Resumen

El ensayo Jurídico denominado “Los delitos informáticos: La insuficiente e inadecuada protección penal en el ordenamiento jurídico ecuatoriano”, contempla las deficiencias de tipificación de los delitos cometidos a través de medios informáticos y contra ellos. El estudio en cuestión plantea los tres pilares fundamentales para lograr una protección penal idónea, armonizada con las legislaciones locales de Estados desarrollados, que constituyen un ejemplo de las mejores prácticas internacionales; así como con los estándares internacionales, los cuales han sido impulsados por los organismos internacionales y los no gubernamentales.

Los tres pilares son:

1. Una política criminal que permita prevenir el cometimiento de los delitos informáticos, a través de la implementación de controles técnicos que garanticen la seguridad de las redes y exijan la autenticación de los usuarios.
2. La tipificación adecuada y actualizada de las posibles conductas ilícitas cometidas en sistemas informáticos o a través de ellos.
3. El fortalecimiento, capacitación y especialización en las instituciones de justicia y policía que permitan perseguir y sancionar al delincuente informático.

Por la amplitud del tema, este ensayo jurídico se enfoca en el segundo pilar mencionado.

El presente estudio ha recogido opiniones doctrinarias de expertos de diversos países, haciendo un recuento histórico que permite distinguir los hitos que han marcado la evolución del conocimiento en esta área. Para ello, he tomado como punto de partida el año 1992 por considerarlo clave para el desarrollo tecnológico que nos compete.

Abstract

The judicial essay by the name of “Computerized Crime: Insufficient and inadequate criminal protection afforded by the Ecuadorian Judicial Framework” envisages the deficiencies that exist in classifying the crimes perpetrated through computerized devices and against them. The analysis in question establishes the three fundamental pillars aimed at attaining an ideal criminal protection that is fine-tuned to the local legislation of those developed countries, which constitute an example of the best international practices; as well as to international standards that are being promoted by the international, non-governmental organizations.

These pillars are:

1. A criminal policy that provides for the prevention of computerized crime, through the implementation of technical controls that guarantee the safety of networks and that demand the authentication of users.
2. Appropriate and updated classification of the potential illicit behavior that entails the use of computerized systems.
3. Strengthening, training and specialization of the justice and police institutions, thus allowing for the pursuit, prosecution and sanctioning of the informational criminal.

Given the broad spectrum of the issue, this judicial essay has gathered doctrine-related opinions originating among experts of various countries, along with a historical recapitulation that facilitates identification of the diverse benchmarks found along the evolution of knowledge in this field. To this end, 1992 has been taken as the starting point given the fact that is a key for the technological development that concerns us.

ÍNDICE

CAPÍTULO II
EL DELITO INFORMÁTICO

CAPÍTULO III

PROBLEMAS RELATIVOS A LA TIPIFICACIÓN DE LOS DELITOS INFORMÁTICOS

CAPÍTULO IV
LA PROTECCIÓN PENAL FRENTE A LA
DELINCUENCIA INFORMÁTICA EN EL ECUADOR

CAPÍTULO I

LA INFORMÁTICA JURÍDICA Y EL DERECHO INFORMÁTICO

La informática jurídica y el Derecho Informático han sido, durante algunos años, materia de estudio por parte de los juristas. Durante muchos años, la informática jurídica fue concebida como parte integrante del Derecho Informático. Con el paso de los años, fue madurando la concepción de que la informática jurídica es una herramienta tecnológica, que, aplicada al Derecho, potencia la actividad del jurista.

Para ubicar claramente los delitos informáticos dentro del Derecho, es importante clarificar, brevemente, el lugar en que se ubican estos conceptos. Dentro de este capítulo se desarrollará el tema de la Informática Jurídica y el Derecho Informático.

I.1 LA INFORMÁTICA JURÍDICA EN LA SOCIEDAD ACTUAL. DESARROLLO Y PERSPECTIVAS

La evolución de la informática jurídica data, aproximadamente, de fines de la década de los cincuenta. En este tiempo ha presentado modificaciones importantes, tanto en el ámbito tecnológico, gracias al desarrollo vertiginoso que se ha producido

en este aspecto; como en la visión doctrinaria hacia esta materia. Por ello, es necesario realizar un breve análisis, enfocado a la informática jurídica, tomando en consideración los distintos hitos que marcan, claramente, esta evolución y que permiten visualizar hacia donde se dirige el tratamiento de esta materia en el futuro. Para ello, se ha escogido doctrina de juristas de diversos países con la finalidad de dar un concepto globalizado del tema, que marque pautas generales; aceptadas, por la mayoría de Estados. Sin embargo, para evitar caer en un análisis, que por tratar de ser retrospectivo, llegue al absurdo de analizar textos desactualizados, debido al gran avance tecnológico del tema; se ha escogido el año 1992, como punto de partida en virtud de que, si bien existe un período de aproximadamente 15 años de evolución, lo cual permite encontrar avances y diferencias; al mismo tiempo es un período que no llega a ser excesivamente extenso como para distorsionar el sentido que tiene el análisis de este tema como parte integrante de este estudio.

I.1.A RELACIÓN ENTRE EL DERECHO INFORMÁTICO Y LA INFORMÁTICA JURÍDICA

Hace 12 años, el argentino Enrique Falcón publicó su libro titulado "¿Qué es la informática Jurídica? Del ábaco al Derecho Informático", en el cual aclaró las diferencias existentes entre la informática jurídica y el Derecho informático, al mismo tiempo que destacó las características de cada uno de ellos. En este numeral se expondrán aquellos que tienen relación con la informática jurídica, dejando las referentes al Derecho Informático, para el siguiente numeral.

Falcón define a la informática como "una disciplina que incluye diversas técnicas y actividades relacionadas con el tratamiento lógico y automático de la información". [1] Esta definición se enmarca en que, como lo explica el citado autor, la

[1] Enrique Falcón; *¿ Qué es la Informática Jurídica? Del Ábaco al Derecho Informático*; 1992. Página 11.

denominación de informática deviene de la unión de dos términos: información y automática.

Es interesante conocer cómo se relaciona la computación con la informática y por qué se entiende que la informática necesariamente tiene relación con los computadores. Falcón nos explica que la aparición de los computadores acaparó rápidamente el término "informática" para las tareas que realizaban y como consecuencia de ello, comunmente se define a la informática como aquello relacionado con el proceso de datos, con los computadores y su empleo, en el sentido más ampio posible. A raíz de ello, se denomina como "preinformática" a la informática que existía antes de las computadoras. De ello concluye el autor, que la computadora ha creado "una cultura informática propia".

Para Jijena Leiva, jurista chileno, la informática jurídica es concebida como "la ciencia que estudia y tiene como objeto el tratamiento automatizado o electrónico de la información". [2] Aunque el libro mencionado fue publicado en el mismo año que el de Falcón, es claro que este autor se ha enfocado en la informática jurídica, desde la aparición de las computadoras; ya que su concepto del tema, necesariamente incluye el tratamiento automatizado o electrónico de la información, dejando de lado el tema de la etapa preinformática de la que nos habla Falcón.

Explica, que "entre el derecho y la informática existen dos grandes tipos de interrelaciones. Si se considera solamente el aspecto instrumental de la informática al servicio del derecho, se está en el campo de la informática jurídica; si se considera a la informática en general, como objeto de estudio jurídico, entramos en el ámbito del derecho informático." [3]

Por su parte, el español Antonio Enrique Pérez-Luño, tiene un concepto de avanzada respecto de la informática jurídica. Su definición se enmarca en un

[2] Renato Javier Jijena Leiva; *Chile,la Protección Penal de la Intimidad y el DelitoInformático*; 1992. Página 15.
[3] Renato Javier Jijena Leiva; *Chile,la Protección Penal de la Intimidad y el DelitoInformático;* 1992. Página 17.

concepto muy utilizado hoy en día, el concepto de Sociedad de la Información. Así, dice: "la informática jurídica tiene por objeto la aplicación de la tecnología de la información al Derecho"[4]. Más adelante dice que Estudia el tratamiento automatizado de: las fuentes de conocimiento jurídico, a través de los sistemas de documentación legislativa, jurisprudencial y doctrinal (informática jurídica documental); las fuentes de producción jurídica, a través de la elaboración informática de los factores lógico formales que concurren en el proceso legislativo y en la decisión judicial (informática jurídica decisional); y los procesos de organización de la infraestructura o medios instrumentales con los que se gestiona el Derecho (informática jurídica de gestión).

En el año 1999, el jurista ecuatoriano Pablo Yánez Narváez hace una explicación completa de la informática, en su libro "Introducción al Estudio del Derecho Informático e Informática Jurídica". Este autor divide a la informática en dos ramas generales, desde el punto de vista de su utilidad. Así, define a la informática como una ciencia por ser "un conjunto de técnicas, métodos y máquinas aplicadas al tratamiento automático y lógico de la información"; y como una actividad científica por estar "dirigida a la investigación de los medios que permite el tratamiento y elaboración en forma automática de las informaciones necesarias para el desarrollo de las actividades humanas."[5]

A su vez, la informática jurídica como ciencia, se divide para este autor en dos ramas; la informática jurídica fundamental y la informática aplicada. La primera se encarga de los fundamentos teóricos, técnicos y prácticos del tratamiento automatizado de datos; la cual se divide en 3 áreas: la informática teórica, que tiene su origen en los años sesenta, y es "aquella que arranca desde que se da una formulación matemática exacta del concepto intuitivo de algoritmo mediante modelos matemáticos hasta el estudio actual que constituye el lugar de convergencia de las

[4] Antonio Enrique Pérez-Luño; *Manual de Informática y Derecho*; 1996. Página 22.
[5] Pablo Yánez Narváez; *Introducción al Estudio del Derecho Informático e Informática Jurídica;*1999. Página 46.

ciencias informáticas y matemáticas se encarga del estudio de áreas como la teoría de los autómatas, teoría de los lenguajes, teoría de las funciones, teoría de la complejidad y teoría de la programación". La informática jurídica técnica, la cual surgió en los años ochenta, "constituye el lugar de convergencia con la electrónica y se encarga del diseño y construcción de sistemas informáticos, estudiando los circuitos, mircroprogramación, estructura de las computadoras, en general, hace referencia a la construcción de computadores".[6] Por último está la informática práctica, la cual desarrolla métodos generales para la programación de sistemas y construcción de programas. Busca confiar los trabajos al computador, sin necesidad de que tenga que conocer los detalles específicos de la estructura interna. Este estudio surgió a partir de los años cincuenta con la introducción de los lenguajes de programación.

Por otro lado, la Informática Aplicada es el uso de la informática a otras ciencias, principalmente de la informática técnica y práctica. Yánez Narváez la define como "la utilización de los medios informáticos para la guía, solución, agilidad o reducción de costos de los procesos o investigaciones utilizados en otras ciencias"[7]; así, en el caso del Derecho, la informática jurídica.

