a la hora de hacer este tipo de gestión.

En la forma que abordaremos la firma electrónica será desde el punto de vista a su utilidad en el comercio electrónico.

La firma digital es una especie de firma electrónica. Al igual que la electrónica, es un método basado en medios electrónicos para la identificación y vinculación de una persona.[62] Desde este punto de vista hacemos la diferencia entre firma digital y firma electrónica, siendo la primera una especie de la segunda. La firma electrónica puede abarcar la tarjeta de coordenadas, usuario y contraseñas y la misma firma digital.

Un concepto que nos ofrece la Directiva 1999/93/CE es que *los datos en forma electrónica anexo a otros datos electrónicos o asociados de manera lógica con ellos, utilizados como medio de autenticación.*[63]En el mismo sentido se expresa el concepto que nos da la ley de firma electrónica de Nicaragua diciendo que *son datos electrónicos integrados a un mensaje de datos o lógicamente asociados a otros datos electrónicos, que pueden ser utilizados para identificar al titular en relación con el mensaje de datos e indicar que el titular aprueba la información contenida en el mensaje de dato.*[64]En ambas definiciones son univocas, diciendo que la firma digital es aquella que son datos integrados a un mensaje electrónico para su identificación. Cabe destacar que la definición que nos da la ley probablemente pudo ser copia del concepto que proporciona la ley modelo

[62] TORRES ÁLVAREZ, Hernán. El sistema de seguridad jurídica en el comercio electrónico. Fondo Editorial PUCP. 2005. Pág. 78.
[63] DIRECTIVA 1999/93/CE del Parlamento Europeo y del Consejo, de 13 de diciembre de 1999, por la que se establece un marco comunitario para la firma electrónica. Publicada Diario Oficial n° L 013 de 19/01/2000 p. 0012 – 0020. Arto. 2.
[64] LEY 729, LEY DE FIRMA ELECTRÓNICA. Publicada en la Gaceta Diario Oficial el 30 de agosto del 2006. Arto. 3.

de la Comisión de Las Naciones Unidas sobre El Derecho Mercantil Internacional (CNUDMI)sobre Firma Electrónica del 2001la cual dice "... *los datos en forma electrónica consignados en un mensaje de datos, o adjuntados o lógicamente asociados al mismo, que puedan ser utilizados para identificar al firmante en relación con el mensaje de datos e indicar que el firmante aprueba la información recogida en el mensaje de datos*".[65]

El objeto de la ley es otorgar valor jurídico a la firma electrónica[66] de igual forma la ley de España el decreto ley Decreto-Ley 14/1999, sobre firma electrónica, le da "…*el reconocimiento de su eficacia jurídica…*"[67] el valor jurídico que tiene es el mismo que la firma manuscrita, por lo tanto "*será admisible como medio de prueba en el proceso judicial o administrativo*"[68]es muy importante dar a conocer que la firma que tiene este privilegio será la firma certificada. En el considerando 21 de la Directiva 1999/93/CE dice al respecto "*Para contribuir a la aceptación general de los métodos de autenticación electrónica, debe garantizarse la admisibilidad de la firma electrónica como prueba en procedimientos judiciales en todos los Estados miembros…*"[69] en el artículo 5 de la misma apartado segundo manifiesta que "*no se niegue eficacia jurídica, ni admisibilidad como prueba en los procesos judiciales por el mero hecho… no se base en un certificado expedido por un proveedor de servicios de certificado acreditad; no esté creada por un dispositivo seguro de creación*

[65] LEY MODELO DE LA CNUDMI SOBRE FIRMAS ELECTRÓNICAS CON LA GUÍA PARA SU INCORPORACIÓN AL DERECHO INTERNO 2001. [en línea] [Consultado el 3 de abril de 2013] Disponible en: <www.uncitral.org/pdf/spanish/texts/electcom/ml-elecsig-s.pdf>

[66] Ibídem. Arto. 1.

[67] REAL DECRETO-LEY 14/1999, Arto. 1. de 17 de septiembre, sobre firma electrónica. Publicada en Boletín Oficial del Estado, núm. 224 de 18 de septiembre de 1999..

[68] LEY 729. Ob. Cit. Arto. 6.

[69] DIRECTIVA 1999/93/CE. Ob. Cit. Considerando 21.

de firma."[70] De tal manera que no se podría alegar como excepción que la firma electrónica no es válida por el simple hecho de que no tiene un certificado conocido.

Algo interesante es el planteamiento de la directiva 1999/93/CE que reconoce las firmas digitales provenientes de terceros países siempre y cuando cumplan con "*que el proveedor de servicios de certificación cumpla los requisitos establecido en la presente Directiva y haya sido acreditada en el marco de un sistema voluntario de acreditación establecido en un Estado miembro"*[71]de igual forma en la ley de firma electrónica, reconoce los certificados del extranjero diciendo "*todo certificado de firma expedido en el extranjero será reconocido por la instancias rectoras de acreditación de firma electrónica, en los mismo términos y condiciones establecidos en la presente ley…"*[72] de esta manera se estaría beneficiando el comercio internacional, ya que dándole valor jurídico a una firma electrónica proveniente de otros países, se podría dar seguridad de que, por ejemplo un contrato del exterior, es válido en Nicaragua y viceversa.

2.5.3. Protección de datos

Es necesario, antes de entrar en detalle a estudiar la protección jurídica que se ofrece a los datos de carácter personal, hacer un breve repaso sobre los orígenes de este Derecho y de su intrínseca conexión con el Derecho a la Intimidad regulado en el artículo 26 de la Constitución nicaragüense. La cual reza "*toda persona tiene derecho: a su vida privada, a la inviolabilidad de su domicilio, su correspondencia y sus comunicaciones*

[70] DIRECTIVA 1999/93/CE. Ob. Cit. Arto. 5.
[71] Ibídem. Arto. 7.
[72] LEY 729. Ob. Cit. Arto.11.

de todo tipo; al respeto a su honra y reputación; a toda información que sobre ella hayan registrado las autoridades estatales, así como el derecho de saber por qué y con qué finalidad tiene esa información…"[73]del mismo modo la constitución de España se manifiesta diciendo "…*La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos."*[74] Como es de notarse en estos dos países el origen de la protección de datos es constitucional.

Como concepto tomaremos el que nos brinda la ley 787, Ley de Protección de Datos Personales la cual manifiesta "*Es toda la información sobre una persona natural o jurídica que la identifica o la hace identificable"* como datos personales informáticos "*Son los datos personales tratados a través de medios electrónicos o automatizados"* la misma ley hace una distinción de datos personales sensibles "*Es 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."*[75]La Directiva 95/46/CE en su artículo 2, sobre las definiciones cambia el nombre de datos personales informáticos por tratamiento de datos personales diciendo "*cualquier operación o conjunto de operaciones, efectuadas o no mediante procedimientos automatizados, y aplicadas a datos personales, como la recogida, registro, organización,*

[73] CONSTITUCIÓN POLÍTICA DE LA REPÚBLICA DE NICARAGUA. 1ra Edición. Jurídica. 2009. Arto. 26.
[74] CONSTITUCIÓN POLÍTICA DEL REINO DE ESPAÑA. Arto. 18 [en línea] [Consultado el 4 de abril de 2013]. Disponible en: <http://www.dat.etsit.upm.es/~mmonjas/politica/ce.html>
[75] LEY DE PROTECCIÓN DE DATOS. LEY 787, Arto. 3. Publicada en La Gaceta No. 61 del 29 de marzo del 2012.

conservación, elaboración o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma que facilite el acceso a los mismos, cotejo o interconexión, así como su bloqueo, supresión o destrucción"[76]como se observa en la Directiva, se hace más especifica la definición que la nuestra.

La Directiva 95/46/CE constituye el texto de referencia, a escala europea, en materia de protección de datos personales. Crea un marco regulador destinado a establecer un equilibrio entre un nivel elevado de protección de la vida privada de las personas y la libre circulación de datos personales dentro de la UE. Con ese objeto, la Directiva fija límites estrictos para la recogida y utilización de los datos personales y solicita la creación, en cada Estado miembro, de un organismo nacional independiente encargado de la protección de los mencionados datos. En Nicaragua está la Ley 787, Ley De Protección De Datos. Publicada en La Gaceta No. 61 del 29 de Marzo del 2012, la cual en su considerando VI dice que se necesita mantener la competitividad del país en actividades comerciales donde la tutela de los datos personales es preocupación central. En el artículo 2 manifiesta sobre el ámbito de aplicación "*las disposiciones de la presente ley serán aplicables al tratamiento de los datos personales que se encuentran en los ficheros de datos públicos y privados*."[77] Pero no especifica la jurisdicción, pensamos que es una laguna legislativa. Veamos lo que dice la Directiva al respecto el artículo 28, apartado 6, implica que las autoridades nacionales de protección de datos puedan ejercer sus poderes cuando al tratamiento de datos personales realizado en su jurisdicción se aplique el Derecho de

[76] DIRECTIVA 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos. Publicada Diario Oficial n° L 281 de 23/11/1995 p. 0031 – 0050. Arto. 2.
[77] LEY 787. Ob. Cit. Arto. 2.

protección de datos de otro Estado miembro. Pero ¿qué pasa si se encuentra en un tercer país? el artículo 4, apartado 1, letra c), procura garantizar el derecho a la protección de datos personales contemplado por la Directiva aun cuando el responsable del tratamiento no esté establecido en el territorio de la Unión Europea, pero el tratamiento de los datos personales tenga una clara conexión con dicho territorio, como se indica en el considerando 20 "*Considerando que el hecho de que el responsable del tratamiento de datos esté establecido en un país tercero no debe obstaculizar la protección de las personas contemplada en la presente Directiva; que en estos casos el tratamiento de datos debe regirse por la legislación del Estado miembro en el que se ubiquen los medios utilizados y deben adoptarse garantías para que se respeten en la práctica los derechos y obligaciones contempladas en la presente Directiva"*[78]En síntesis este considerando expresa que cuando los datos estén albergados en un tercer país no es motivo de obstaculizar la aplicación de la Directiva en mención ya que estos casos serán resueltos por la legislación del Estado donde están los medios utilizados, o sea donde está surtiendo los efectos. Estas cuestiones presentan particular importancia en entornos de red, como la computación en la nube, o en el contexto de compañías multinacionales.