De este modo, la informática jurídica no constituye una ciencia autónoma, sino el resultado que la informática le ofrezca en su beneficio. No es una rama del derecho, es una aplicación de una ciencia matemática, aplicada a la actividad jurídica, con el fin de facilitar las tareas del jurista. Poco a poco, se comienza a comprender que la informática jurídica no constituye una parte del Derecho Informático, como se creía en años anteriores. Siguiendo al autor, el objeto de la informática jurídica es la "aplicación de las tecnologías de la información, al Derecho".[8] Define a la informática jurídica como "todo procedimiento electrónico, telemático o en general científico de tratamiento de la información que permite la

[6]Ibidem. Página 47 y 48.
[7]Ibídem. Página 48.
[8] Pablo Yánez Narváez; *Introducción al Estudio del Derecho Informático e Informática Jurídica;* 1999. Página 77.

actualización, mejora, desarrollo de los sistemas y procesos en materia jurídica, participando además en la solución de sus problemas".[9]

Para el español Eugenio Ull Pont, la informática jurídica "supone el estudio y la aplicación de las tecnologías informáticas como instrumento en el campo del Derecho, que deviene en Informática Judicial, en cuanto presta sus recursos conforme a las necesidades de la Judicatura y su entorno. Se trata de poner la informática al servicio de la actividad jurídica, en diversas manifestaciones". [10]

En el año 2000, la jurista argentina Andrea Viviana Sarra, en su libro "Comercio Electrónico y Derecho", aclara el concepto de sociedad de la información y la comunicación, ya introducido por Pérez-Luño en el año 1996. Sarra explica que a finales del siglo XX, se produjo una expansión del conocimiento humano de una manera exponencial, nunca antes vista. El conocimiento humano tuvo un ritmo de crecimiento lento hasta 1950. Desde este año, los intervalos de tiempo existentes entre los distintos niveles de crecimiento del conocimiento humano, se ven disminuidos notablemente. Ha llegado a tales niveles de crecimiento, que Sarra considera que "hasta el mismo cambio cambia".[11] Este crecimiento exponencial del conocimiento, se debe a que el mundo entró en una nueva sociedad, la Sociedad de la Información y la Comunicación, la cual se caracteriza por estar impulsado por las denominadas tecnologías de la información y la comunicación (TIC´s).

La palabra tecnología se compone de dos palabras; "tecno", que significa habilidad técnica o pericia, y "logía", que significa conocimiento sistematizado y organizado. La doctrina distingue entre las tecnologías tradicionales y las nuevas tecnologías. Las tecnologías nacidas antes de la Segunda Guerra Mundial se relacionan, salvo excepciones, con la automatización mecánica y son las denominadas tecnologías tradicionales. Las nuevas tecnologías son aquellas

[9] Ibídem. Página 79.
[10] Eugenio Ull Pont; *Derecho Público de la Informática (Protección de Datos de Carácter Personal)*; 2000. Página 31.
[11] Andrea Viviana Sarra; *Comercio Electrónico y Derecho*; 2000. Página 7.

nacidas con posterioridad a la segunda Guerra Mundial y se caracterizan porque su evolución y desarrollo se han manifestado de forma acelerada, con una magnitud de trascendencia nunca antes vista en la historia de la humanidad. Es decir, son aquellas tecnologías pertenecientes al desarrollo de la sociedad de la información. Estas nuevas tecnologías se dividen en tres grandes grupos: las biotecnologías, dentro de las cuales se encuentra la ingeniería molecular y la genética; los nuevos materiales, que son nuevos procesos en función del mejoramiento de materiales tradicionales y desarrollo de materiales nuevos; y las tecnologías de la información (TIC´s), que engloban "todo aquello que implique la creación, procesamiento y transmisión de señales digitales y está conformada por hardware, software, cibernética, sistemas de información, redes, chips inteligentes, criptografía, robótica, inteligencia artificial y realidad virtual"[12]

Sin embargo, aún en el año 2003, existe parte de la docrtrina que se niega a reconocer que la informática jurídica no se subsume al Derecho Informático. Este es el caso del jurista peruano Juan José Blossiers Hüme, quien considera que la informática jurídica es una subárea del Derecho Informático. Considero que es un error considerar a la informática jurídica como una rama del Derecho, ya que, como explica Sarra, es evidentemente coincidente con la tecnología y no con el Derecho. Es interesante exponer su opinión, por el hecho de que, aún en estos tiempos, cuando se habla de inteligencia artificial, sistemas neuronales artificiales y robótica, existe discusión en la doctrina jurídica sobre la ubicación de la informática dentro del Derecho.

En la actualidad, queda claro para la mayoría de la doctrina, que la informática es una herramienta que facilita el trabajo de los ciudadanos en distintas áreas profesionales; la cual, debido a sus características se ubica dentro del área tecnológica. Esta herramienta, de orden técnico- computacional, por motivos de utilidad social, se adapta a las necesidades de los juristas; lo cual no la convierte en

[12] Ibídem. Página 12.

parte integrante del Derecho Informático, sino que simplemente facilita las tareas de quienes trabajan en el campo del Derecho.

I.1.B VENTAJAS Y DESVENTAJAS QUE TRAE CONSIGO LA INFORMÁTICA JURÍDICA

Falcón realiza un escueto análisis de las ventajas y desventajas que trae la informática, lo cual, aunque parece obvio desde la perspectiva actual, permite visualizar con claridad la rapidez con que se desarrolla la tecnología. Por ello, se exponen brevemente: los pasos previos a la informatización; es decir, todas aquellas acciones que deben ser realizadas antes de informatizar un sistema son indispensables para su implementación; entre las cuales están: la formación de la conciencia informática (en la cual se debe dejar en claro que la informática no sustituye al hombre, sino que le dota de herramientas que le posibilitan a la mejor realización de estas tareas); un estudio previo del sistema existente, previa informatización, con el fin de descubrir los errores y falencias de este y corregirlas antes de informatizar el sistema; racionalización de trámites (para evitar la repetitividad interna de los programas, que se pueden dar por la existente repetitividad de trámites); y, la formación del personal que trabaje con el sistema.

Las ventajas son la velocidad y orden que brinda la implementación de un sistema informatico. Explica que para el jurista se vuelve fácil el manejo de grandes cantidades de informacíon que, antes de la informatización, eran casi imposibles de conocer. Por otro lado, expone como problemas derivados de la informatización, el perjuicio que causa a la vista el uso de monitores por períodos prolongados de tiempo; crea una personalidad individualista y poco sociable en las personas, y se necesita de un fluido eléctrico permanente para evitar la pérdida de información. Los aspectos señalados, sobretodo los negativos, han sido superados en el transcurso

de estos últimos 12 años. De aquí, que los argumentos explicados solo sirven para demostrar el vertiginoso desarrollo de la tecnología.

I.1.C ELEMENTOS

Yánez Narváez considera que existen cuatro elementos indispensables para alcanzar una adecuada evaluación del tratamiento automatizado de datos jurídicos. Así, debe ser eficiente, lo cual se determina cuando se ha permitido alcanzar la mayor cantidad de información o datos solicitados del banco de datos que ofrezcan información relacionada con la solicitada. Debe ser aprovechable, que se mide por la relación entre el uso efectivo de información recuperada, frente al máximo uso posible del sistema. Accesible, es decir, que el acceso a la información requerida sea fácil de manejar y con una orientación clara. Por último debe ser ágil, que se mide por el tiempo transcurrido entre el momento que se realiza la solicitud de información al computador y el momento en que se obtiene una respuesta; no sería útil la informática jurídica si no cumpliera con este último requisito, es decir, la capacidad de aumentar la velocidad operativa, conforme se va desarrollando.

I.1.D CLASIFICACIÓN

Falcón expone la clasificación realizada por López Muñiz Goñi por considerarla apropiada para explicar la informática jurídica. Este autor clasifica a la informática jurídica en tres ramas: la informática jurídica operacional, dedicada a la gestión de juzgados, estudios jurídicos y cámaras legislativas; la informática jurídica registral, relacionada con los registros públicos; la informática jurídica decisional, con la resolución automática de casos respectivos y la informática jurídica documental, relacionada con los bancos de datos jurídicos.

El autor en cuestión explica que existen tres visiones sobre la informática jurídica: una amplia, una intermedia y una limitada. Se inclina por la visión amplia que considera a la informática jurídica como toda cuestión de derecho relacionada con la informática. Al respecto entra en la denominada informática jurídica la llamada iuscibernética (lo cual comprende las relaciones jurídicas provinientes de la cibernética; es decir, de la ciencia que estudia los sistemas de control y comunicación de los animales y máquinas), las cuatro categorías de informática jurídica antes mencionadas y el Derecho informático. A esta visión amplia de la informática jurídica se la denominará iurismática o deremática. Así, la informática jurídica se entenderá como la relación existente entre la máquina y el ordenador.

Jijena Leiva distingue tres tipos de informática jurídica: el sistema de informática jurídica aplicada, de gestión o administrativa, la cual se divide en la informática decisional, informática registral y la informática operacional; el sistema de informática jurídica documental o de las fuentes del derecho y el sistema de informática jurídica mixto.

Los sistemas de informática jurídica aplicada se orientan a la administración y control de la información jurídica. La informática decisional, se explica como "la mecanización del proceso de razonamiento jurídico. Su estudio implica adentrarse en temas como la inteligencia artificial (la imitación por medio de programas computacionales de algunas aplicaciones del cerebro humano) y los sistemas expertos (programas capaces de realizar operaciones sobre una materia específica con un alto grado de eficiencia)."[13] Por su parte, la informática jurídica registral retiene y actualiza, de manera permanente, información de carácter histórico. Por ello, es de gran interés para notarios o registradores. La informática jurídica decisional se ocupa de diligenciar la información producida dentro de la actividad judicial.

[13] Renato Javier Jijena Leiva; *Chile,la Protección Penal de la Intimidad y el DelitoInformático;* 1992. Página 15.

Los sistemas de informática jurídica documental se utilizan para recuperar automáticamente, mediante sistemas informáticos, toda información jurídica para facilitar al jurista el manejo de la enorme cantidad de textos que debe consultar.

Los sistemas de informática jurídica mixtos son sistemas que abarcan funciones documentales y, adicionalmente, se ocupan de las gestionales.

Pérez- Luño destina tres capítulos de su libro a la explicación de las tres fuentes de la informática jurídica. De esta explicación profunda, mencionaré sus características brevemente. Distingue tres clases de informática jurídica: la informática jurídica documental, la informática jurídica de gestión y la informática jurídica decisional. Explica que la IJ documental se refiere a la automatización de las fuentes de conocimiento jurídico. Hace notar que gracias a la teledocumentación, el jurista se halla en posibilidad de acceder, desde cualquier punto interconectado, a toda información que se encuentre situada en los distintos bancos de datos a los cuales se accede por estas redes telemáticas. Los sistemas de teledocumentación constituyen la respuesta tecnológica al fenómeno de la explosión bibliográfica, rasgo característico de la sociedad de la información. A las consecuencias de la sociedad informatizada, Pérez-Luño ha denominado "la crisis de inabarcabilidad de la información jurídica"[14]. Así, frente a esta crisis, se debe buscar una respuesta tecnológica que permita superarla. Así, "la imagen del jurista investigador artesano, que consume su tiempo en una lenta, paciente y trabajosa búsqueda de fuentes, que una vez identificadas, deberán localizarse a través, muchas veces, de un costoso peregrinaje intelectual, ha devenido obsoleta."[15] Frente a ello, el jurista de la sociedad de la información puede obtener, mediante el acceso a bancos de datos informatizados, las siguientes e importantes ventajas: posibilidad de maximizar y optimizar el campo temático de consulta; rapidez e incluso, inmediatez de acceso a la información existente, y ahorro en los costos de adquisición de materiales

[14] Antonio Enrique Pérez-Luño; *Manual de Informática y Derecho*; 1996. Página 134.
[15] Ibidem. Página 135.

bibliográficos, ya que solamente se reproduce en papel aquella información extremadamente relevante para la investigación.

Los problemas que se pueden presentar, a criterio de Pérez-Luño, en el campo de la informática jurídica documental son técnicos y dentro de ellos, pueden ser, operativos, linguísticos, y, lógicos e informáticos.

Los problemas operativos se pueden producir por diversas causas, entre los cuales figuran el elevado costo de plasmar en medios informáticos el texto completo o “full-text” que es el sistema usado por los norteamericanos, el carácter vago e impreciso del sistema de referencias, aunque su costo es bajo por su simplicidad y la escasa integridad que plantea un sistema de abstracts o resúmenes, el cual se ha solucionado, parcialmente, con la idea de que dichos resúmenes sean realizados por quienes escriben originariamente el texto completo para no dejar de lado su sentido y así evitar que se desvirtúe su sentido.

Por otro lado, es un presupuesto necesario para informatizar la documentación jurídica el elaborar un lenguaje jurídico preciso, unívoco y coherente. Los problemas lingüísticos se producen cuando no se logran estos presupuestos; lo cual puede suceder por diversas causas como la homonimia, lo cual hace referencia a aquellos términos que tienen idéntica forma, pero distinto significado; la polisemia, lo cual se produce cuando existe pluralidad de significados de una misma palabra; o la sinonimia, que es el contrario a la homonimia, es decir, palabras diferentes en su forma, pero de idéntico significado. Para resolver estos problemas de lenguaje jurídico es necesario convertir el lenguaje jurídico en un lenguaje simbólico suceptible de procesamiento informático. Para combatir estos problemas, Pérez-Luño describe la existencia del “Thesaurus”, al cual lo define como “un conjunto ordenado, jerarquizado y dinámico de términos o descriptores que forman un cuerpo documental de un determinado campo de conocimiento”; es decir, se trata de un “instrumento de clasificación y ordenación de textos y documentos en función de sus

relaciones semánticas de analogía, vecindad, inclusión o jerarquía."[16] Explica que este sistema opera en tres niveles: primero, identificando las nociones jurídicas solicitadas y ubicándolas a sus descriptores; en segundo lugar, conectando estas nociones con otras afines o sinónimas; y por último, excluyendo aquellas nociones irrelevantes, impertinentes o redundantes. De este modo, se superan los problemas linguísticos mencionados.

Por último, existen problemas lógicos e informáticos, los cuales se solucionan mediante los diagramas de Euler Venn, los cuales sirven para explicar, de forma gráfica, la jerarquía de redes de relaciones lógicas entre diferentes áreas, clases o conjuntos que se interconectan por diversos puntos. Así, al unir varios conjuntos, se forma un espacio en donde todos ellos se juntan y coinciden por tener puntos en común. Esta información es la que debe ser presentada y así, se solucionan los conflictos que pueden producirse en el campo lógico e informático.

La Informática Jurídica de Gestión, la cual se ha desarrollado en los últimos años (aproximadamente a principios de los noventa), y que se refiere a la ofimática o burótica, lo cual alude a la expresión inglesa "office automation". Esta denominación se refiere a la automatización de las tareas rutinarias que se llevan a cabo en cualquier oficina. Este sistema busca lograr resultados "más uniformes, imparciales, transparentes, rápidos y económicos", para que los juristas y jueces se dediquen solamente a aquellas tareas que exigen una actividad creadora.

Por su parte, la informática jurídica decisional o metadocumental "es aquella integrada por procedimientos dirigidos a la sustitución o reproducción de las actividades del jurista. Es destinada a ofrecerle soluciones de problemas y no mera documentación sobre ellos."[17] Explica que en este punto se aplica la inteligencia artificial y los sistemas expertos. "La inteligencia artificial es el conjunto de

[16] Antonio Enrique Pérez-Luño; *Manual de Informática y Derecho*; 1996. Página 152.
[17] Ibidem. Página 24.

actividades informáticas que si fueran realizadas por el hombre se considerarían producto de su inteligencia.” “Los sistemas expertos son programas que reproducen las actuaciones que ha previsto el experto que los diseña.” Distingue como los sistemas expertos más usados los destinados a diseño artístico o arquitectónico, a la localización de yacimientos minerales y el diagnóstico médico. Han proliferado proyectos de sistemas expertos en materias tales como liquidaciones tributarias, cálculo de indemnizaciones por accidentes laborales o de tráfico, predicción de consecuencias jurídicas de impactos medioambientales, condiciones de adquisición de nacionalidad y Derecho de familia (matrimonio y divorcio). Existe hasta el momento una fuerte resistencia por parte de la doctrina y de los profesionales del derecho, en utilizar técnicas de inteligencia artificial al Derecho, aunque solo sea para brindar apoyo a decisiones o ampliar la gama de soluciones posibles. Con el paso del tiempo, el desarrollo y utilización de estos sistemas en otras disciplinas, disminuirá esta resistencia y las adoptará poco a poco para que sean utilizadas en el campo jurídico.

Cabe enfatizar la aclaración que realiza Pérez-Luño acerca del uso de sistemas expertos y de inteligencia artificial para realizar las tareas del jurista. Recalca que este sistema es muy eficaz para tareas relacionadas con matemáticas, pero muy peligroso para aquellas tareas relacionadas con las ciencias sociales, y en especial, con la ciencia jurídica. Explica que no es fácil realizar un balance entre la realidad actual y las perspectivas para el futuro de los sistemas expertos aplicados al Derecho, ya que su mutación y progreso es constante. Sin embargo, reflexiona sobre las consideraciones que se han dado hasta el momento en que escribió ese libro. De ellas, las más relevantes, a mi criterio, se resumen en la necesidad de evitar que la evolución de los sistemas expertos confundan, tanto a juristas como a técnicos en computación en dos aspectos; a los juristas, en creer que los sistemas expertos van a reemplazar su actividad creadora y de razonamiento, necesario para cada caso concreto; y que los técnicos, a su vez, consideren que los sistemas expertos son aplicables a todas las materias, sin excepción, y que por ello, dejen de

observar la dificultad de aplicarlos al derecho. Si esto ocurre, el tratamiento legal de los casos va a ser normalizado y no va a ser profundizado con el nivel de responsabilidad e individualidad necesarias para generar derecho. Existen muchas críticas respecto de lo que sucederá con la aplicación de esta rama de la informática jurídica al Derecho; de ellas, las más cercanas a la realidad son aquellas que integran, los puntos positivos de cada polo de opinión y que logran un análisis más pormenorizado y menos fanático del tema. Sin embargo, no existe una manera de conocer lo que pasará en el futuro, se espera que sea una adaptación de la informática al Derecho con el fin de apoyar a los juristas en su tarea, sin que esto signifique una deshumanización de las decisiones, que integran varios criterios y que son productos propios de la inteligencia humana. Se debe tener claro que las máquinas pueden apoyar al ser humano, pero no reemplazarlo.

Yánez Narváez sigue la clasificación hecha por Pérez-Luño y coincide con sus argumentos plenamente. Ull Pont, por su parte, sigue con esta misma clasificación, pero, sin embargo, se manifiesta reticente a la aplicación de la informática jurídica decisional, la cual se basa en inteligencia artificial y sistemas expertos, por motivos éticos y técnicos.

Sarra, con la inclusión del concepto tecnologías de la información y comunicación, replantea la ubicación de la informática jurídica en relación con el Derecho. Plantea que ubicar un término obsoleto como informática jurídica dentro del Derecho informático no cabe, por cuanto existe un campo de estudio específico, que no se subsume al Derecho, el de las Tecnologías de la Información y la Comunicación, que abarca a la informática en general. La informática nunca ha sido parte del Derecho; se la ha querido introducir como parte del Derecho informático por su utilidad en el campo jurídico. Sin embargo, es una rama independiente, transversal, que toca a muchas disciplinas, dentro de las cuales está el Derecho. Por ello, hablar de informática jurídica es hablar de un término inexistente. La informática afecta al derecho, pero no se puede hablar de una rama independiente denominada

informática jurídica. Coincido con Sarra en que la informática jurídica carece de sustrato jurídico en su esencia. Su esencia es tecnológica, por lo cual, el incluirla dentro de una rama del Derecho, como es el Derecho informático implica una invasión del campo tecnológico por el Derecho.

I.1.E ALGUNAS INICIATIVAS INTERESANTES ADOPTADAS POR DIVERSOS ESTADOS

Falcón cita las mejores fuentes de la informática jurídica en Argentina hasta el momento de la publicación de su libro. Entre ellas destaca el SAIJ (Sistema Argentino de Informática Jurídica), al que denomina el mayor banco de datos de la nación. Tiene registrado el sistema legislativo y recupera información de manera insuperable. Este sistema es un organismo dependiente de la Subsecretaría de Asuntos Legislativos del Ministerio de Justicia. Es de carácter público y su alcance es nacional. Nace en 1979 cuando el Poder Ejecutivo aprobó el Programa de Ordenamiento y Sistematización de la Legislación Nacional. Cita otros bancos de datos como el programa Microisis de la Unesco , el cual ordena la jurisprudencia de la provincia de Buenos Aires. Adicionalmente, expone como novedad el sistema de Albremática, creado en Argentina en 1989, mediante el cual una persona puede comprar un cd-rom con toda la información de los repertorios de jurisprudencia publicados en la revista jurídica el Derecho y la Revista Jurídica Trabajo y Seguridad Social de la misma editorial, con la posiblilidad de recuperar los fallos allí mencionados, más la totalidad de los códigos de fondo, la totalidad de los tratados internacionales ratificados por el país y un diccionario jurídico de tres tomos.

Falcón explica en su libro que la inteligencia artificial es una fantasía, por cuanto no existe, pero que puede llegar a existir en el futuro. Hoy en día, quienes han escrito sobre el tema en la actualidad, dicen que existe la inteligencia artificial y que se aplica en algunos aspectos para facilitar el trabajo de los juristas.

Jijena Leiva comenta como novedad que en la Universidad de Zaragoza, a través del Equipo de Investigación de Informática Jurídica, ha desarrollado un sistema experto sobre la base del derecho civil aragonés, información a la cual se accede utilizando categorías jurídicas. Este ejemplo fue mencionado el el X Curso Internacional de Informática y Derecho, realizado en Santiago del 10 de julio al 4 de agosto de 1989.

Yánez Narváez realiza un extracto en el cual explica cuáles son los mejores sistemas informáticos de algunos países de América y de Europa. A continuación expongo los más relevantes, tomando en consideración a aquellos países con los que el Ecuador se relaciona más.

- Estados Unidos: Lexis, la cual funciona desde 1973 y es la base de datos más grande del mundo. Acumula alrededor de 35 000 sentencias por año, y contiene sentencias extranjeras. Su competidor es Westlaw, sistema privado con sede el Nueva York, funciona desde 1975.
- Canadá: CADEPOL, base de datos del Ministerio de Justicia; DATUM; con sede en Québec y QUICK LAW; sistema dependiente de la Queen´s University.
- Argentina: SAIJ (Sistema Argentino de Informática Jurídica). Depende del ministerio de Justicia de la Nación y contiene información normativa jurisprudencial y doctrinaria.
- Brasil: PRODASEN, base de datos dependiente del Senado Federal. Contiene datos jurisprudenciales, normativos y doctrinarios, e incluso, algunos proyectos de ley.
- Bélgica: CREDOC, base dependiente de una asociación sin fines de lucro, creada en 1967 por la Federación de Notarios y por la Unión de Abogados de Bélgica. Funciona desde 1969.
- Francia: JURISDATA, base privada con sede en París, especializada en jurisprudencia y que opera desde 1974; CRIDON, con sede en Lyon, contiene información notarial y un sistema propio de investigación llamado SYDONI; IRETIJ, base especializada en jurisprudencia y doctrina, dependiente de la Universidad de

Montpellier; CEDIJ, dependiente del Consejo de Estado y del Tribunal Supremo. Se especializa en legislación y jurisprudencia y LEXIS, la mencionada base norteamericana que funciona también en algunos países de Europa.

- Reino Unido: LEXIS y EUROLEX, base normativa y jurisprudencial, que recoge información británica, así como de otros países europeos.