En el artículo12 de la ley de protección de datos habla sobre habla sobre la confidencialidad en el primer párrafo expresa que el responsable del tratamiento de datos está obligado a mantener el secreto profesional, la que también se estará obligado aun cuando "*después de finalizada su relación con el responsable del fichero de datos*".[79] En este sentido se pronuncia el artículo 16 de la Directiva. El mismo artículo en el segundo párrafo se manifiesta sobre las políticas de privacidad, el cual el responsable de los

[78] DIRECTIVA 95/46/CE. Ob. Cit. Considerando 20.
[79] LEY 787. Ob. Cit. Arto. 12.

ficheros tiene que notificar sobre los modificaciones a su titular. Se refiere al derecho que tiene el titular de solicitar información relativa a sus ficheros de datos, el registro que lleve a efecto estos datos brindara la información de manera gratuita.

Un aspecto relevante que toma la ley es el derecho al olvido, este derecho tiene bastante relación con el habeas data y la protección de datos, esta se puede definir como el derecho que tiene el titular de un dato personal borrar, bloquear o suprimir información personal que se considera obsoleta por el transcurso del tiempo o que de alguna manera afecta el libre desarrollo de alguno de sus derechos fundamentales, en ciertos casos este derecho suele colisionar con la libertad de expresión. Como ya dijimos la ley lo refleja en el arto 10 "*El titular de los datos tiene derecho a solicitar a las redes sociales, navegadores y servidores que se supriman y cancelen los datos personales que se encuentren en sus ficheros.*"[80] En este aspecto la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal de España dice que si los dados en todo o en parte no son exactos estos tendrán que ser cancelados o sustituidos de oficio, el mismo nos remite al artículo 16 el cual reza "*El responsable del tratamiento tendrá la obligación de hacer efectivo el derecho de rectificación o cancelación del interesado en el plazo de diez días…*" [81]

Una temática que abordaremos a continuación es lo que respecta a los datos sensibles. La ley de protección de datos lo define como "Es toda información que revele el origen racial, étnico, filiación política, credo religioso, filosófico o moral, sindical, relativo a su salud o vida sexual,

[80] Ibídem. Arto. 10.

[81] LEY ORGÁNICA 15/1999, del 13 de diciembre, de protección de datos de carácter Personal de España. Publicada Boletín Oficial del Estado, núm. 298 de 14 de diciembre de 1999. PP 43088 a 43099. Arto. 16.

antecedentes penales o faltas administrativas, económicos financieros; así como información crediticia y financiera y cualquier otra información que pueda ser motivo de discriminación"[82] por ejemplo, en base al artículo3 de la nueva ley de promoción, protección y defensa de los derechos humanos ante el VIH y SIDA para su prevención y atención "(…), *no divulgarán en espacios públicos o privados: nombre, dirección, datos clínico-epidemiológicos y otros datos, que identifiquen a las personas con el VIH, o que pueda afectar su vida privada, económica, social, política y cultural.*"[83] Como vemos la protección de datos personales de esta índole son muy sensibles de acuerdo a su naturaleza, pero compararemos nuestra ley con la Directiva la cual refleja que se prohibirán el tratamiento de datos personales que revelen el origen racial o étnico, las opiniones políticas, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, así como el tratamiento de los datos relativos a la salud o a la sexualidad salvo cuando el titular del derecho haya dado su consentimiento explícito a dicho tratamiento.[84]

2.5.4. Habeas data

En Nicaragua recientemente aprobaron la Ley 831, ley de reforma y adiciones a la ley 49, ley de amparo, donde introdujeron la figura de habeas data, tal ley fue publica en la Gaceta número 29, del 14 de febrero del 2013. La cual viene a ser un equilibrio con otras leyes aprobadas como la ley protección de datos que acabamos de comentar y Ley No. 621, ley de acceso a la información pública, la cual en su artículo 4 inciso b hace

[82] LEY 787. Ob. Cit. Arto. 3.
[83] LEY DE PROMOCIÓN, PROTECCIÓN Y DEFENSA DE LOS DERECHOS HUMANOS ANTE EL VIH Y SIDA PARA SU PREVENCIÓN Y ATENCIÓN. Publicada en la Gaceta Diario Oficial No 242 del 18 de diciembre del 2012. Arto. 3.
[84] DIRECTIVA 95/46/CE. Ob. Cit. Arto. 8.

referencia al habeas data la cuales en su parte *infine* dice "*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*"[85].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. El mismo nace como imperativo frente a los problemas que se generan como consecuencia de los constantes avances tecnológicos.

El artículo 26 de nuestra Constitución es el escenario donde nace como fundamento este derecho, el cual pone de manifiesto que las personas tenemos derecho a nuestra privacidad individual como de familia, que se respete la inviolabilidad de nuestro domicilio etc.

Pero veamos lo que nos dice la ley 831, ley de reforma y adiciones a la ley 49, ley de amparo (en adelante la ley) en el artículo 2 expresa que "*el habeas data se crea como una garantía de tutela de 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

[85] LEY DE ACCESO A LA INFORMACIÓN PÚBLICA, Ley No. 621. Publicada en la Gaceta Diario Oficial No. 118 del 22 de junio del 2007. Arto. 4.

dice que el recurso de habeas data cabe contra los responsables y cualquier otra persona que hubiere hecho uso indebido de ficheros de datos.[86]

El órgano encargado para conocer y resolver el recuero de habeas data es la sala de lo constitucional de la Corte Suprema de Justicia.[87]

2.6. Sobre el Acuerdo de asociación entre la Unión Europea y Centroamérica.

Como hemos planteado en la introducción de este capítulo, Nicaragua ha ratificado el AdA con la UE, el cual está basado en tres pilares fundamentales: dialogo político, cooperación y comercio. Siendo este ultimo el que abordaremos en este capítulo, por la naturaleza del mismo.

En el ámbito de las relaciones internacionales la UE tiene la facultad de "celebrar con uno o varios Estados o con organizaciones internacionales acuerdos que establezcan una asociación que entrañe derechos y obligaciones recíprocos, acciones comunes y procedimientos particulares"[88] En este sentido, el recurso a los Acuerdos de asociación ha sido utilizado por la Unión Europea para establecer (o para intentar instaurar) de forma más estable y duradera relaciones especiales o privilegiadas de cooperación política y económica con los Estados de Latinoamérica, que, en términos generales, por un lado, presentan características comunes en su contenido y, por otro lado, pueden mostrar algunos matices en relación con la forma de negociación.[89]

[86] LEY 831. LEY DE REFORMA Y ADICIONES A LA LEY 49, LEY DE AMPARO. Publicada en la Gaceta Diario Oficial número 29, del 14 de febrero de 2013. Arto. 5.
[87] Ibídem.
[88] TJCE, sentencia de 30 de septiembre de 1987 (C-12/86).
[89] MEJÍA HERRERA, Orlando. Acuerdo de asociación entre la Unión Europea y Centroamérica. Contexto y perspectivas. *Revista de Derecho Comunitario Europeo.* núm. 35, Madrid, enero/abril (2010). pág. 156.

En cuanto al AdA en su aspecto económico supone la creación de una área de libre comercio entre las dos regiones en términos de eliminación de la mayor parte de las barreras arancelarias y no arancelarias a su comercio. En tal sentido beneficiaria el desarrollo del comercio electrónico, por el rápido y fácil acceso que por su naturaleza ofrece. Tal beneficio se desprende del artículo 75 del AdA correspondiente a la cooperación en cuanto a la sociedad de la información, el cual en su parte toral dice *"...la cooperación en este ámbito también estará encaminada en promover… el dialogo y el intercambio de las experiencias sobre el desarrollo de comercio electrónico y firma electrónica…"*[90]

El AdA establece dentro de su marco normativo la protección de datos, contenido en el artículo 34 donde *"… acuerdan cooperar para mejorar el nivel de protección de los datos personales hacia los más altos estándares internacionales,… y trabajar en aras de la libre circulación de datos personales entre las Partes, teniendo en cuenta sus legislaciones internas"*.[91]

Se reconoce en el artículo 55 del Ada *"...la importancia de la cooperación de asistencia técnica en materia de transferencia de tecnología para fortalecer la propiedad intelectual y acuerdan cooperar"*.[92]

El AdA examina los servicios de informática, expresado en el artículo 180 denominado Entendimiento sobre servicios de informática; donde"… *cubre las funciones básicas utilizadas para suministrar todos los servicios de informática y servicios conexos: los programas informáticos, definidos*

[90] ACUERDO, por el que se establece una Asociación entre la Unión Europea y sus Estados miembros, por un lado, y Centroamérica, por otro. Publicado en el Diario Oficial de la Unión Europea el 15 de diciembre del 2012. Arto 75.
[91] Ibídem, Arto. 34.
[92] Ibídem, Arto. 55.

como el conjunto de instrucciones requeridas para el funcionamiento y comunicación de los ordenadores (incluidos su desarrollo e implementación), el procesamiento y almacenamiento de datos, así como los servicios conexos, como los servicios de consultoría y formación para el personal de los clientes. Como resultado de los desarrollos tecnológicos, cada vez con más frecuencia se ofrecen estos servicios en forma de conjuntos o paquetes de servicios conexos que pueden incluir algunas de estas funciones básicas o todas ellas…" También contiene los servicios de telecomunicaciones "… *que incluyen servicios telefónicos de voz, servicios de transmisión de datos con conmutación de paquetes, servicios de transmisión de datos con conmutación de circuitos, servicios de télex, servicios de telégrafo, servicios de facsímil, servicios de circuitos privados arrendados y servicios y sistemas de comunicación móvil y personal…"*[93]

Como vemos el acuerdo significa indiscutiblemente una oportunidad y un reto para Centroamérica a fin de lograr un desarrollo económico. Los países centroamericanos necesitan mejorar aún más sus niveles de productividad y competitividad comercial en un mundo globalizado. Y para ello una zona de libre comercio con la UE implicaría un reto en el que ambas partes deben buscar un «equilibrio razonable» (no muy fácil de conseguir desde una perspectiva política y económica) entre los principios de nación más favorecida, trato nacional y trato especial y diferenciado.[94]

[93] Ibídem, Arto. 180.
[94] MEJÍA HERRERA, Orlando. Ob. Cit. Pág. 166.

CAPÍTULO III: DELITOS INFORMÁTICOS.

3.1. Concepto de delitos informáticos.

Esta denominación proviene de las expresiones inglesas *Computer crime y Computer related crime.* La primera definición fue propuesta por la Organización para la Cooperación y el Desarrollo Económico (OCDE), según ésta constituye delitos informáticos las conductas antijurídicas, no éticas o no autorizadas que impliquen el procesamiento automático de datos y/o la transmisión de datos. Para Rodríguez Mourullo, *"los delitos informáticos son todas aquellas conductas que ponen en peligro o lesionan la integridad, confidencialidad y/o disponibilidad de los datos y sistemas informáticos, y con ello sin perjuicio de que, además, puedan suponer una puesta en peligro o lesión de bienes jurídicos distintos".*[95]

Lucrecio Rebollo Delgado en su libro Derechos Fundamentales y Protección de Datos, expresa que delito informático es *"la realización de una acción que, reuniendo las características que delimitan el concepto de delito, sea llevada a cabo utilizando un elemento informático o vulnerado los derechos del titular de un elemento informático, ya sea hardware o software".*[96]

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)".*[97]

[95] DICCIONARIO JURÍDICO DE LOS MEDIOS DE COMUNICACIÓN. Colección de derecho de las nuevas tecnologías. Editorial Reus, 2006. Pág. 97.
[96] REBOLLO DELGADO, Lucrecio. Derechos Fundamentales y Protección de Datos. Edición ilustrada, Librería-Editorial Dykinson, 2004. Pág. 186.
[97] TÉLLEZ VALDÉS, Julio. Ob. Cit. Pág. 163.

3.2. Características de los delitos informáticos.

Los delitos informáticos presentan las siguientes características:

— Son conductas criminales de cuello blanco (*white collar crimes*), en tanto que sólo un determinado número de personas con ciertos conocimientos (en este caso técnicos) puede llegar a cometerlas.

— Son acciones ocupacionales porque muchas veces se realizan cuando el sujeto está en el trabajo.

— Son acciones de oportunidad debido a que se aprovecha una ocasión creada o altamente intensificada en el mundo de funciones y organizaciones del sistema tecnológico y económico.

— Provocan serias pérdidas económicas para los afectados y casi siempre producen beneficios de más de cinco cifras a aquellos que los realizan.

— Ofrecen facilidades de tiempo y espacio, ya que en milésimas de segundo y sin una necesaria presencia física pueden llegar a cometerse.

— Son muchos los casos y pocas las denuncias, todo ello debido a la falta misma de regulación jurídica a nivel internacional.

— Son sumamente sofisticados y frecuentes en el ámbito militar.

— Presentan grandes dificultades para su comprobación, esto por su mismo carácter técnico.

— En su mayoría son dolosos o intencionales, aunque también hay muchas de carácter culposo o imprudenciales y en ocasiones van más allá de la intención (preterintencionales).

— Ofrecen facilidades para su comisión a los menores de edad.

— Tienden a proliferar cada vez más, por lo que requieren una urgente regulación jurídica a nivel internacional.[98]

3.3. Clasificación de los delitos informáticos.

Se clasifican en atención a dos criterios:

1) Como instrumento o medio: se tienen a las conductas criminales que se valen de las computadoras como método, medio o símbolo en la comisión del ilícito. Por ejemplo:

— Falsificación de documentos vía computarizada (tarjetas de crédito, cheques, etcétera).

— Variación de los activos y pasivos en la situación contable de las empresas.

— Planeación o simulación de delitos convencionales (robo, homicidio, fraude, etcétera).

— Robo de tiempo de computadora.

— Lectura, sustracción o copiado de información confidencial.

— Modificación de datos tanto en la entrada como en la salida.

— Aprovechamiento indebido o violación de un código para penetrar a un sistema con el fin de introducir instrucciones inapropiadas (esto

[98] Ibídem, pág. 163.

es lo que se conoce en el medio como el método del Caballo de Troya).

— Variación en cuanto al destino de pequeñas cantidades de dinero hacia en cuenta bancaria apócrifa, método conocido como la técnica de salami.

— Uso no autorizado de programas de cómputo.

— Insertar instrucciones que provocan interrupciones en la lógica interna de los programas, a fin de obtener beneficios.

— Alteración en el funcionamiento de los sistemas.

— Obtención de información residual impresa en papel o cinta magnética luego de la ejecución de trabajos.

— Acceso a áreas informatizadas en forma no autorizada.

— Intervención de las líneas de comunicación de datos o teleproceso.

2. Como fin u objetivo: se enmarcan las conductas que van dirigidas en contra de la computadora, accesorios o programas como entidad física. Por ejemplo:

— Programación de instrucciones que producen un bloqueo total del sistema.

— Destrucción de programas por cualquier método.

— Daño a la memoria.

— Atentado físico contra la máquina o sus accesorios (discos, cintas, terminales, etcétera).

— Sabotaje político o terrorismo en que se destruya o surja un apoderamiento de los centros neurálgicos computarizados.

— Secuestro de soportes magnéticos en los que figure información valiosa, con fines de chantaje, pago de rescate, etcétera.[99]

3.4. Sujetos del delito informático.

En derecho penal, la ejecución de la conducta punible supone la existencia de dos sujetos, a saber, 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 el elemento localizador de los sujetos y de su posición frente al delito. Así, el titular del bien jurídico lesionado será el sujeto pasivo, quien puede diferir del sujeto perjudicado, el cual puede, eventualmente, ser un tercero. De otra parte, quien lesione el bien que se protege, a través de la realización del tipo penal, será el ofensor o sujeto activo.[100]

3.4.1. Sujeto activo.

Las personas que cometen los delitos informáticos son aquellas que poseen ciertas características que no presentan el denominador común de los delincuentes, esto es, los sujetos activos que 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

[99] Ibídem, pp. 165 y 166.

[100] ANÁLISIS DEL PROCESO IMPLEMENTADO PARA GENERAR PRUEBAS VÁLIDAS EN UNA INVESTIGACIÓN DE DELITOS INFORMÁTICOS. *Sujetos del delito informático.* [en línea] [Consultado el 11 de octubre del 2012]. Disponible en: <http://www.irdaoc.com/irdaoc/documentos/PIDAT_II_2010/GRUPO_4_ANALISIS_DE_PROCESO_DELITOS_INFORMATICOS.pdf>

informatizados, aun cuando, en muchos de los casos, no desarrollen actividades laborales que faciliten la comisión de este tipo de delitos.

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 delitos 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.[101]

En este apartado, cabe ejemplificar algunos sujetos activos como son los hackers y cracker. La palabra hacker es un neologismo, que en informática se utiliza para referirse a un gran experto en algún área de dominio. Si bien se relaciona más con los conocimientos técnicos e informáticos, es posible extender el concepto hacia otras disciplinas. De esta manera, se define así a cualquier persona a la que le apasiona el conocimiento, el aprendizaje y el funcionamiento de las cosas. Por su parte el término cracker proviene del vocablo inglés crack (romper). Aplicado a la informática, se trata de alguien que viola la seguridad de un sistema de modo ilegal y con diferentes fines. También se aplica específicamente al software, para denotar a aquellas personas que utilizan la ingeniería inversa sobre él con el objetivo de desprotegerlo, modificar su comportamiento o ampliar sus funcionalidades originales. En general, cuando se habla de delincuentes o piratas informáticos, hacemos referencia los crackers.[102]

[101] DEL PINO, Santiago Acurio. *Delitos informáticos: Generalidades.* [en línea]. [Consultado el 11 de octubre de 2012]. Profesor de Derecho Informático de la PUCE. Pág.15. Disponible en: <http://www.oas.org/juridico/spanish/cyb_ecu_delitos_inform.pdf>

[102] PACHECO, Federico; JARA Héctor. *Ethical Hacking.* 1ª ed. Buenos Aires: Fox Andina. En coedición con DÁLAGA S.A. 2012. pp. 19, 22, 23.

Un hacker era originalmente una persona interesada en las computadoras y que le gustaba explorar programas y sistemas de cómputo ya fuera dentro de su propio sistema o de alguien más. A los hackers maliciosos se les conoce como crackers, o personas que infringen la seguridad de un sistema de cómputo con la finalidad de dañarlo. Los crackers son individuos o pequeños grupos de personas que ocasionan serios problemas de seguridad. A los verdaderos delincuentes cibernéticos debería llamárseles crackers y no hackers.[103]

3.4.2. Sujeto pasivo.

El 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.

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.[104]

[103] BOEN OEKLERS, Dotty. *Comercio Electrónico.* Serie business. Cengage Learning Editores, 2004. Pág.124.
[104] DEL PINO, Santiago Acurio. Ob. Cit. pp. 18,19.

3.5. Regulación de los Delitos informáticos en la Unión Europea y en la República de Nicaragua.

3.5.1. Abordaje de los delitos informáticos en el Tratado de la Unión Europea, Tratado de Funcionamiento de la Unión Europea y Convenio sobre la Ciberdelincuencia.