Eugenio Ull Pont hace énfasis en la necesidad de aplicar la informática jurídica en la función judicial. La llama informática jurídica judicial, y, siguiendo a Páez Maña, la define como "aquella parte de la informática jurídica que pretende lograr la optimización del trabajo desarrollado en las diferentes oficinas judiciales mediante la aplicación de la informática de gestión y la posterior interconexión entre las distintas oficinas, a fin de agilizar tanto la labor interna de los juzgados, como las relaciones entre los mismos, facilitando las notificaciones, traslados de expedientes, exhortos, etc., como la consulta directa de los bancos de datos jurisprudenciales, legislativos y doctrinales, creados por los servicios de los diferentes órganos jurisdiccionales, tendiendo a una cooperación y homogeneización práctica".[18]

Blossiers Hüme realiza una recopilación de los proyectos piloto más importantes que se han producido en el Perú en el campo judicial. Así, explica que se comenzó a realizar estos proyectos desde el año de 1974 y que por falta de recursos y de decisión política se los ha dejado de lado por considerarlos no prioritarios para el mejoramiento de la administración de justicia el hecho de implementar tecnologías informáticas en esta área. Entre éstos se pueden mencionar: el registro nacional de detenidos, que consiste en un banco de datos de los detenidos; el sistema de notificaciones, la cual tuvo éxito y opera actualmente y es administrado por el Colegio de Abogados de Lima en coordinación con el Poder Judicial; el Registro Central de Condenas, el cual inició como un proyecto de la Universidad Nacional Mayor de San Marcos en 1978 y fue retomada por el Poder Judicial en 1987 y ofrece

[18] Eugenio Ull Pont; *Derecho Público de la Informática (Protección de Datos de Carácter Personal);* 2000. Página 32.

los servicios de consulta automático a los juzgados y salas sobre información referente a la certificación jurisdiccional, atendiendo un promedio de 1500 a 2000 consultas por día. Tambíen ofrece sus servicios a los usuarios particulares en un promedio de 300 a 400 personas al día para la obtención de certificaciones con fines de estudios, viajes, entre otros. Tambíen existe el Consejo Supremo de Justicia Militar, quien ha asumido como una prioridad la automatización dentro de su institución. Por último existe el sistema mesa de partes única, que es dependiente del Poder Judicial, y se viene aplicando con éxito para los juzgados civiles de Lima y tiene por objeto mantener un sistema de ingreso de demandas mediante computadora, para las cuales se genera un código numérico automatizado, en función del cual se realiza la distribución de los casos a los diferentes juzgados de Lima. Este sistema se compone de tres etapas; la inicial consiste en el ingreso de expedientes a las bases de datos computarizadas; la segunda etapa consiste en instalar una red con el fin de enlazar o comunicar la oficina del juez con la del secretario; y la tercera etapa busca la automatización completa del expediente judicial mediante la introducción de equipos especiales que permitan la grabación óptica de textos, así como la filmación de imágenes y la grabación de voces. Incluso es posible actualmente realizar actos notariales a través de un portal, mediante el uso de correo electrónico, garantizando la identidad y voluntad de los solicitantes mediante firmas electrónicas. De este modo, se pueden realizar actos notariales sin necesidad de la presencia física de los solicitantes. El dinero correspondiente se abona mediante una transferencia electrónica en cuenta corriente y se registran los documentos a través de los Registros Públicos correspondientes, y recurriendo a fedatarios informáticos para la recepción de los testimonios de las Minutas respectivas. Este proceso todavía no se realiza en forma integral en el Perú, por ahora, debido a problemas de tipo normativo, de disponibilidad técnica de seguridad o de características de orden cultural. Sin embargo, la tendencia es clara y hacia allá se encaminan las notarías peruanas.

En Ecuador existen LEXIS y FIEL, dos sistemas privados que recogen datos normativos y jurisprudenciales. Ambos son competidores. Estos sistemas se implementaron en el Ecuador posteriormente a la publicación del libro de Yánez Narváez, por lo cual no constan en el cuadro. Adicionalmente, el Registro de la Propiedad del Cantón Quito ha creado una base de datos informatizada (informática jurídica documental) para ordenar archivos. Este proyecto viene funcionando desde 1993 y ha provocado una gran mejora en cuanto al tiempo de los trámites. Asimismo, se puede poner de ejemplo a los municipios de Quito y Guayaquil, los cuales han incluído en sus páginas web funciones interactivas para realizar investigaciones on-line. Se está promoviendo el e-government en el Ecuador, en muchas instituciones públicas, con lo cual se ahorra tiempo y recursos a los usuarios. El proyecto Quito Digital es un proyecto de avanzada en esta área.

Se busca lograr la aplicación de la informática jurídica de gestión en las notarías y registros públicos, así como en la Función Judicial. Yánez Narváez cita como ejemplo el caso de las notarías costaricenses, donde los notarios formulan consultas por módem al computador del Registro Nacional, y el caso mexicano, que ha permitido recolectar valiosa información histórica y analizar los cambios económicos y sociales de importancia desde 1929. Se piensa en la necesidad de implementar esta información en la Legislatura y en el Ejecutivo. Esto es gobierno electrónico.

I.2 EL DERECHO INFORMÁTICO. ÁMBITO

Como consecuencia de la sociedad de la información, el derecho vive un momento histórico, debe responder a los nuevos problemas producidos dentro de este nuevo entorno, a la celeridad y con la profundidad con que avanza la tecnología en general. Para ello, existe actualmente una rama del Derecho encargada de plantear soluciones en este campo, esta rama se denomina Derecho Informático.

Para Enrique Falcón, el Derecho Informático se ubica dentro de la *iurismática o deremática,* que ya fue explicada en el punto anterior. Así, Dentro de esta gran rama se ubican el Derecho Informático, la informática jurídica, la iuscibernética y las extensiones que cada área plantee. Para este autor, existe la duda sobre si el Derecho informático puede ser considerado como una rama independiente del Derecho. Plantea que la autonomía de una rama del Derecho no implica que deba separarse de la ciencia a la cual pertenece y de la cual depende, sino que aborde los problemas con métodos e instituciones propios. Así, debería asentarse en 4 pilares: en el campo normativo, deberá tener legislación específica; en el campo docente, estudio particularizado de la materia; en el campo científico, debe tener investigadores y doctrinarios que aborden los problemas específicos de la materia; y por útlimo, en el campo institucional (por tener instituciones propias que no se encuentren en otras áreas del Derecho). Aclara que el único elemento que no se ha dado, de manera completa, ni siquiera en el campo internacional, es en el área normativa, por lo cual, no se puede hablar aún de un Derecho informático. Esta realidad corresponde al año 1992, por lo cual, esta duda sobre la existencia o no del Derecho Informático ha quedado superada; actualmente, nadie discute de su existencia como una rama independiente del Derecho, la cual tiene características propias.

En el mismo año 1992, Jijena Leiva dejó claro que “al momento de realizar este estudio se encuentra suficientemente demostradas la pertinencia y validez del DI, lo que permite a la doctrina concebirlo como una rama autónoma y especializada en los problemas jurídicos que se presentan en torno al fenómeno informático.”[19]

Dentro del mismo orden de ideas, en Congreso Mundial de Derecho Informático, que tuvo lugar en Quito, en la Mitad del Mundo, en el año 2001, existen algunas ponencias interesantes, entre las cuales cabe resaltar, para este efecto, la

[19] Renato Javier Jijena Leiva; *Chile,la Protección Penal de la Intimidad y el DelitoInformático*; 1992. Página 20.

ponencia del conferencista venezolano Héctor Ramón Peñaranda Quintero, dentro de la cual explica: “Aquellos que niegan la autonomía del Derecho Informático, tendrán que analizar nuevamente los principios que rigen la autonomía de una rama del Derecho, por cuanto es evidente que estas características están contenidas contundentemente en el Derecho Informático. Con respecto a aquellos que consideran como rama potencial al Derecho Informático, deben tener cuidado, debido a que se podrían quedar con ese criterio de potencialidad para siempre, porque es de resaltar que el Derecho Informático, a diferencia de otras ramas del Derecho, no tiene ningún tipo de restricciones en su desarrollo, ya que éste siempre estará evolucionando en el tiempo hacia el futuro, y así como no se puede divisar el límite del desarrollo informático, tampoco el del Derecho Informático, debido a que éste siempre tratará de darle solución a los conflictos que surjan consecuentes del desarrollo de la tecnología. Este punto debe ser exaltado, porque una de las razones que sustenta la doctrina que estima potencial la autonomía del Derecho Informático, es que éste no da solución de inmediata a ciertas situaciones; al respecto este humilde autor responde, que por las características antes expuestas referentes a que el Derecho Informático constituye una rama atípica del Derecho, se encuentra sin límites visibles, siempre tratará de buscar protección y soluciones jurídicas a nuevas instituciones Informáticas, lo que no quiere decir, que no sea una rama autónoma del Derecho, al contrario, desarrollará aún más sus bases.”[20]

I.2.A OBJETO DEL DERECHO INFORMÁTICO

Eugenio Ull Pont define al Derecho Informático como “el conjunto de normas positivas referidas al tratamiento automatizado de la información y su comunicación, en su múltiples aspectos”.[21]

---

[20] Ponencia del Dr. Héctor Ramón Peñaranda Quintero; *El Derecho Informático como Rama Autónoma del Derecho;* Congreso Mundial De Derecho Informático; Alfa Redi_ OMDI; CdRom.
[21] Eugenio Ull Pont; *Derecho Público de la Informática (Protección de Datos de Carácter Personal*; 2000. Página 39.

Pérez Luño explica que el Derecho informático es una rama del Derecho que se debe concebir ampliamente. Debe concebirse como un Derecho Internacional, por cuanto su objeto rebasa los límites territoriales; por lo cual debe ser un derecho común a todos los países, o al menos, que se armonice entre las legislaciones informáticas de otros Estados. Al mismo tiempo, es un derecho transversal, por cuanto influye, tanto en el campo público como en el privado, que sin embargo, no constituye un conjunto de normas sueltas, sino que entraña una metodología propia.

El objeto de protección jurídica de esta rama del Derecho, es la información. En el sistema tradicional jurídico, se protege la propiedad de los bienes materiales, por lo cual, constituye un conflicto, aplicar dichas normas a la información, que constituye un bien inmaterial, pero que es susceptible de ser apropiado, al igual que los bienes materiales. Por ello, la naturaleza de esta rama del Derecho es distinta y debe ser tratada bajo otra óptica.

Pablo Yánez Narváez explica el problema que nos plantea el derecho informático consiste "en que los comportamientos y las actividades desplegadas con o en virtud de la tecnificación no se encuentran previstos por la legislación anterior y constituyen de este modo auténticas lagunas en los textos legales. Es posible, como pura operación mental, el encaje del hecho nuevo en una norma antigua, que prevea, no tal hecho en su singularidad, pero si, cuando menos, el tipo jurídico al que el hecho pertenece."[22] Acertadamente, en el año 2002, se dictó en el Ecuador la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, en la cual se aclaran algunos temas referidos al Derecho Informático. Por ello, este argumento del autor, aunque sigue siendo cierto en esta época por la insuficiencia de normativa en algunos sectores del DI, pierde fuerza por cuanto ya existe cierta normativa.

Pérez Luño define al Derecho informático como "el conjunto de disposiciones dirigido a la regulación de las nuevas tecnologías de la información y la

[22] Pablo Yánez Narváez; *Introducción al Estudio del Derecho Informático e Informática Jurídica;* 1999. Página 161.

comunicación, es decir, la informática y la telemática." [23] En este punto, considero que existe, como ya expliqué anteriormente, un error, ya que ni la informática ni la telemática son parte del Derecho, pertenecen a la tecnología. Las nuevas tecnologías de la información y la comunicación se refieren a tres aspectos distintos, de entre los cuales, el Derecho informático solamente se aplica a las TIC´s.

I.2.B PARTICULARIDADES

Para Jijena Leiva, el Derecho Informático se caracteriza por ser un "connubio indisoluble de normas de derecho público y privado, por ser imperfecto, al tener normas o principios que no arrancan exclusivamente de la ciencia jurídica, sino que son inherentes a la dinámica del desarrollo tecnológico; por ser dinámico y, en consecuencia, estar en constante evolución".[24]

Así, se consideran temas propios del derecho público la criminalidad informática, los aspectos probatorios de los medios informáticos, la protección de datos personales y nuevos principios como la libertad informativa, el flujo transfronteras y el derecho de acceso a la información. Por su parte, son temas del Derecho Privado, la tutela del software y la contratación informática. Sin embargo, el tratamiento del Derecho Informático merece un tratamiento unitario y globalizador que contribuya a su esclarecimiento.

A continuación explico los aspectos propios del Derecho Informático, público y privado:

I.2.B.1 Derecho Público Informático

[23] Antonio Enrique Pérez-Luño; *Manual de Informática y Derecho;* 1996. Página 18.

[24] Cita de Jijena Leiva a Eduardo Hajnar; *La enseñanza del Derecho Informático en los Estudios del Derecho;* ponencia presentada al I Congreso Iberoamericano de Informática Jurídica.

I.2.B.1.a Los Delitos Informáticos

La Sociedad de la Información no solo ha traído consigo un gran avance tecnológico que enriquece a la sociedad y proporciona herramientas que facilitan el trabajo, los negocios y el comercio; sino que consigo se han generado nuevas formas de criminalidad, desconocidas por el mundo jurídico hasta entonces.

Estas nuevas formas de criminalidad, que no han sido consideradas por el Derecho Penal tradicional, han sobrepasado los niveles de protección que los Estados habían destinado hasta entonces. Adicionalmente, las características típicas de los delitos penales tipificados antes de esta explosión de criminalidad son muy distintas de las características típicas de los delitos informáticos.

En el Ecuador, la protección penal frente a esta nueva forma de criminalidad es casi inexistente. Tenemos tipificadas 7 infracciones penales de este tipo desde el año 2002. Existe un vacío legislativo en lo referente al delito informático en el área penal. Adicionalmente, no existen políticas públicas de prevención, ni capacitación idónea para quienes persiguen y juzgan las actuaciones enmarcadas dentro de este tema.

La criminalidad informática no puede ser regulada por los tradicionales tipos penales, debido a los aspectos mencionados. En los próximos capítulos trataré este tema a fondo, por lo cual simplemente planteo que la delincuencia informática es parte integrante del Derecho informático, y que la protección penal existente en el Ecuador frente a esta realidad imperante, no es suficiente.

1.2.B.1.b Valor Probatorio de los Medios Informáticos

En este aspecto, es necesario proteger dos intereses: propiciar el uso de los medios tecnológicos existentes, de la manera más eficaz posible; y tutelar la confianza de todos los ciudadanos en la seguridad de los documentos generados y transmitidos por medios electrónicos.

La Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos establece, en su Art. 2 establece que “los mensajes de datos tendrán igual valor jurídico que los documentos escritos. Su eficacia, valoración y efectos se someterá al cumplimiento de lo establecido en esta Ley y su Reglamento”. De esta manera, otorga igual valor jurídico a los mensajes de datos que a los documentos escritos en papel. Para probar la validez de estos documentos es necesario que se garantice su integridad. Para ello existen las firmas electrónicas, establecidas del artículo 13 al artículo 18. El artículo 13 define a la firma electrónica como “los datos en forma electrónica, consignados en un mensaje de datos, adjuntados o lógicamente asociados al mismo, y que pueden ser utilizados para identificar al titular de la firma en relación con el mensaje de datos, e indicar que el titular de la firma aprueba y reconoce la información contenida en el mensaje de datos.”

Por su parte, el art. 14 establece los efectos de la firma electrónica disponiendo que “la firma electrónica tendrá igual validez y se le reconocerán los mismos efectos jurídicos que a una firma manuscrita en relación con los datos consignados en documentos escritos y será admitida como prueba en juicio.”

En este aspecto, dentro del ordenamiento jurídico ecuatoriano, existe el reconocimiento legal de que los mensajes de datos tienen el mismo valor jurídico que los documentos escritos en papel, lo cual es un gran adelanto.

1.2.B.1.c Protección de Datos Personales

La necesidad de tutelar la vida privada de los individuos constituye una exigencia de orden jurídico internacional. Dentro de este tema, se debe tutelar, a criterio de Jijena Leiva, "su recolección, correcta administración, permanente actualización, utilización para fines específicos e irrestricto derecho de acceso"[25]

Dentro de nuestro país, el derecho a la intimidad se recoge en el art. 23, numeral 8, de la siguiente manera: " Sin perjuicio de otros derechos establecidos en esta Constitución y en los intrumentos internacionales vigentes, el Estado reconocerá y garantizará a las personas los siguientes: ... num 8. El derecho a la honra, a la buena reputación y a la intimidad personal y familiar. La ley protegerá el nombre, la imagen y la voz de la persona;". De este derecho fundamental garantizado por la mayoría de Constituciones del mundo civilizado, nacen las siguientes figuras jurídicas y garantías constitucionales para hacer efectivo este derecho.

1.2.B.1.c.1 Libertad Informativa

Este aspecto interesa al Derecho Constitucional y Administrativo. Se refiere a la libertad que tiene cada individuo para determinar qué, quién y bajo qué circunstancias, se puede dar a conocer información referente a sí mismo. De este derecho, se deriva el Hábeas Data, que es una garantía procesal, constitucionalmente establecida, para hacer efectivo el respeto y aplicación del derecho a la libertad informativa o informática. Es decir, la libertad informática nace como un derecho nuevo de autotutela de la identidad informática; destinado a precautelar los datos de las personas.

---

[25] Renato Javier Jijena Leiva; *Chile,la Protección Penal de la Intimidad y el Delito Informático*; 1992. Página 30.

Yánez Narváez explica las doce reglas a seguir para lograr que los datos personales sean respetados, dentro del derecho de libertad informativa, al ser manejados y tratados automáticamente. De esta manera, los datos deben ser: 1) lícitos: tanto en su recopilación, como en su uso; 2) determinados, es decir, que solo puedan ser usados para la finalidad para la que fueron recopilados; 3) pertinentes, es decir, que sean exactos y completos; 4) actualizados, que respondan con veracidad a la situación actual de su titular; 5) temporales, es decir, que no serán conservados en forma que permita la identificación del interesado durante un período que sea mayor al necesario para cumplir los fines para los cuales se recopilaron dichos datos; 6) accesibles, almacenados de tal forma que permita el derecho de acceso de su titular; 7) rectificables, que admitan la posibilidad de rectificación; 8) cancelables, que admitan la posibilidad de ser borrados fácilmente; 9) Consentidos, la recopilación de dichos datos deberá obedecer a la voluntad expresa del titular, quien podrá reservarse aquellos datos que no desee entregar; 10) identificables, los datos procesados expresarán la identidad y domicilio del responsable de su manejo; 11) seguros, los responsables de su manejo responderán por su alteración, pérdida, tratamiento o acceso no autorizado; 12) secretos, quienes tengan acceso a dichos datos, en cualquier momento, está obligado al secreto profesional respecto de los mismos. Esta obligación subsiste incluso al finalizar las relaciones con el titular del banco de datos, o con el responsable del mismo.

En el Ecuador, rige por mandato constitucional la garantía del Hábeas Data; mecanismo idóneo para precautelar la integridad interna del ciudadano, es decir, su intimidad. Esta garantía se establece en el Art. 94 de la Constitución Política, y su procedimiento, se rige por los artículos 34 a 45 de la Ley de Control Constitucional. El art. 94 de la Constitución ecuatoriana dispone que “Toda persona tiene derecho a acceder a los documentos, bancos de datos e informes sobre sí misma o sobre sus bienes que consten en entidades públicas o privadas, así como a conocer el uso que se haga de ellos y su propósito. Podrá solicitar ante el funcionario respectivo la

actualización de los datos o su rectificación, eliminación o anulación, si fueren erróneos o afectaren ilegítimamente sus derechos. Si la falta de atención causare perjuicio, el afectado podrá demandar indemnización. La ley establecerá un procedimiento especial para acceder a los datos personales que consten en los archivos relacionados con la defensa nacional."

Por su parte, el art. 9 de la ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos establece: " Para la elaboración, transferencia o utilización de bases de datos obtenidas directa o indirectamente del uso o transmisión de mensajes de datos, se requerirá el consentimiento expreso del titular de éstos, quien podrá seleccionar la información a compartirse con terceros.

La recopilación y uso de datos personales responderá a los derechos de privacidad, intimidad y confidencialidad garantizados por la Constitución Política de la República y esta Ley, los cuales podrán ser utilizados o transferidos únicamente con autorización del titular u orden de autoridad competente. No será preciso el consentimiento para recopilar datos personales de fuentes accesibles al público, cuando se recojan para el ejercicio de las funciones propias de la administración pública, en el ámbito de su competencia, y cuando se refieran a personas vinculadas por una relación de negocios, laboral, administrativa o contractual y sean necesarios para el mantenimiento de las relaciones o para el cumplimiento del contrato.

El consentimiento al que se refiere este artículo podrá ser revocado a criterio del titular de los datos; la revocatoria no tendrá en ningún caso efecto retroactivo". Para efectos de la aplicación de la ley define los téminos relevantes en el glosario de términos.

A pesar de ello, existe un vacío en el campo de prevención. No existe disposición alguna en la legislación ecuatoriana que garantice el derecho del titular a

impedir la publicación de los datos personales. La garantía del Hábeas Data opera para corregir los abusos, pero no para prevenirlos.

I.2.B.1.d Acceso a la Información

En el Ecuador existe la Ley Orgánica de Transparencia y Acceso a la Información Pública, la cual fija normas para garantizar el acceso de todos los ciudadanos al acceso oportuno y de forma fácil a cualquier dato, consignado en bancos de datos de las instituciones públicas. Impone ciertas limitaciones para datos personales y para datos relacionados con la seguridad nacional.

I.2.B.1.e El Flujo Transfronteras

Jijena Leiva explica el tema al decir que "la tecnología ha hecho caer las fronteras en muchos aspectos... uno de ellos es la pérdida de la intimidad nacional de los países mal llamados subdesarrollados o en vías de desarrollo, frente a los de mayores recursos y tecnológicamente más avanzados".[26] De esta manera surgen problemas que inciden sobre la soberanía de los Estados, por lo cual se propone por la doctrina consagrar el principio de soberanía de la información, en una ley que regule el flujo de datos transfronteras. Esta area de estudio, le interesa al Derecho Internacional Público.

Pérez Luño amplía el tema por considerar que se ha sucitado un conflicto de intereses entre los países productores y los países consumidores de datos informáticos. Los países desarrollados recogen, almacenan y distribuyen

[26] Renato Javier Jijena Leiva; *Chile,la Protección Penal de la Intimidad y el DelitoInformático*; 1992. Página 28.

información, gracias a que cuentan con un gran desarrollo de tecnología. Los países subdesarrollados, a diferencia de los anteriores, solo están en condiciones de recibir y consumir información; en muchos casos, ni siquiera pueden acceder a ella por carecer de los medios técnicos necesarios para ello. Por esta razón, los países desarrollados han mantenido una política tendiente a la libertad ilimitada de intercambio de información entre los países, mientras que los países subdesarrollados, exigen que se reconozca la facultad de ejercer un control sobre los datos que puedan recogerse en su territorio.

Así, los Convenios internacionales ratificados por países desarrollados han sido emitidos en el sentido de promover el libre flujo de datos. En este sentido se creó EURONET, el sistema de comunicación de datos entre los países miembros de la Comunidad Económica Europea, actual Unión Europea. En el mismo sentido fue suscrito el Acuerdo de Schengen, el cual se refiere a la supresión gradual de controles entre las fronteras comunes de los países signatarios. Para ello, se regula el flujo de información personal en función de la cooperación policial.

Pérez Luño aclara el tema expresando que "La propuesta de la Directiva de la Unión Europea y el Acuerdo Schengen formalmente se adhieren a los principios de protección de datos personales consagrados en el Convenio del Consejo de Europa. Ahora bien, su normativa debilita las garantías de los derechos fundamentales en función de la libre circulación de mercancías, personas, servicios y capitales que hacen necesaria la circulación de datos personales entre los Estados miembros."[27]

Electronic Data Interchange (EDI) es una modalidad de contratación por medios informáticos, que presenta las particularidades de adolecer de firma manuscrita, no registrarse en soporte de papel, y utilizar formas simplificadas y normalizadas para establecer los acuerdos contractuales. Por medio de esta vía se transfieren la mayoría de datos transfronteras.

[27] Antonio Enrique Pérez-Luño; *Manual de Informática y Derecho*; 1996. Página 108.