La Unión Europea proporciona una serie de garantías a todos los ciudadanos de los Estados miembros, y así se observa el artículo 3 inciso 2 del Tratado de la Unión Europea *"La Unión ofrecerá a sus ciudadanos un espacio de libertad, seguridad y justicia sin fronteras interiores, en el que esté garantizada la libre circulación de personas conjuntamente con medidas adecuadas en materia de control de las fronteras exteriores, asilo, inmigración y de prevención y lucha contra la delincuencia"*.[105]

Por su parte el Tratado de Funcionamiento de la Unión Europea (en lo sucesivo denominado "TFUE"), desarrolla las distintas políticas y todas las acciones de ésta, cabe destacar que prevé la coordinación y cooperación entre las autoridades, por lo que se debe prestar atención al artículo 67 inciso 3, autenticando que *"La Unión se esforzará por garantizar un nivel elevado de seguridad mediante medidas de prevención de la delincuencia, el racismo y la xenofobia y de lucha en contra de ellos, medidas de coordinación y cooperación entre autoridades policiales y judiciales y otras autoridades competentes, así como mediante el reconocimiento mutuo de las resoluciones judiciales en materia penal y, si es necesario, mediante la aproximación de las legislaciones penales"*.[106]

La delincuencia no es un tema desapercibido en el TFUE, ya que establece los ámbitos delictivos, y lo manifiesta en el artículo 83 apartado 1, los

[105] TUE, Arto. 3, Inc. 2.
[106] TFUE, Arto. 67, Inc. 3.

cuales *"...son los siguientes: el terrorismo, la trata de seres humanos y la explotación sexual de mujeres y niños, el tráfico ilícito de drogas, el tráfico ilícito de armas, el blanqueo de capitales, la corrupción, la falsificación de medios de pago, la delincuencia informática y la delincuencia organizada…"*[107]

Se observa el rol que desempeñan algunas de las instituciones de la Unión Europea previniendo las posibles actuaciones futuras sobre cualquier tipo de delincuencia que dañe o afecte a los Estados miembros; manifestado en el artículo 84 *"El Parlamento Europeo y el Consejo podrán establecer, con arreglo al procedimiento legislativo ordinario, medidas que impulsen y apoyen la actuación de los Estados miembros en el ámbito de la prevención de la delincuencia, con exclusión de toda armonización de las disposiciones legales y reglamentarias de los Estados miembros"*.[108]

Es importante conocer ciertos organismos que se desempeñan bajo el lema de coordinación y cooperación por lo cual juegan un papel significativo en la lucha contra la delincuencia, a saber Eurojust y Europol. La unidad Eurojust es un órgano de la Unión Europea, con personalidad jurídica propia. [109] Según el artículo 85 apartado 1 del TFUE *"La función de Eurojust es apoyar y reforzar la coordinación y la cooperación entre las autoridades nacionales encargadas de investigar y perseguir la delincuencia grave que afecte a dos o más Estados miembros o que deba perseguirse según criterios comunes, basándose en las operaciones efectuadas y en la información proporcionada por las autoridades de los*

[107] Ibídem, Arto. 83, Inc. 1.
[108] Ibídem, Arto. 84.
[109] DECISIÓN DEL CONSEJO (2002/187/JAI), de 28 de febrero de 2002, por la que se crea Eurojust para reforzar la lucha contra las formas graves de delincuencia. Diario Oficial n° L 063 de 06/03/2002 p. 0001 – 0013.

Estados miembros y por Europol."[110] Por su parte la Oficina Europea de Policía (Europol), con personalidad jurídica.[111] Tiene la función según el artículo 88 apartado 1 del TFUE de "…*apoyar y reforzar la actuación de las autoridades policiales y de los demás servicios con funciones coercitivas de los Estados miembros, así como su colaboración mutua en la prevención de la delincuencia grave que afecte a dos o más Estados miembros, del terrorismo y de las formas de delincuencia que lesionen un interés común que sea objeto de una política de la Unión, así como en la lucha en contra de ellos."*[112] Trata de alcanzar una Europa más segura en interés de todos sus ciudadanos mediante la ayuda a las autoridades policiales de la Unión a través del intercambio y el análisis de información sobre actividades delictivas.[113]

En el TFUE se estable un marco jurídico en el cual se contemplan medidas generales pero de muy alto alcance en la Unión, para brindar seguridad a todos sus Estados miembros, ya que poseen una herramienta que es la cooperación entre todas sus instituciones y órganos las cuales velan por la erradicación de la delincuencia.

Con respecto al Convenio sobre Ciberdelincuencia (en lo sucesivo denominado "el Convenio"), emitido por el Consejo de Europa en Budapest el 23 noviembre 2001, tiene como objetivo conseguir una unión más estrecha entre sus miembros; ya que por los profundos cambios provocados por la globalización continua de las redes informáticas y por el

[110] TFUE, Arto. 85. Inc.1.
[111] DECISIÓN DEL CONSEJO (2009/371/JAI), de 6 de abril de 2009, por la que se crea la Oficina Europea de Policía (Europol). Publicada Diario Oficial L 121 de 15.5.2009, p. 37/66. Arto.2. Inc.1.
[112] TFUE, Arto. 88. Inc.1.
[113] PANORAMA DE EUROPOL. *"Informe general sobre las actividades de Europol"*. [en línea]. [Consultado el 14 de abril del 2013] Disponible en: <https://www.europol.europa.eu/sites/default/files/publications/es_europolreview.pdf>

riesgo de que las redes informáticas y la información electrónica sean utilizadas para cometer delitos y de las pruebas relativas a dichos delitos sean almacenadas y transmitidas por las redes, se vio en la necesidad de aplicar, con carácter prioritario una política penal común encaminada a proteger a la sociedad frente a la ciberdelincuencia mediante la adopción de una legislación adecuada y el fomento de la cooperación internacional.[114]

3.5.2. Medidas y estrategias implementadas por la Unión Europea en lucha contra los delitos informáticos.

3.5.2.1. Creación de la Agencia Europea de Seguridad de las Redes y de la Información (ENISA).

Dada la omnipresencia de las redes de comunicación y los sistemas de información, el problema de la seguridad se ha convertido en un tema de creciente preocupación para la sociedad. La Unión Europea con el fin de garantizar a los usuarios un mayor grado de seguridad, se ha dotado de una Agencia europea encargada de la seguridad de las redes y de la información (en lo sucesivo denominado "ENISA"), que tiene como función el asesoramiento y coordinación de las medidas adoptadas por la Comisión y los países de la Unión para dar seguridad a sus redes y sistemas de información.[115]

[114] MINISTERIO DE ASUNTOS EXTERIORES Y DE COOPERACIÓN. *Convenio sobre la Ciberdelincuencia.* [en línea]. [Consultado el 30 de noviembre de 2012]. Disponible en: <http://www.agpd.es/portalwebAGPD/canaldocumentacion/legislacion/consejo_europa/convenios/common/pdfs/Convenio_Ciberdelincuencia.pdf>

[115] AGENCIA EUROPEA DE SEGURIDAD DE LAS REDES Y DE LA INFORMACIÓN (ENISA). [en línea]. [Consultado el 9 de abril de 2013] Disponible en: < http://europa.eu/legislation_summaries/justice_freedom_security/fight_against_organised_crime/l24153_es.htm>

Según el reglamento (CE) nº 460/2004[116] del Parlamento Europeo y del Consejo, de 10 de marzo de 2004, por la que creó ENISA, tiene como objetivo principal reforzar la capacidad de la Unión Europea, en cuanto a la prevención, la reacción y la gestión de los problemas vinculados con la seguridad de las redes y la información.

Asimismo, ENISA presta asistencia a la Comisión en los trabajos preparatorios de carácter técnico de actualización y desarrollo de la normativa comunitaria. Del mismo modo, facilita y fomenta la cooperación entre los agentes de los sectores público y privado y permite, así, alcanzar un nivel de seguridad suficientemente elevado en los países de la Unión.

3.5.2.2. Política general de lucha contra la ciberdelincuencia.

En el comunicado de la Comisión al Parlamento Europeo, al Consejo y al Comité de las Regiones, de 22 de mayo de 2007, "Hacia una política general de lucha contra la ciberdelincuencia"[117], tiene por objeto la elaboración de una política general destinada a mejorar la coordinación de la lucha contra la ciberdelincuencia a escala europea e internacional. Enunciando un conjunto de medidas para hacer frente a este fenómeno y mejorar la colaboración entre los distintos protagonistas en la Unión Europea, tales como la mejora de la cooperación operativa de las autoridades policiales y judiciales, la mejora de la cooperación y la coordinación política entre los Estados miembros, la cooperación política y jurídica con terceros países, la intensificación del diálogo con la industria, la sensibilización, la formación y la investigación.

[116] REGLAMENTO (CE) Nº 460/2004. Publicado en Diario Oficial nº L 77 de 13.3.2004.
[117] [COM(2007) 267 FINAL. Bruselas, 22.5.2007. Comunicación de la comisión al Parlamento Europeo, al Consejo y al Comité de las Regiones: "Hacia una política general de lucha contra la ciberdelincuencia".

3.5.2.3. Protección de ciberataques e interrupciones a gran escala.

Según el comunicado de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones, del 30 de marzo de 2009, sobre protección de infraestructuras críticas de información, se debe "Proteger Europa de ciberataques e interrupciones a gran escala: aumentar la preparación, seguridad y resistencia".[118] Se propone un plan de acción articulado en torno a los siguientes ejes:

— Preparación y prevención: La cual insta a los Estados miembros a definir, con la ayuda de la ENISA, un nivel mínimo de capacidades y servicios para los equipos de respuesta a incidentes de seguridad de la información. Se pondrá en marcha una asociación público privada europea de resistencia sobre objetivos de mejora de la seguridad y la resistencia.
— Detección y respuesta: Se desarrollará y pondrá en marcha un sistema europeo de intercambio de información y alerta que llegue a los ciudadanos y las pymes.
— Mitigación y recuperación: Los Estados miembros deben elaborar planes nacionales de contingencia, a organizar ejercicios de simulación de incidentes a gran escala de seguridad de las redes y a estrechar la cooperación entre los equipos nacionales o gubernamentales.
— Cooperación internacional: Se prevé la cooperación internacional en lo que respecta principalmente a la resistencia y estabilidad de

[118] [COM (2009) 149 FINAL. Bruselas, 30.3.2009. Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité económico y social europeo y al Comité de las regiones: "Proteger Europa de ciberataques e interrupciones a gran escala".

internet para la definición de prioridades, principios y directrices, en primer lugar a escala europea, y después a nivel mundial.

— Establecimiento de criterios relativos a infraestructuras críticas europeas en el sector de las TIC: Se elaborarán criterios para caracterizar las infraestructuras europeas del sector de las TIC.

3.5.2.4. Creación del Centro Europeo de Cibercriminalidad (EC3).

Desde el 11 de enero de 2013, el nuevo Centro Europeo de Cibercriminalidad (en lo sucesivo denominado "EC3"), está en funcionamiento para ayudar a proteger a los ciudadanos y las empresas europeas del cibercrimen, su inauguración oficial se realizó en el Centro establecido en Europol en La Haya (Países Bajos).[119] El EC3 se centra en actividades ilegales en línea realizadas por grupos del crimen organizado, especialmente los ataques dirigidos a la banca electrónica y otras actividades financieras en línea, la explotación sexual infantil en línea y aquellos delitos que afectan a la infraestructura crítica y los sistemas de información en la Unión Europea.

El EC3 también facilita la investigación y desarrollo, garantiza la creación de capacidad entre la policía, los jueces y los fiscales y produce evaluaciones de amenazas, incluyendo análisis de tendencias, predicciones y alertas tempranas. Con el fin de desmantelar las redes, la ciberdelincuencia y procesar a más sospechosos, el EC3 recopila y procesa datos relacionados con delitos informáticos y proporciona un servicio de asistencia para las unidades de delito cibernético. Se ofrece apoyo operacional a los países de la Unión Europea (por ejemplo, contra la

[119] COMUNICADOS DE PRENSA DE LA COMISIÓN EUROPEA. *"Centro Europeo de Ciberdelincuencia (CE 3) se abre el 11 de enero"*. IP/13/13. [en línea]. [Consultado el 20 de febrero de 2013] Disponible en: <http://europa.eu/rapid/press-release_IP-13-13_en.htm>

intrusión, el fraude, el abuso sexual infantil en línea, etc.) y entrega conocimientos de alto nivel técnico, analítico y forense en las investigaciones conjuntas de la Unión Europea.

El EC3 funciona con tecnología de última generación y un sólido equipo de personal altamente cualificado y especializado que ofrece una amplia gama de servicios desde ayudar a los Estados miembros a analizar complejas pruebas forenses digitales a las tendencias y los escenarios de pronóstico; el EC3 se convertirá en el punto focal en la lucha contra la delincuencia informática en la Unión.[120]

3.5.2.5. Estrategia de ciberseguridad de la Unión Europea: Un ciberespacio abierto, protegido y seguro.

Según la propuesta presentada por la Comisión y la Alta Representante de la Unión Europea para Asuntos Exteriores y Política de Seguridad, al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones (Bruselas, del 7 de febrero de 2013), para que el ciberespacio siga siendo abierto y libre, deben aplicarse en línea los mismos principios, valores y normas que la Unión Europea promueve fuera de línea. Los derechos fundamentales, la democracia y el Estado de Derecho deben ser protegidos en el ciberespacio. Se expone la visión de la Unión Europea en este campo, aclara funciones y responsabilidades y establece las medidas necesarias, basadas en una protección y una promoción amplias y efectivas de los derechos de los ciudadanos con el fin

[120] COMUNICADOS DE PRENSA DE LA COMISIÓN EUROPEA. *"El Centro Europeo de Ciberdelincuencia CE 3"*. MEMO/13/6. [en línea]. [Consultado el 20 de febrero de 2013] Disponible en: <http://europa.eu/rapid/press-release_MEMO-13-6_en.htm>

de que el entorno en línea de la Unión Europea llegue a ser el más seguro del mundo. [121]

Se brinda protección a los Derechos fundamentales, la libertad de expresión, los datos personales y la intimidad esto quiere decir que todo intercambio de información a efectos de ciberseguridad en que se manejen datos personales debe cumplir la normativa de protección de datos de la Unión Europea y tomar plenamente en consideración los derechos de las personas en este ámbito.

También propone una gobernanza multilateral democrática y eficaz ya que el mundo digital no está controlado por una sola entidad sino intervienen en él varias partes, muchas de las cuales son entidades comerciales y no gubernamentales que participan en la gestión diaria de los recursos, protocolos y normas de internet y en su futuro desarrollo. De esta forma la Unión Europea reafirma la importancia de todas las partes interesadas en el actual modelo de gobernanza de internet y respalda este planteamiento de gobernanza multilateral. Se garantiza la seguridad como una responsabilidad compartida es por eso que todas las partes interesadas, ya sean las administraciones públicas, el sector privado o los ciudadanos, han de reconocer esta responsabilidad compartida, tomar medidas para protegerse y en caso necesario, ofrecer una respuesta coordinada para reforzar la ciberseguridad.

[121] COMUNICACIÓN CONJUNTA AL PARLAMENTO EUROPEO, AL CONSEJO, AL COMITÉ ECONÓMICO Y SOCIAL EUROPEO Y AL COMITÉ DE LAS REGIONES: *"Estrategia de ciberseguridad de la unión europea"*. [en línea]. Fecha de publicación: 7 de febrero 2013. [Consultado el 20 de febrero de 2013]. Disponible en: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=JOIN:2013:0001:FIN:ES:PDF >

3.5.3. Tratamiento de los delitos informáticos en el Convenio sobre la Ciberdelincuencia de la Unión Europea y el Código Penal de Nicaragua.

Es necesario, señalar ciertas garantías contempladas en la Constitución Política de la República de Nicaragua, las cuales brindan seguridad, protección a los individuos y así se establece en el artículo 25 *"Toda persona tiene derecho: A la libertad individual; A su seguridad; Al reconocimiento de su personalidad y capacidad jurídica".*[122] Señala la capacidad de actuar del individuo, de acuerdo a su voluntad; brinda protección a las personas en las diferentes situaciones jurídicas que puedan darse en el ámbito social.

Otra garantía se encuentra en el artículo 26 de la Constitución Política *"toda persona tiene derecho: 1) A su vida privada y a la de su familia; 2) A la inviolabilidad de su domicilio, su correspondencia y sus comunicaciones de todo tipo.3) Al respeto de su honra y reputación. 4) A conocer toda información que sobre ella hayan registrado las autoridades estatales, así como saber por qué y con qué finalidad tiene esa información…"*[123] en consecuencia si se incurre en lo contrario se convierte en delito y se debe sancionar.

La libertad de expresión es otra de las garantías que se contempla en la Constitución y así lo ratifica el artículo 30 *"Los nicaragüenses tienen derecho a expresar libremente su pensamiento en público o en privado,*

[122] CONSTITUCIÓN POLÍTICA DE LA REPÚBLICA DE NICARAGUA. Ob. Cit. Arto. 25.
[123] Ibídem, Arto. 26.

individual o colectivamente, en forma oral, escrita o por cualquier otro medio".[124]

Ahora se observa el tratamiento del Convenio sobre la Ciberdelincuencia (en lo sucesivo denominado "el Convenio") sobre los distintos delitos de carácter informático, es así que en el artículo 2 establece el Acceso ilícito, que consiste en *"…el acceso deliberado e ilegítimo a la totalidad o a una parte de un sistema informático. Cualquier Parte podrá exigir que el delito se cometa infringiendo medidas de seguridad, con la intención de obtener datos informáticos o con otra intención delictiva, o en relación con un sistema informático que esté conectado a otro sistema informático".*[125] Se observa que se infringen medidas de seguridad con clara intención de obtener el acceso a sistemas y datos informáticos. Por su parte, el artículo 198 del Código Penal, contempla el Acceso y uso no autorizado de información; el cual expresa lo siguiente *"Quien, sin la debida autorización, utilice los registros informáticos de otro, o ingrese, por cualquier medio, a su banco de datos o archivos electrónicos, será penado con prisión de uno a dos años, y de doscientos a quinientos días multas".*[126]

El artículo 3 del Convenio, denominado Interceptación ilícita expresa que *"…la 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 informáticos. Cualquier Parte*

[124] Ibídem, Arto. 30.
[125] CONVENIO SOBRE LA CIBERDELINCUENCIA. Ob. Cit. Arto. 2.
[126] CÓDIGO PENAL DE LA REPÚBLICA DE NICARAGUA. Ley Nº 641. Bibliografías Técnicas S.A. Pág. 64. Arto.198.

podrá exigir que el delito se haya cometido con intención delictiva o en relación con un sistema informático conectado a otro sistema informático".[127] Cabe destacar que la interceptación ilícita recae sólo en materia de carácter informático, por el contrario sucede en el artículo 192 del Código Penal nicaragüense, Apertura o intercepción ilegal de comunicaciones; el que se refiere a la obtención del contenido de cualquier tipo de comunicación en sus diferentes modalidades *"Quién ilegítimamente abra, intercepte o por cualquier otro medio se entere del contenido de una carta, un pliego cerrado o un despacho telegráfico, telemático, electrónico o de otra naturaleza que no le esté dirigido, será penado con prisión de seis meses a dos años de prisión. Si además difundiera o revelara el contenido de las comunicaciones señaladas en el párrafo anterior, se impondrá prisión de uno a tres años".*[128]

En el Convenio se mencionan dos clases de interferencia, la de datos y la del sistema cada una presenta sus particularidades pero ambas recaen en los obstáculos que dificultan sus funciones; y así se ve en el artículo 4 apartado 1 nombrado Interferencia en los datos, el cual señala que es *"…la comisión deliberada e ilegítima de actos que dañen, borren, deterioren, alteren o supriman datos informáticos".*[129] Y la Interferencia del sistema, contemplado en el artículo 5 donde se establece que es*"…la obstaculización grave, deliberada e ilegítima del funcionamiento de un sistema informático mediante la introducción, transmisión, provocación de*