I.2.B.2 DERECHO PRIVADO INFORMÁTICO

I.2.B.2.a Protección Legal del Software

La OMPI (Organización Mundial de Propiedad Intelectual) define al software, como objeto de protección legal, como "el conjunto de instrucciones que, una vez transferido a un soporte legible para la máquina, permite que una máquina para procesar informaciones desarrolle su función, realice su tarea o logre un resultado específico".[28]

La doctrina, en general, considera como medios de protección los siguientes: el derecho de patentes o sistema de registro de marcas y patentes y los derechos de autor o copyright.

I.2.B.2.a.1 Derecho de Patentes

Abarca la protección del software como parte de un procedimiento para operar un determinado proceso industrial, pero no opera para proteger la expresión de las ideas, mientras no tengan este fin específico. Sin embargo, este tipo de protección intelectual no ha sido acogida por la mayoría de países.

Aclara Pérez Luño el tema, al exponer las ventajas y desventajas que presenta este tipo de protección. Considera como ventajas la protección de 20 años, lo cual le otorga un monopolio temporal, en lo referente a su explotación, garantizándole que durante este período, nadie puede producir, comercializar o utilizar el programa sin consentimiento del individuo que ha obtenido el derecho de patente sobre dicho

[28] Tomado del libro de Antonio Enrique Pérez Luño, página 120.

programa de computaciòn. Transcurrido dicho plazo, se considera que tal programa pasa a ser de dominio público y por ello es objeto de libre utilización. Por su parte, considera como dificultades los requisitos de patentabilidad, ya que necesariamente debe reunir las siguientes características para que se considere patentable: novedad, es decir, que represente, de forma objetiva una innovación; materialidad, es decir, que el objeto a patentar no se componga de meras ideas, sino de un objeto tangible, susceptible de traducirse en resultados prácticos; industrialidad, debe ser una creación que tenga aplicación práctica en la producción o transformación de productos y que represente un avance tecnológico en esa área.

La mayor parte de la doctrina considera que este medio de protección intelectual no es aplicable al software. Pérez Luño realiza una breve explicación de las razones aducidas de la siguiente manera “la innovación, porque las más de las veces un programa tiene que ser una derivación o modificación de otros anteriores; la materialidad, porque el es básicamente el producto de una actividad mental, se trata de algoritmos, de un procedimiento lógico de elaboración de informaciones que, precisamente por ello, tiene una autonomía respecto al equipo físico (salvo el caso del firmware, o software de base, o de la memoria ROM, que son programas integrados en los propios circuitos electrónicos del ordenador); y la industrialidad, ya que el software carece de los certificados de operatividad y de sistemas de mantenimiento características de los objetos industriales patentables”.[29]

Estas teorías contrarias a la patentabilidad del software han encontrado cabida en el Art. 52 del Convenio para la Patente Europea suscrito en Munich en 1973, en el cual se establece que “no son invenciones los programas de ordenadores”.

I.2.B.2.a.2 Derechos de Autor o Copyright

[29] Antonio Enrique Pérez-Luño; *Manual de Informática y Derecho;* 1996. Páginas 117 y 118.

Se considera al programa como una obra, como una creación intelectual que permite manipular los datos existentes en la memoria del computador; asimilación que no es fácil de aceptar por cuanto esta figura de protección intelectual no fue pensada para el software, por lo cual, algunos autores consideran que debería proponerse una categoría especial de protección, la de los “métodos intelectuales”, dentro de la cual se proteja el software. Sin embargo, la mayoría de países la ha adoptado como la forma de protección penal del software, entre ellos, el Ecuador.

Esta forma de protección, como figura aplicable al software, fue introducida por los Estados Unidos en la década de los sesenta. Las condiciones para su operabilidad eran dos: que se acreditara su originalidad y que se depositaran copias en un lenguaje que fuera inteligible. Esta forma de protección nace por la decisión de la empresa IBM (International Bussines Machines), al separar, por motivos de comercialización, la parte lógica (software) de la parte física (hardware). A partir de entonces, la doctrina y la jurisprudencia estadounidense tendió a extender la protección del software a la disciplina de los derechos de autor.

Luego de algunas modificaciones estatutarias, se dictó en 1980 el Computer Crime Copyright Act, que modificó las condiciones anteriores en los siguientes términos: Define al software y admite expresamente su tutela por disposiciones referidas a los derechos de autor; dicha protección se condiciona al carácter original del programa; prohibe la reproducción y la utilización de los programas protegidos; admite que los usuarios legitimados realicen copias del programa para su uso personal. Este tipo de protección abarca hasta los 50 años transcurridos desde la muerte de su autor y su carácter es universal; es decir, no está sujeto a limitaciones territoriales.

El Tratado de la OMPI sobre derecho de autor adoptado en Ginebra por la Conferencia Diplomática el 20 de Diciembre de 1996, en su artículo 4 establece que

los programas de ordenador están protegidos como obras literarias, cualquiera que sea su forma de expresión, en el marco de lo dispuesto por el artículo 2 del Convenio de Berna.

La mayoría de países han seguido estas disposiciones, entre ellos el Ecuador. La protección jurídica del software dentro de nuestra legislación se encuentra establecida en la Ley de Propiedad Intelectual, y específicamente, en los artículos 8, 28, 29 y 30. De ellos, se cita el artículo 8, que es el relevante para el caso. Los demás establecen disposiciones especiales sobre ciertas obras de los programas de ordenador.

El Art. 8 establece que: " La protección del derecho de autor recae sobre todas las obras del ingenio, en el ámbito literario o artístico, cualquiera que sea su género, forma de expresión, mérito o finalidad. Los derechos reconocidos por el presente Título son independientes de la propiedad del objeto material en el cual está incorporada la obra y su goce o ejercicio no están supeditados al requisito de registro o al cumplimiento de cualquier formalidad. Las obras protegidas comprenden, entre otras, las siguientes: b) colecciones de obras, tales como antologías o compilaciones y bases de datos de toda clase, que por la selección o disposición de las materias constituyan creaciones intelectuales, sin perjuicio de los derechos de autor que subsistan sobre los materiales o datos. K) programas de ordenador."

I.2.B.2.b La Contratación Informática y los Contratos Informáticos

Es importante distinguir la diferencia existente entre dos términos que, aparentemente tienen el mismo significado, pero que tratan dos temas completamente distintos; la contratación electrónica y el contrato informático. La contratación electrónica se enfoca en la protección jurídica necesaria para realizar

contratos por medio de medios electrónicos, especialmente Internet. Por su parte, el contrato electrónico ubica su preocupación en el objeto de negociación contractual, es decir, opera cuando existe un bien o servicio relacionado con la tecnología como objeto del contrato; el cual puede ser realizado mediante medios tradicionales o mediante medios electrónicos.

I.2.B.2.b.1. La Contratación Electrónica

Yánez Narváez expresa su preocupación por la dificultad de determinar, en este tipo de contratos, el momento de nacimiento de la obligación. Determina que el momento de perfeccionamiento del contrato celebrado por medios electrónicos cuando la aceptación llega a conocimiento de la parte que ofrece dar, hacer o no hacer una cosa o prestar un servicio. Adicionalmente, dice que se entenderá aceptado el contrato cuando la información emitida haya llegado a conocimiento de la otra parte, es decir, en el momento en que se registre dicho mail como ingresado en el sistema de la otra parte. La competencia y el Derecho aplicable, en caso de no ser determinado por las partes contratantes, será el lugar en el que se realiza la oferta electrónica.

La ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, establece normas para la contratación electrónica en los artículos 45 al 47.

I.2.B.2.b.2 Los Contratos Informáticos

Es necesario dejar en claro que los contratos informáticos, si bien se rigen por las reglas de contratación establecidas en el Derecho Civil, o en el Derecho Internacional Privado, para los casos de contratación entre Estados; tiene sus peculiaridades. Generalmente, este tipo de contratos son de adhesión.

Jijena Leiva, dentro de su explicación, considera que existen cuatro clases de contratos informáticos: de suministro o compraventa de equipos (hardware) y programas (software); de prestación de bienes y servicios, como mantenimiento y asesoría técnica; de leasing de equipos y los relacionados con el personal informático.

Pérez Luño coincide con el mencionado autor en las modalidades de contratación informática existentes. Añade que los contratos informáticos tienen la peculiaridad de ser plurilaterales, al ser contratos realizados entre una empresa y varios usuarios, es decir, son contratos de adhesión.

Yánez Narváez, con relación al Derecho Ecuatoriano, saca a relucir la desventaja existente entre el contratante y el contratista de esta clase de negocios jurídicos, por cuanto el usuario no tiene los conocimientos técnicos que tiene el proveedor de bienes o servicios informáticos. Al ser contratos de adhesión, el usuario se encuentra desprotegido frente al proveedor por su el diferente nivel de conocimiento tecnológico. Para ello, existe la intervención del Estado con el fin de proteger al usuario, y lo hace partiendo de el art. 22, numeral tres de la Constitución, el cual establece: “El derecho a disponer de bienes y servicios de óptima calidad, así como a ser informado sobre su contenido y características. La Ley establecerá los mecanismos de control de calidad de bienes y servicios, los procedimientos de defensa del consumidor y las sanciones correspondientes por la violación de éstos derechos”. Por su parte, la Ley de defensa al consumidor establece parámetros legales de protección para este tipo de riesgos.

CAPÍTULO II

EL DELITO INFORMÁTICO

Como se ha señalado en el capítulo anterior, la inclusión de la informática en la actualidad ha llegado a tener una trascendencia tal que incluso se habla del nacimiento de una nueva sociedad: la Sociedad de la Información y la Comunicación. Esta explosión tecnológica ha sobrepasado los problemas de distancia, dificultad de obtener información y por supuesto, ha generado nuevas y mejores vías de comunicación.

Lamentablemente, la explosión tecnológica que ha tenido cabida desde los años 50 aproximadamente, no ha traído consigo únicamente las ventajas, sino que ha creado nuevos vacíos jurídicos y ha dejado a algunas áreas del Derecho con deficiencia de protección frente a estos nuevos acontecimientos. Como consecuencia de esta nueva sociedad, la protección que el Derecho brindaba, de manera eficaz antes de la explosión de las nuevas tecnologías, se ha quedado corta frente a este fenómeno social. Esta situación no es extraña para el Derecho Penal, en donde se ha visto una proliferación de nuevos delitos, que no hubieran sido posibles en otra época, a la vez que, ha permitido perfeccionar los anteriores.

En el presente capítulo se tratará el problema del delito informático, el cual se compone de diversas características propias, razón por la cual, es inapropiada la protección penal tradicional, existente en nuestro Código Penal actual; al igual que se dará una visión amplia y general de la nueva perspectiva desde la cual se mira al Derecho Penal como una moderna rama del Derecho, que abarca

estas nuevas formas de criminalidad, tomando en consideración al sujeto activo de dichos delitos: el delincuente informático, quien opera con una psicología distinta a la del delincuente tradicional, y como consecuencia, proyecta reacciones distintas en la sociedad.

II.1 EL DERECHO PENAL INFORMÁTICO

El impacto de la informática en la sociedad actual nos conduce a una inevitable transformación del orden jurídico penal tradicional. Es claro que sin ella, la protección penal existente en la actualidad resulta insuficiente para cubrir el amplio espectro de delitos que se han producido y se seguirán produciendo como consecuencia de la informatización. Las sociedades se desarrollan, cada vez con mayor rapidez, y el Derecho debe, a su vez, desarrollarse con ella. Si el ciclo no funciona a este ritmo, el Derecho no alcanzará su objetivo principal que es el de ofrecer mecanismos de protección que garanticen la paz y el orden social, a través de la protección de los derechos individuales de cada ciudadano.

Ante los progresos tecnológicos, el delito no puede ser analizado bajo las perspectivas tradicionales. De esta manera, entramos en una nueva perspectiva de análisis, la perspectiva que brinda el Derecho Penal Informático. Con ello, como explica Jijena Leiva, "no se trata de configurar un nuevo Derecho Penal, sino de adaptar el vigente a las nuevas exigencias, configurando y considerando nuevos bienes jurídicos, analizando las modalidades de atentar contra los mismos y, en definitiva, tipificando las nuevas figuras criminales."[30] Dicho de otra manera, es necesario que se revalorice y se adapte el tradicional Derecho Penal para que abarque las nuevas exigencias que impone el mundo actual.

[30] Jijena Leiva, Renato Javier; CHILE. LA PROTECCION PENAL DE LA INTIMIDAD Y EL DELITO INFORMATICO:1992; página 31.

II.1.A JUSTIFICACIÓN

El Derecho Penal Informático, para algunos juristas como Jijena Leiva, comprende dos ámbitos que se relacionan entre sí. Estos son: "La problemática respecto de la privacidad (entiéndase intimidad), que requiere la estructuración de una normativa específica, fundamentalmente por la existencia de grandes bancos de datos nominativos y la posibilidad de su interconexión telemática, y 2) la problemática de los delitos informáticos, ya sea ubicando a la informática como medio utilizado para consumar el delito o como objeto de comisión del mismo, constituye un factor criminológico de creciente importancia que va requiriendo la estructuración de tipologías y regulaciones específicas".[31]

De esta manera, cuando el abuso de la informática llegue a transgredir derechos individuales, será necesario que el Derecho Penal rija para evitar dichos abusos. En estas circunstancias se requiere la intervención del *ius puniendi* del Estado. Para que esta intervención sea idónea, deberá regularse por los principios básicos del Derecho Penal, los cuales son perfectamente explicados por Jijena Leiva. A continuación se enuncian las razones fundamentales, desde el punto de vista legal y doctrinal, que justifican la existencia de una categoría penal especial.

Los delitos informáticos son "aquel conjunto de conductas criminales que se realizan a través del ordenador electrónico, o que afectan al funcionamiento de los sistemas informáticos."[32] Cabe aclarar, que a criterio de Pérez Luño, bajo esta denominación, se suelen incluir a aquellas conductas menos relevantes, que no pasan de ser meras faltas. Esto se produce por la gran trascendencia que tienen los delitos informáticos en la sociedad actual. Por ello, muchas veces se incurre en el error de denominar como delitos informáticos a las infracciones civiles y

[31] Idem.
[32] Pérez Luño, Antonio Enrique; MANUAL DE INFORMÁTICA Y DERECHO1996; página 69.

administrativas de las cuales se encarga el Derecho Informático, como ya se analizó en el capítulo anterior.

Ricardo Mata y Martín explica que el concepto de delito informático es ambiguo, que no corresponde en sentido estricto a ninguna categoría jurídico penal. El grupo de expertos convocados por la OCDE, en el año 1985, para el análisis de este tipo de delincuencia, se refiere a este tipo de delitos como "delitos relacionados con ordenadores" (computer-related crime), dentro del cual se encuentra cualquier comportamiento antijurídico, no ético o no autorizado, relacionado con el procesamiento automatizado de datos.

En las conclusiones del Congreso sobre el delito informático, realizado en Zaragoza en 1989, se define al delito informático como "toda acción dolosa que provoca un perjuicio a personas o entidades, en cuya comsión intervienen dispositivos habitualmente utilizados en las actividades informáticas."[33]

Ricardo Mata y Martín concuerda con Jijena Leiva en que cabe diferenciar, siguiendo a la doctrina alemana, los delitos en cuyos casos el ordenador es el objeto material del delito, de aquellos en los cuales el ordenador es un mero instrumento para cometer delitos tradicionales. La doctrina alemana, para evitar confusiones, define al delito informático como "el conjunto de actos (punibles o dignos de incriminación) en los cuales el ordenador (o el procesamiento automatizado de datos) es el instrumento o el objeto de la comisión."[34]

Es interesante la explicación que brinda Gabriel Cámpoli en su ponencia, en la cual explica la diferencia, dentro de la hermenéutica penal, de dos conceptos que se usan como sinónimos, pero que difieren en su aplicación penal. Se trata de las expresiones "delitos informáticos" y "delitos electrónicos". Define a los términos de la siguiente manera, y recomienda su utilización en la doctrina penal: "Delitos

[33] Mata y Martín, Ricardo; DELINCUENCIA INFORMÁTICA Y DERECHO PENAL: 2001, página 21.
[34] Ibidem, página 23.

Informáticos: Son todos aquellos en los cuales el sujeto activo lesiona un bien jurídico que puede o no estar protegido por la legislación vigente y que puede ser de diverso tipo por medio de la utilización indebida de medios informáticos"; mientras que "Delitos electrónicos o informáticos electrónicos: son una especie del género delitos informáticos en los cuales el autor produce un daño o intromisión no autorizada en equipos electrónicos ajenos y que a la fecha por regla general no se encuentran legislados, pero que poseen como bien jurídico tutelado en forma específica la integridad de los equipos electrónicos y la intimidad de sus propietarios."[35]

II.1.A.a Justificaciones Referidas a los Principios que Rigen el Derecho Penal.

II.1.A.a.1 Principio de Legalidad o Reserva

El principio de legalidad es el principio angular de todo el sistema jurídico-penal y se resume en que no hay delito, ni pena, sin ley previa que lo establezca como tal; o como lo explica el aforismo latino, *nullum crimen, nulla poena sine lege.* Este principio encierra tres conclusiones lógicas a considerar: " 1) Solo la ley puede crear delitos y establecer penas; 2) la ley penal no puede operar retroactivamente; y 3) la ley penal, al crear delitos y penas, debe referirse directamente a los hechos que constituyen aquéllos y a la naturaleza y límites de éstas, es decir, el principio de tipicidad."[36]

De esta manera, queda claramente explicado, que por el principio de legalidad penal, y principalmente por el principio de tipicidad, no se admite la aplicación de analogías, por cuanto se niega dicho principio. En consecuencia, solo cabrá

[35] Cámpoli, Gabriel; HACIA UNA CORRECTA HERMENÉUTICA PENAL- DELITOS INFORMÁTICOS VS. DELITOS ELECTRÓNICOS; ponencia presentada dentro del Congreso Mundial de Derecho Informático, realizado en la Mitad del Mundo en el año 2001.
[36] Jijena Leiva, Renato Javier; CHILE, LA PROTECCIÓN PENAL DE LA INTIMIDAD Y EL DELITO INFORMÁTICO:1992; página 72.

considerar aquellas conductas que claramente se encuentren tipificadas. Dicho en otras palabras, no se admite que una norma penal prevista para sancionar un hecho determinado, sea aplicada a otro hecho similar al determinado.

Jijena Leiva explica la tipificación de la siguiente manera: "al tipificar, el legislador escoge las conductas que atentan contra bienes jurídicos fundamentales y, por mandato constitucional, forma un catálogo de tipos. Cada una de las descripciones del legislador se llama "tipo", y en consecuencia habrá "tipicidad" cuando el acto acaecido encuadre o corresponda a la hipótesis del hecho de una ley penal incriminatoria"[37]

La Constitución Ecuatoriana establece, en su artículo 24, numerales 1 y 3 el principio de legalidad de la siguiente manera: "Art. 24. - Para asegurar el debido proceso deberán observarse las siguientes garantías básicas, sin menoscabo de otras que establezcan la Constitución, los instrumentos internacionales, las leyes o la jurisprudencia:

1. " Nadie podrá ser juzgado por un acto u omisión que al momento de cometerse no esté legalmente tipificado como infracción penal, administrativa o de otra naturaleza, ni se le aplicará una sanción no prevista en la Constitución o la ley. Tampoco se podrá juzgar a una persona sino conforme a las leyes preexistentes, con observancia del trámite propio de cada procedimiento."

3. "Las leyes establecerán la debida proporcionalidad entre infracciones y sanciones. Determinará también sanciones alternativas a las penas de privación de la libertad, de conformidad con la naturaleza de cada caso, la personalidad del infractor y la reinserción social del sentenciado."

[37]Ibidem. página 74.

II.1.A.a.2. Principio de “*Última Ratio”*

Es importante tener presente que la eficacia de la norma penal requiere la articulación previa de medidas preventivas, de un aparato administrativo que opere de acuerdo a las necesidades y de normativa civil y administrativa que cubra y proteja la problemática derivada del tratamiento automatizado de datos; la cual deberá estar coordinada con el Derecho Penal, el cual deberá estar reservado para su intervención en los casos especialmente graves, que no puedan ser cubiertos por el Derecho Civil ni Administrativo. Consecuentemente, se vuelve necesario acudir al derecho penal para tipificar a aquellas conductas dolosas, que constituyan ataques graves y lesivos de los derechos individuales; y se remitirán al campo civil a aquellas conductas derivadas de la negligencia, las cuales se sancionarán con la obligación de indemnizar daños y perjuicios.

El derecho penal solamente debe entrar a regir cuando los mecanismos de protección previstos por las distintas disciplinas del ordenamiento jurídico no resulten adecuadas para su tutela. Este principio se basa en la concepción legal de que no debe existir intervención penal, a menos que los otros mecanismos existentes en el campo jurídico sean insuficientes para sancionar una conducta, por carecer de la fuerza coercitiva necesaria. El Derecho Penal es un mecanismo que opera cuando los demás, por no ser los suficientemente rígidos, carecen de eficacia.

II.1.A.a.3. Principio de Lesividad

En principio, no todos los hechos socialmente reprochables e incluso ilícitos resultan penalmente relevantes, ya que el derecho penal solamente se legitima cuando la conducta afecte a intereses fundamentales de la persona o la sociedad. Solamente en estos casos, se justifica la intervención penal.

II.1.A.a.4. Principio de Fragmentariedad

El derecho Penal no brinda una protección absoluta a los bienes jurídicos penales. Una vez ingresado el bien al campo jurídico penal, no resulta protegido contra cualquier tipo de agresión. El tipo penal establece las modalidades de agresión que resulten abarcadas por el Derecho Penal, e implícitamente, rechaza a aquellas modalidades que no están dentro del tipo y de las cuales puede ser objeto de agresión ese bien jurídico protegido.

II.1.A.2. Justificaciones Doctrinarias

Jijena Leiva resume las opiniones más relevantes que justifican la existencia de una categoría penal especial. Se hará un resumen de las diferentes tendencias expresadas.

Riklin, citado por Jijena Leiva explica que “si una de las tareas principales del legislador consiste en definir el comportamiento punible, significa que las disposiciones penales deben ser lo suficientemente precisas (lo que no es igual que restringidas) en cuanto a la definición de los elementos constitutivos de la infracción. Una definición muy vaga abrirá la puerta a la arbitrariedad en la aplicación del Derecho”.[38]

Carlos Romeo Casabona entra a analizar si los tipos penales existentes pueden ser interpretados de manera extensiva, basándose en una visión evolutiva o progresiva de los mismos; con lo cual, los delitos informáticos podrían ser subsumidos por los tipos tradicionales. Personalmente, concuerdo con Jijena Leiva

[38] Jijena Leiva, Renato Javier; CHILE, LA PROTECCIÓN PENAL DE LA INTIMIDAD Y EL DELITO INFORMÁTICO; 1992; página 75.

en que no es posible descansar en los tipos penales tradicionales para cubrir la delincuencia informática, debido a la inmaterialidad del objeto de protección penal que es la información y que difiere, en su esencia, de los delitos tradicionales, los cuales han sido planteados con la finalidad de proteger objetos materiales.

Ulrich Sieber explica los principios que, en su opinión, deberían inspirar una regulación normativa de los atentados contra la vida privada en relación con la informática. Los principios formulados son: " 1) principio de *última ratio* en la aplicación de las medidas de carácter penal; 2) principio de precisión de las disposiciones penales, describiendo los actos constitutivos de los delitos (con lo que se descarta el recurso a la técnica de las leyes penales en blanco); 3) principio de claridad; 4) principio de diferenciación en la tipificación de las actuaciones incriminadas; 5) principio de exclusión de las conductas culposas y 6) principio de procedibilidad de instancia de parte."[39]

En general, la doctrina se inclina, mayoritariamente, por la opción de constituir nuevos tipos penales, bajo la denominación de Derecho Penal Informático. La razón fundamental radica en la consideración de que los tipos penales tradicionales no abarcan las particularidades de la delincuencia informática. Sin embargo, como ya se advirtió, se debe tener cautela al establecer tipos penales informáticos, con la finalidad de evitar que se penalicen conductas que pueden ser sancionadas por medios menor rigurosos. Como ya se dijo anteriormente, el Derecho Penal es un recurso que debe ser usado, solamente cuando no exista otra manera de sancionar dicha conducta; cuando en su esencia exista una conducta dolosa.