[127] CONVENIO SOBRE LA CIBERDELINCUENCIA. Ob. Cit. Arto. 3.
[128] CÓDIGO PENAL DE LA REPÚBLICA DE NICARAGUA. Ob. Cit. Arto.192.
[129] CONVENIO SOBRE LA CIBERDELINCUENCIA. Ob. Cit. Arto. 4. Apartado 1.

daños, borrado, deterioro, alteración o supresión de datos informáticos".[130]

Por otro lado los artículos 245 y 246 del Código Penal nicaragüense sancionan a aquellas personas que destruyen los registros informáticos y usan programas destructivos conocidos como virus que causan daños y que vienen a afectar directamente las funciones y equipos de la computadora. He aquí lo que contemplan dichos artículos:

Artículo 245. Destrucción de registros informáticos. *"Quien destruya, borre o de cualquier modo inutilice registros informáticos, será penado con prisión de uno a dos años o de noventa a trescientos días multa. La pena se elevará de tres a cinco años, cuando se trate de información necesaria para la prestación de un servicio público o se trate de un registro oficial".*[131]

Artículo 246. Uso de programas destructivos. "*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".*[132]

En el artículo 6 Abuso de los dispositivos, del Convenio expresa que es la comisión deliberada e ilegítima de "*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 los delitos previstos…; una*

[130] Ibídem, Arto. 5.
[131] CÓDIGO PENAL DE LA REPÚBLICA DE NICARAGUA. Ob. Cit. Arto. 245.
[132] Ibídem, Arto. 246.

contraseña, un código de acceso o datos informáticos similares que permitan tener acceso a la totalidad o a una parte del sistema informático…"[133]

El Código Penal en el artículo 197 denominado Registros prohibidos, dispone *"El que sin autorización de ley promueva, facilite, autorice, financie, cree o comercialice un banco de datos o un registro informático con datos que puedan afectar a las personas naturales o jurídicas, será penado con prisión de dos a cuatro años y de trescientos a quinientos días multa"*. [134]

Los delitos informáticos se avistan en dos artículos del Convenio, por un lado el artículo 7 Falsificación informática, la cual se da"…*cuando se cometa de forma deliberada e ilegítima, 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…"*.[135] Y por otro lado, el artículo 8 considera que, el fraude informático son "…*los actos deliberados e ilegítimos que causen un perjuicio patrimonial a otra persona mediante:*

a. *cualquier introducción, alteración, borrado o supresión de datos informáticos;*
b. *cualquier interferencia en el funcionamiento de un sistema informático, con la intención fraudulenta o delictiva de obtener*

[133] CONVENIO SOBRE LA CIBERDELINCUENCIA. Ob. Cit. Arto. 6.
[134] CÓDIGO PENAL DE LA REPÚBLICA DE NICARAGUA. Ob. Cit. Arto. 197.
[135] CONVENIO SOBRE LA CIBERDELINCUENCIA. Ob. Cit. Arto. 7.

ilegítimamente un beneficio económico para uno mismo o para otra persona". [136]

El artículo anteriormente expuesto del Convenio presenta una breve semejanza con el artículo 229 del Código Penal denominado Estafa, párrafo segundo, en el cual se castiga con prisión de uno a cuatro años y de noventa a trescientos días multas *"a quien con el propósito de obtener un provecho ilícito, consiga la transferencia no consentida de cualquier activo patrimonial en perjuicio de tercero, mediante la manipulación de registros informáticos o programas de computación o el uso de otro artificio semejante".*[137]

Cabe enfatizar que, la Unión Europea pretende prevenir y combatir la pornografía infantil en internet; y así lo ratifica en la Decisión (2000/375/JAI)[138] de 29 de mayo de 2000, ya que insta en el artículo 1 apartado1 lo siguiente"…*los Estados miembros adoptarán las medidas necesarias para animar a los usuarios de internet a que comuniquen a las autoridades policiales, directa o indirectamente, sus sospechas sobre la difusión de material pornográfico infantil en internet, cuando encuentren material de este tipo...."*[139] El Convenio lo tutela en el artículo 9 Delitos relacionados con la pornografía infantil, "… *la comisión deliberada e ilegítima de los siguientes actos:*

a. *la producción de pornografía infantil con vistas a su difusión por medio de un sistema informático;*

[136] Ibídem, Arto. 8.
[137] CÓDIGO PENAL DE LA REPÚBLICA DE NICARAGUA. Ob. Cit. Arto. 229.
[138] DECISIÓN DEL CONSEJO (2000/375/JAI) de 29 de mayo de 2000. Relativa a la Lucha contra la pornografía infantil en internet. Diario Oficial de las Comunidades Europeas 9.6.2000 L 138/1.
[139] Ibídem, Arto. 1. Inc.1.

b. *la oferta o la puesta a disposición de pornografía infantil por medio de un sistema informático;*
c. *la difusión o transmisión de pornografía infantil por medio de un sistema informático,*
d. *la adquisición de pornografía infantil por medio de un sistema informático para uno mismo o para otra persona;*
e. *la posesión de pornografía infantil en un sistema informático o en un medio de almacenamiento de datos informáticos.*

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

a. *un menor comportándose de una forma sexualmente explícita;*
b. *una persona que parezca un menor comportándose de una forma sexualmente explícita;*
c. *imágenes realistas que representen a un menor comportándose de una forma sexualmente explícita.*

3. A los efectos del anterior apartado 2, por menor se entenderá toda persona menor de 18 años. No obstante, cualquier Parte podrá· establecer un límite de edad inferior, que será como mínimo de 16 años".[140]

Sus intentos de erradicar estos delitos no terminan ahí, ya que la Comisión Europea realizó la declaración sobre el lanzamiento de la alianza global contra el abuso sexual infantil en línea, MEMO/12/944 (Bruselas el 5 de diciembre 2012); se anunció el compromiso de perseguir los objetivos políticos comunes, que consisten en mejorar los esfuerzos para identificar a

[140] CONVENIO SOBRE LA CIBERDELINCUENCIA. Ob. Cit. Arto. 9.

las víctimas, cuyo abuso sexual se representa en la pornografía infantil; asegurar que se reciba asistencia necesaria, apoyo y protección e identificar los delincuentes; aumentar la conciencia pública sobre los riesgos que suponen las actividades de los niños en línea; establecer un marco necesario para la criminalización de la línea abuso sexual infantil y el enjuiciamiento efectivo de los responsables; mejorar los esfuerzos conjuntos de las autoridades policiales a través de países de la Alianza Global; alentar la participación del sector privado en la identificación y eliminación de material de pornografía infantil; y aumentar la velocidad de la notificación y los procedimientos de remoción tanto como sea posible sin poner en peligro las investigaciones penales.[141]

El Código Penal nicaragüense no se queda atrás con respecto al tema de pornografía infantil, aunque le dedica una breve atención, se observa el artículo 175 párrafo segundo la Explotación sexual, pornografía y acoso sexual con adolescentes mediante pago; *"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".*[142]

[141] COMUNICADOS DE PRENSA DE LA COMISIÓN EUROPEA. *"Declaración sobre el lanzamiento de la Alianza Global contra el abuso sexual infantil en línea"*. MEMO/12/944. [en línea]. [Consultado: el 20 de febrero de 2013] Disponible en:<http://europa.eu/rapid/press-release_MEMO-12-944_en.htm>
[142] CÓDIGO PENAL DE LA REPÚBLICA DE NICARAGUA. Ob. Cit. Arto. 175.

Otro tema de gran interés afrontado por el Convenio, son los delitos relacionados con infracciones de la propiedad intelectual y los derechos afines, contenido en el artículo 10 que refiere en parte sobre la protección de las obras literarias y artísticas relacionados con el comercio los cuales se dan *"…cuando esos actos se cometan deliberadamente, a escala comercial y por medio de un sistema informático*".[143] Y sobre la protección de las obras de intérpretes y ejecutantes y los productores de fonogramas y los organismos de radiodifusión*"…cuando esos actos se cometan deliberadamente, a escala comercial y por medio de un sistema informático".*[144]

Siguiendo la temática en el caso de Nicaragua, el Código Penal artículo 247 trata sobre el Ejercicio no autorizado del derecho de autor y derechos conexos y que *"Será sancionado con noventa a ciento cincuenta días multa o prisión de seis meses a dos años e inhabilitación especial por el mismo período para ejercer cargo, profesión, oficio, industria o comercio relacionado con la conducta delictiva, quien contraviniendo la ley de la materia, y con el propósito de obtener un beneficio económico para sí o para un tercero, realice cualquiera de los actos siguientes sin autorización escrita del titular del derecho: …. G) La realización de cualquier acto que eluda o pretenda eludir una medida tecnológica implementada por el titular del derecho para evitar la utilización no autorizada de una obra o fonograma;….J) La importación, distribución, comercialización, arrendamiento o cualquier otra modalidad de distribución de obras o*

[143] CONVENIO SOBRE LA CIBERDELINCUENCIA. Ob. Cit. Arto. 10. Inc. 1.
[144] Ibídem, Arto. 10. Inc. 2.

fonogramas cuya información sobre gestión de derechos ha sido suprimida o alterada".[145]

De igual forma el artículo 248 denominado Reproducción ilícita, establece que *"Será sancionado con 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, quien contraviniendo la Ley de la materia y con el propósito de obtener un beneficio económico para sí o para un tercero, realice cualquiera de los siguientes actos sin autorización escrita del titular del derecho: a) La reproducción, total o parcial, de una obra o fonograma por cualquier medio, forma o procedimiento; b) La distribución de ejemplares de una obra o fonograma por medio de venta, arrendamiento, préstamo público, importación, exportación o cualquier otra modalidad de distribución;…"*[146]

Se realizó un protocolo adicional al Convenio relativo a la penalización de actos de índole racista y xenófoba cometidos por medio de sistemas informáticos (Estrasburgo, 30 de enero de 2003), con la finalidad de completar, las disposiciones del Convenio.[147] En dicho Protocolo se entiende por material racista y xenófobo *"todo material escrito, toda imagen o cualquier otra representación de ideas o teorías, que propugne, promueva o incite al odio, la discriminación o la violencia, contra cualquier persona o grupo de personas, por razón de la raza, el color, la*

[145] CÓDIGO PENAL DE LA REPÚBLICA DE NICARAGUA. Ob. Cit. Arto. 247.
[146] Ibídem, Arto. 248.
[147] MINISTERIO DE ASUNTOS EXTERIORES Y DE COOPERACIÓN. *Protocolo adicional al Convenio sobre la ciberdelincuencia relativo a la penalización de actos de índole racista y xenófoba cometidos por medio de sistemas informáticos.* [en línea]. [Consultado el 14 de abril de 2013] Disponible en: <https://www.gdt.guardiacivil.es/webgdt/media/Legislacion/Protocolo_adicional_convencion_cibercrimen.pdf>

ascendencia o el origen nacional o étnico, así como de la religión en la medida en que ésta se utilice como pretexto para cualquiera de esos factores.[148] El Protocolo escarmienta la difusión de material racista y xenófobo; las amenazas con motivación racista y xenófoba; los insultos con motivación racista y xenófoba; la negación, minimización, aprobación o justificación del genocidio o de crímenes contra la humanidad todos expuestos por medios de sistemas informáticos.

Cabe destacar el artículo 250 del Código Penal alusivo a la Protección de programas de computación, el cual establece que *"Será sancionado 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, quien contraviniendo la ley de la materia 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".*[149]

Es necesario citar el artículo 275 denominado Apoderamiento de secretos de empresa, la cual sanciona a *"Quien, en provecho propio o de un tercero, se apodere por cualquier medio, de información, de datos, documentos escritos o electrónicos, registros informáticos u otros medios u objetos que contengan un secreto empresarial, sin autorización de su poseedor legítimo o del usuario autorizado, será castigado con pena de prisión de dos a cuatro años o de trescientos a seiscientos días multa. Lo dispuesto en*

[148] Ibídem.
[149] CÓDIGO PENAL DE LA REPÚBLICA DE NICARAGUA. Ob. Cit. Arto. 250.

el presente artículo se entenderá sin perjuicio de las penas que puedan corresponder por los actos de apoderamiento o los daños ocasionados".[150]

Nos resultó muy interesante que en el Código Penal está tipificado la conducta de Intrusión, el cual protege la seguridad del Estado, situado en el artículo 417 estableciendo que *"Será sancionado con pena de cuatro a ocho años de prisión, quien indebidamente con fines de espionaje cometa alguno de los siguientes actos:…c) Se introduzca en los programas informáticos relativos a la seguridad nacional o defensa nacional;…"*[151]

[150] Ibídem, Arto. 275.
[151] Ibídem, Arto. 417.

CONCLUSIONES.

1. En nuestra sociedad es de vital importancia la informática, esta ciencia la encontramos en todas y cada una de nuestras actividades a consecuencia de lo que es llamado el mundo globalizado, por lo que su regulación permite que el Derecho este acorde con la realidad.

2. El derecho informático se encuentra íntimamente relacionado con las distintas ramas del Derecho des de el punto de vista doctrinal y legislativo, ya que este siempre está presente en determinados hechos informáticos.

3. Las normas relativas del Derecho informático de la Unión Europea se podría implementar en Nicaragua a nivel interno tomando como base ciertos aspectos legislativos de ésta, los beneficios que traería consigo serian, seguridad en el uso del internet y las fuentes electrónicas, brindando una mayor confianza en el uso del comercio electrónico, por ende un incentivo más para promover esta nueva modalidad de comercio ya que en la actualidad Nicaragua atraviesa una debilidad en esta materia.

4. La falta de una ley que regula de manera especial el comercio electrónico hace más incierto el uso de esta modalidad de comercio, lo que conlleva que los compradores tengan una actitud indiferente a la hora de comprar por internet.

5. La ley de defensa de los consumidores es una ley retrograda en la actualidad, la cual no regula de manera eficiente la protección del consumidor frente al comercio electrónico.

6. La informática reúne características que la convierten en el medio idóneo para la comisión de delitos informáticos, éstos son realizadas por especialistas en la materia capaces de efectuar el delito y borrar las huellas de los hechos; afectan al ser humano violando su integridad, privacidad; ocasionando grandes pérdidas económicas a sus víctimas.

7. Los delitos informáticos, no conocen fronteras y generan grandes beneficios a los delincuentes, éstos se aprovechan a menudo del anonimato de los dominios de los sitios web.

8. Los delitos informáticos es una de las formas de delincuencia de crecimiento más rápido y para hacerle frente a estos delitos se deben disponer herramientas y capacidades operativas idóneas. Donde los cuerpos de seguridad deben adoptar un enfoque coordinado y colaborativo para responder a esta amenaza creciente.

9. La implementación del Acuerdo de Asociación traerá beneficios ya sea técnicos o jurídicos para la implementación del comercio electrónico.

10. Para la elaboración de nuestro trabajo fue dificultoso encontrar bibliografía, revistas o artículos especializados en el estudio del fenómeno que tuvieran la rigurosidad científica y académica para poder utilizarlos como fuentes bibliográficas.

RECOMENDACIONES.

— En el momento de la elaboración de una ley especial de comercio electrónico se debería tomar en consideración ciertos instrumentos legales de la Unión Europea, como modelo.

— En Nicaragua se debería de invertir más en tecnología, que a la vez vaya de la mano con las leyes para una mayor seguridad en el uso de la tecnología.

— La ley No. 182, ley de defensa de los consumidores debería ser reformada o derogada por una ley que proteja al consumidor frente a esta nueva modalidad de comercio.

— En Nicaragua se debería crear una institución encargada a la investigación y persecución de delitos informáticos, ya que en la actualidad es difícil la captura de los actores de un delito informático.

— Implementar en el pensum académico de las facultades de derecho de las universidades del país una asignatura del derecho informático, para fortalecer el conocimiento del futuro profesional.

BIBLIOGRAFÍA.

Fuentes directas.

Legislación de la Unión Europea:

— [COM(2007) 267 Final]. Bruselas, 22.5.2007. Comunicación de la comisión al Parlamento Europeo, al Consejo y al Comité de las Regiones "Hacia una política general de lucha contra la ciberdelincuencia".

— [COM (2009) 149 Final. Bruselas, 30.3.2009. Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité económico y social europeo y al Comité de las Regiones: "Proteger Europa de ciberataques e interrupciones a gran escala".

— DECISIÓN DEL CONSEJO (2000/375/JAI) de 29 de mayo de 2000. Relativa a la Lucha contra la pornografía infantil en Internet. Diario Oficial de las Comunidades Europeas 9.6.2000 L 138/1.

— DECISIÓN DEL CONSEJO (2002/187/JAI), de 28 de febrero de 2002. Por la que se crea Eurojust para reforzar la lucha contra las formas graves de delincuencia. Diario Oficial n° L 063 de 06/03/2002.

— DECISIÓN DEL CONSEJO (2009/371/JAI), de 6 de abril de 2009. Por la que se crea la Oficina Europea de Policía (Europol). Publicada Diario Oficial L 121 de 15.5.2009.

— DIRECTIVA 2000/31/CE del Parlamento Europeo relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular el Comercio Electrónico y del Consejo de 8 de junio de 2000. Publicada Diario Oficial n° L 178 de 17/07/2000.

— DIRECTIVA 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos. Publicada Diario Oficial n° L 281 de 23/11/1995.

— DIRECTIVA 1999/93/CE del Parlamento Europeo y del Consejo, de 13 de diciembre de 1999, por la que se establece un marco comunitario para la firma electrónica. Diario Oficial n° L 013 de 19 de enero del 2000.

— REGLAMENTO (CE) Nº 460/2004. Publicado en Diario Oficial nº L 77 de 13.3.2004.

— ACUERDO, por el que se establece una Asociación entre la Unión Europea y sus Estados miembros, por un lado, y Centroamérica, por otro. Publicado en el Diario Oficial de la Unión Europea el 15 de diciembre del 2012.

Legislación de Nicaragua.

— CONSTITUCIÓN POLÍTICA DE LA REPÚBLICA DE NICARAGUA. 1ra Edición. Jurídica. 2009.

— CÓDIGO CIVIL DE LA REPÚBLICA DE NICARAGUA, tomo II. Anotada y concordada, por los doctores Carlos A. Morales, Joaquín cuadra Zavala y Mariano Arguello. 3ra edición. Casa Editorial Carlos Heuberger. Managua, Nicaragua. 1933.

— CÓDIGO PENAL DE LA REPÚBLICA DE NICARAGUA. Ley Nº 641. Bibliografías Técnicas S.A.

— LEY DE DEFENSA DE LOS CONSUMIDORES, ley 182. Publicada en la Gaceta Diario Oficial No. 213 del 14 de noviembre de 1994.

— LEY DE FIRMA ELECTRÓNICA, Ley 729. Publicada en la Gaceta Diario Oficial el 30 de agosto del 2006.

— LEY MODELO DE LA CNUDMI SOBRE FIRMAS ELECTRÓNICAS CON LA GUÍA PARA SU INCORPORACIÓN AL DERECHO INTERNO 2001. [en línea] Disponible en: <www.uncitral.org/pdf/spanish/texts/electcom/ml-elecsig-s.pdf>

— LEY DE PROTECCIÓN DE DATOS, Ley 787. Publicada en la Gaceta Diario Oficial No. 61 del 29 de marzo del 2012.

— LEY DE PROMOCIÓN, PROTECCIÓN Y DEFENSA DE LOS DERECHOS HUMANOS ANTE EL VIH Y SIDA PARA SU PREVENCIÓN Y ATENCIÓN. Publicada en la Gaceta Diario Oficial No 242 del 18 de diciembre del 2012.

— LEY DE ACCESO A LA INFORMACIÓN PÚBLICA, Ley No. 621. Publicada en la Gaceta Diario Oficial No. 118 del 22 de junio del 2007

— LEY 831. Ley de reforma y adiciones a la Ley 49, Ley de Amparo. Publicada en la Gaceta Diario Oficial número 29, del 14 de febrero de 2013.

Legislación española:

— CONSTITUCIÓN DE ESPAÑA. Boletín Oficial del Estado, núm. 311 de 29 de diciembre de 1978.

— REAL DECRETO-LEY 14/1999, de 17 de septiembre, sobre firma electrónica. Publicada en Boletín Oficial del Estado, núm. 224 de 18 de septiembre de 1999.

— REAL DECRETO, Ley Código Civil. Publicada en Boletín Oficial del Estado, núm. 206 de 25 de julio de 1889. España.

— LEY DE SERVICIOS DE LA SOCIEDAD DE LA INFORMACIÓN Y DE COMERCIO ELECTRÓNICO DE ESPAÑA, Ley 34/2002, de 11 de julio, BOE núm. 166 de 12 de julio del 2002.

— LEY ORGÁNICA 15/1999, de 13 de diciembre, de protección de datos de carácter personal de España. Publicada Boletín Oficial del Estado, núm. 298 de 14 de diciembre de 1999.

Libros:

— ASIMOV, Isaac. Enciclopedia biográfica de ciencia y tecnología: la vida y la obra de 1197 grandes científicos desde la antigüedad hasta nuestros días. Alianza Editorial Mexicana. México. 1988.

— BRIZ, Julián; LASO, Isidro. Internet y Comercio Electrónico. 2da edición. Ediciones Mandí-Prensa. Madrid, España. 2000.

— BRENES CORDOBA, Alberto. Tratado de los contratos. 6ta ed. Editorial Juricentro. San José, Costa Rica. 2009.

— BOEN OEKLERS, Dotty. Comercio Electrónico. Serie business. Cengage Learning Editores, 2004.

— CONICYT, secretaria ejecutiva. Anteproyecto de ley de comercio electrónico. Junio 2006.

— DAVARA RODRÍGUEZ, Miguel Ángel. Manual de Derecho Informático. Ed. Aranzadi. Madrid. 2001.

— DE MIGUEL, Pedro. Directiva sobre comercio electrónico, determinación de la normativa aplicable a las actividades transfronterizas, en la *Revista de la Contratación Electrónica*. Ed. Editora de Publicaciones Científicas y Profesionales (EDICIP), Cádiz, 2001.

— DICCIONARIO JURÍDICO DE LOS MEDIOS DE COMUNICACIÓN. Colección de derecho de las nuevas tecnologías. Editorial Reus, 2006.

— FERNÁNDEZ FERNÁNDEZ, RODOLFO. Contratación electrónica: la prestación del consentimiento en Internet. Ed. J.M. Bosch. Editor, Barcelona 2001.

— GARIBOLDI, Gerardo. Comercio electrónico: conceptos y reflexiones básicas. BID-INTAL. 1999.

— GUILLÉN BUSTAMANTE, Giovanny. Cibernética. Caracas Venezuela, Especialista Certificado en Sistemas IBM AS/400. Publicado 13 de Enero de 2000.

— GARCIA CUEVAS, Roque. Principios básicos de Informática. Librería-Editorial Dykinson. 2007.

— KATZ, Jorge M. Los caminos hacia una sociedad de la información en América Latina y el Caribe. United Nations Publications. 2003.

— LA INFORMÁTICA, PRESENTE Y FUTURO EN LA SOCIEDAD, Volumen 15 de Ciencias experimentales y tecnología. Librería-Editorial Dykinson. 2006.

— MANGAS MARTÍN, ARACELI Y LIÑÁN NOGUERAS, DIEGO. Instituciones y Derecho de la Unión Europea. Editorial Tecnos. Madrid, España. 5ta. Edición. 2005.

— MEJÍA HERRERA, Orlando. Acuerdo de asociación entre la Unión Europea y Centroamérica. Contexto y perspectivas. *Revista de Derecho Comunitario Europeo*. núm. 35, Madrid, enero/abril. 2010.

— MORENO NAVARRETE, Miguel Ángel. DERECHO-e Derecho del Comercio Electrónico. Ed. Marcial Pons. Madrid. 2002.

— MINELLI, Alejandra; et al. Breve historia de la informática. Publicado 22 de octubre de 2001.

— ORÚE CRUZ. Jose. Manual de Derecho mercantil. 2da edición. Editorial HISPAMER. Managua, Nicaragua. 2008

— PACHECO, Federico. JARA, Héctor. Ethical Hacking. 1ª ed. Buenos Aires: Fox Andina. En coedición con DÁLAGA S.A. 2012.

— TORRES ÁLVAREZ, Hernán. El sistema de seguridad jurídica en el comercio electrónico. Fondo Editorial PUCP. 2005.

— TÉLLEZ VALDÉZ, Julio. Derecho Informático. Tercera edición, Mc Graw-Hill Interamericana Editores S.A, México 2004.

— REBOLLO DELGADO, Lucrecio. Derechos Fundamentales y Protección de Datos. Edición ilustrada, Librería-Editorial Dykinson, 2004.

— SUÑE LLINÁS, Emilio. Tratado de Derecho Informático. Volumen I, Introducción y protección de datos personales. Ed. Universidad Complutense de Madrid. Madrid.2000.

— VILLABELLA ARMENGOL, CARLOS MANUEL. La investigación y comunicación científica en las ciencias jurídicas. Primera edición. Editorial Instituto de Ciencias Jurídicas de Puebla. Puebla México. 2009.

Fuentes electrónicas.

Páginas consultadas.

— ANÁLISIS DEL PROCESO IMPLEMENTADO PARA GENERAR PRUEBAS VÁLIDAS EN UNA INVESTIGACIÓN DE DELITOS INFORMÁTICOS. *Sujetos del delito informático.* Disponible en :<http://www.irdaoc.com/irdaoc/documentos/PIDAT_II_2010/GRUPO_4_ANALISIS_DE_PROCESO_DELITOS_INFORMATICOS.pdf>.

— AGENCIA EUROPEA DE SEGURIDAD DE LAS REDES Y DE LA INFORMACIÓN (ENISA).Disponible en: <http://europa.eu/legislation_summaries/justice_freedom_security/fight_against_organised_crime/l24153_es.htm>.

— BELTRÁN FUENTES, Fernando Patricio; BELTRÁN FUENTES, Soraya Viviana. “Derecho Informático”. Publicado: Miércoles, 27 de mayode2009.Disponible en:<http://www.derechoecuador.com/index.php?option=com_content&task=view&id=4980>.

— COMUNICADOS DE PRENSA DE LA COMISIÓN EUROPEA. "Declaración sobre el lanzamiento de la Alianza Global contra el abuso sexual infantil en línea". MEMO/12/944. Disponible en:<http://europa.eu/rapid/press-release_MEMO-12-944_en.htm>

— COMUNICADOS DE PRENSA DE LA COMISIÓN EUROPEA. "Centro Europeo de Ciberdelincuencia (CE 3) se abre el 11 de enero". IP/13/13. Disponible en: <http://europa.eu/rapid/press-release_IP-13-13_en.htm>

— COMUNICADOS DE PRENSA DE LA COMISIÓN EUROPEA. "El Centro Europeo de Ciberdelincuencia CE 3". MEMO/13/6. Disponible en: <http://europa.eu/rapid/press-release_MEMO-13-6_en.htm>

— COMUNICACIÓN CONJUNTA AL PARLAMENTO EUROPEO, AL CONSEJO, AL COMITÉ ECONÓMICO Y SOCIAL EUROPEO Y AL COMITÉ DE LAS REGIONES: "Estrategia de ciberseguridad de la Unión Europea". Disponible en: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=JOIN:2013:0001:FIN:ES:PDF >

— MINISTERIO DE ASUNTOS EXTERIORES Y DE COOPERACIÓN. "*Convenio sobre la Ciberdelincuencia*" Disponible en: <http://www.agpd.es/portalwebAGPD/canaldocumentacion/legislacion/consejo_europa/convenios/common/pdfs/Convenio_Ciberdelincuencia.pdf>

— MINISTERIO DE ASUNTOS EXTERIORES Y DE COOPERACIÓN. "*Protocolo adicional al Convenio sobre la ciberdelincuencia relativo a la penalización de actos de índole racista y xenófoba cometidos por medio de sistemas informáticos*". Disponible en: <https://www.gdt.guardiacivil.es/webgdt/media/Legislacion/Protocolo_adicional_convencion_cibercrimen.pdf>.

— DICCIONARIO DE LA REAL ACADEMIA ESPAÑOLA. Disponible en: <http://lema.rae.es/drae/?val=informatica>.

— DEL PINO, Santiago Acurio. "*Delitos informáticos: Generalidades*". Profesor de Derecho Informático de la PUCE. Disponible en:<http://www.oas.org/juridico/spanish/cyb_ecu_delitos_inform.pdf>.

— MOJICA, Germán. "*Informática jurídica: relación con el Derecho civil- Contratos informáticos*". Publicado 6 de Junio del 2009. Disponible en:<http://informaticajuridicausco.blogspot.com/2009/06/relacion-con-el-derecho-civil-contratos.html>.

— PANORAMA DE EUROPOL. "Informe general sobre las actividades de Europol". Disponible en: <https://www.europol.europa.eu/sites/default/files/publications/es_europolreview.pdf>

— VERSION CONSOLIDADA DEL TRATADO DE LA UNION EUROPEA [en línea] Disponible en: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2010:083:0047:020:es:PDF>

— VERSION CONSOLIDADA DEL TRATADO DE FUNCIONAMIENTO DE LA UNION EUROPEA [en línea] Disponible en: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2010:083:0047:0200:es:PDF>