También es importante, al momento de tipificar los delitos informáticos, cuidarse de no regular en forma casuística, ya que puede llevar a la aparición de verdaderas lagunas de no punibilidad. Como explica Jijena Leiva, el casuismo es una técnica legislativa que "pretende cubrir todas las lagunas, y que se caracteriza por no

[39] Ibidem; 1992; página 78.

cumplir nunca su objetivo, razón por la cual también consideramos que no es la mejor técnica la descripción, en el tipo penal, de una multiplicidad de conductas".[40]

II.1.B ALCANCES

El Derecho Penal Informático, como se explicó en líneas anteriores, se compone por aquella ciencia jurídica dedicada a la formulación de criterios jurídico-penales, que promuevan la protección de los sujetos pasivos del delito, frente a las nuevas formas de criminalidad existentes y que se preveen por existir en el mundo actual; y que básicamente se ubican en dos grupos: aquellas conductas antijurídicas que se realizan por medio de computadores y aquellas que se producen en contra de los sistemas informáticos (delitos informáticos propiamente tales).

El Derecho Penal informático, dentro de su campo de acción, debe dedicarse a tres tareas fundamentales: en un principio, debe plantear una política criminal que promueva la prevención del cometimiento de estos delitos (tema que trataré en el capítulo IV); luego debe legislar sobre el tema, con el fin de tipificar aquellas conductas que sean lesivas para los bienes jurídicos protegidos que se hayan identificado como vulnerables frente a esta clase de criminalidad; y por último, preveer los mecanismos necesarios para lograr una adecuada persecución del delito, tanto en el ámbito policial, mediante la implementación de métodos de criminalística forense que permitan identificar y perseguir al sujeto activo del delito, como en una adecuada regulación procesal que permita capturar y juzgar al delincuente, una vez identificado.

II.1.C DESARROLLO

[40] Jijena Leiva, Renato Javier; CHILE, LA PROTECCIÓN PENAL DE LA INTIMIDAD Y EL DELITO INFORMÁTICO: 1992; página 80.

A continuación realizo un breve resumen del desarrollo histórico de los delitos informáticos, basado en estadísticas obtenidas de diversas fuentes, que permiten al lector, clarificar sus ideas sobre la gravedad de los daños que producen los delitos informáticos en los bienes jurídicos vulnerados por ellos y dejan en evidencia la necesidad de brindar protección penal a los ciudadanos, frente a esta nueva forma de criminalidad.

En los Estados Unidos, el Stanford Research Institute detectó la existencia de 10 delitos informáticos en el año 1969, cifra que se disparó, ya que para el año 1977, esa cifra llegaba a 85 delitos.

Pierini, Lorences y Tornabene, en su libro titulado Hábeas Data, dan a conocer las estadísticas obtenidas del Instituto de Seguridad para las Computadoras de los Estados Unidos, durante el año 1997. De este informe se conoce que en el año mencionado, los ataques a computadores se incrementaron en un 16%, siendo cada vez más sofisticados. En este año, se reconocieron en los Estados Unidos, pérdidas por el “cibercrimen”, por 130 millones de dólares, de acuerdo con informes del FBI. Estos hechos delictivos se produjeron por Internet, y entre los más comunes estaban el acceso sin autorización a computadores por parte de empleados, ataques vía proveedores de servicios; robo de información o de software, fraudes financieros, sustracción de materiales, fraudes en las telecomunicaciones; entre otros.

Pablo Palazzi comenta en su libro que “en la década de los 80 hacen aparición los delitos de hacking, los virus informáticos y otras clases de programas destructivos. Este peligro se hizo evidente en 1989, cuando una investigación criminal en Alemania detectó varios hackers que usaban redes internacionales para acceder a información americana e inglesa y la vendían a los servicios de la KGB. En el mismo año, un virus escrito por un estudiante de informática de la Universidad

de Cornell, Estados Unidos, infectó y dejó sin funcionamiento a más de 6000 ordenadores conectados a lo que en ese entonces era Internet."[41]

A fines de la década de los 80, surge la piratería informática, la cual constituye en la manipulación de cajeros informáticos y el abuso de las telecomunicaciones. Esta manipulación reveló la gran vulnerabilidad de los sistemas informáticos y la necesidad de prevenir y controlar esta nueva criminalidad; la que era propia de esta nueva sociedad de la información y la comunicación.

Palazzi comenta que la criminalidad informática ha crecido en Francia un 184% desde 1984, frente a una tasa de 46% respecto de accidentes y una disminución del 11% en pérdidas adjudicadas a errores.[42]

Es entonces, que desde los años 80, los delitos informáticos han sido una preocupación constante para la doctrina jurídica y las legislaciones de la mayoría de Estados. La mayoría de ellos han promulgado leyes especiales sobre delitos informáticos o han adaptado los tipos ya existentes a las necesidades que imponen las nuevas tecnologías.

En Alemania en 1987 se reportaron alrededor de 3000 hechos punibles relacionados con la delincuencia informática. De ellos, más del 80% eran casos de fraude informático en los cuales se usaron tarjetas de débito de cajeros automáticos obtenidas ante todo por hurto.

El Computer Emergency and Response Team de Carnegie-Mellon reportó desde 1991 a 1994, un 498% de incremento de intrusiones informáticas; un 702% de incremento en el número de sitios afectados.

---

[41] Palazzi, Pablo; DELITOS INFORMÁTICOS; 2000; página 38.
[42] Palazzi, Pablo; DELITOS INFORMÁTICOS; 2000; página 58.

La consultora Deloitte & Touche preparó un informe en el año 1997, a pedido de la Unión Europea,publicada en el Financial Times del 24 de abril de 1997, en el cual concluyó que los delitos relacionados con la informática y con la Internet producían pérdidas anuales de 77 billones de dólares.

Según la encuesta realizada en 1998 entre empresas y agencias públicas de los Estados Unidos por el Computer Security Institute y la oficina de San Francisco del International Computer Crime Squad del FBI, el 44% de los encuestados reconocen haber sufrido incidentes de acceso no autorizado por empleados, el 25% había sido víctima de ataques de "denegación de servicio", el 24% había sido objeto de entradas en sus sistemas desde el exterior, el 18% de sustracción de información reservada, el 15% había sufrido incidentes de fraude financiero y el 14% actos de sabotaje de datos o redes. El número de encuestados que reconocían que su conexión a Internet era un frecuente punto de ataque había pasado de un 37% en 1996, a un 47% en 1997 y a un 54% en 1998.

Una investigación realizada por la Oficina Criminal Australiana, denominada Office of Strategic Crime Assesments, conjuntamente con la Policía de Victoria; encontró que de 300 encuestados, el 20% había tenido, como mínimo 6 incidentes relacionados con abusos informáticos; el 77% había sufrido ataques informáticos que produjeron pérdidas aproximadas de diez mil dólares australianos o más. Las entidades financieras reportaron que los accesos ilegítimos a sus sistemas son el delito más cometido y llega a cubrir el 57% de los ataques; le siguen las empresas de tecnología que reportaron a este delito como merecedor del 55% y las comunicaciones con el 50%. Esta encuestra indica que los delitos informáticos han aumentado un 200% en los últimos dos años.[43]

Otra investigación realizada alrededor de 2200 empresas orientadas a comercializar productos a través de web sites, ha demostrado que dos tercios de

[43] www.infowar.com

ellas han tenido problemas significativos de seguridad que no han podido solucionar hasta el momento.

El Instituto de Seguridad de Computadoras (CSI), realizó un estudio en el año 2000, denominado “Estudio de Seguridad y Delitos Informáticos”, el cual se basó en 273 instituciones, entre las cuales figuran, principalmente, Corporaciones y Agencias del Gobierno. Entre lo más destacado, se puede incluir lo siguiente: “90% de los encuestados descubrió violaciones a la seguridad de las computadoras dentro de los últimos doce meses; 70% reportaron una variedad de serias violaciones de seguridad de las computadoras, y que el más común de estas violaciones son los virus de computadoras, robo de computadoras portátiles o abusos por parte de los empleados -- por ejemplo, robo de información, fraude financiero, penetración del sistema por intrusos y sabotaje de datos o redes; 74% reconocieron pérdidas financieras debido a las violaciones de las computadoras, las cuales ascendieron a $265,589,940 (el promedio total anual durante los últimos tres años era $120,240,180); 6I encuestados cuantificaron pérdidas debido al sabotaje de datos o redes para un total de $27,148,000. Las pérdidas financieras totales debido al sabotaje durante los años anteriores combinados ascendido a sólo $10,848,850. Como en años anteriores, las pérdidas financieras más serias, ocurrieron a través de robo de información (66 encuestados reportaron $66,708,000) y el fraude financiero (53 encuestados informaron $55,996,000). Adicionalmente, 71% de los encuestados descubrieron acceso desautorizado por personas dentro de la empresa. Pero por tercer año consecutivo, la mayoría de encuestados (59%) mencionó su conexión de Internet como un punto frecuente de ataque, los que citaron sus sistemas interiores como un punto frecuente de ataque fue un 38%. Basado en contestaciones de 643 practicantes de seguridad de computadoras en corporaciones americanas, agencias gubernamentales, instituciones financieras, instituciones médicas y universidades, los hallazgos del "Estudio de Seguridad y Delitos Informáticos 2000" confirman que la amenaza del crimen por computadoras y otras violaciones de seguridad de información continúan constantes y que el fraude financiero está ascendiendo;25% de encuestados descubrieron penetración al sistema del exterior; 79% descubrieron

el abuso del empleado por acceso de Internet (por ejemplo, transmitiendo pornografía o pirateo de software, o uso inapropiado de sistemas de correo electrónico); 85% descubrieron virus de computadoras."[44]

Esta misma encuesta, por segundo año, realizó una serie de preguntas acerca del comercio electrónico por Internet. Algunos de los resultados fueron: 93% de encuestados tienen sitios de www; 43% maneja el comercio electrónico en sus sitios (en 1999, sólo era un 30%); 19% experimentaron accesos no autorizados o inapropiados en los últimos doce meses; 32% dijeron que ellos no sabían si hubo o no, acceso no autorizado o inapropiado; 35% reconocieron haber tenido ataques, reportando de dos a cinco incidentes; 19% reportaron diez o más incidentes; 64% reconocieron ataques reportados por vandalismo de la Web; 8% reportaron robo de información a través de transacciones; 3% reportaron fraude financiero.

De éstos datos, el estudio concluye que "las tendencias que el estudio de CSI/FBI ha resaltado por años son alarmantes. Los "Cyber crímenes" y otros delitos de seguridad de información se han extendido y diversificado. El 90% de los encuestados reportaron ataques. Además, tales incidentes pueden producir serios daños. Las 273 organizaciones que pudieron cuantificar sus pérdidas, informaron un total de $265,589,940. Claramente, la mayoría fueron en condiciones que se apegan a prácticas legítimas, con un despliegue de tecnologías sofisticadas, y lo más importante, por personal adecuado y entrenando, practicantes de seguridad de información en el sector privado y en el gobierno."[45]

En otro orden de ideas, la "línea caliente" de la Internet Watch Foundation (IWF), abierta en diciembre de 1996, ha recibido, principalmente a través del correo electrónico, 781 informes sobre unos 4.300 materiales de Internet considerados ilegales por usuarios de la Red. La mayor parte de los informes enviados a la "línea

[44] www.monografías.com
[45] Idem

caliente" (un 85%) se refirieron a pornografía infantil. Otros aludían a fraudes financieros, racismo, mensajes maliciosos y pornografía de adultos.

Según datos recientes del Servicio Secreto de los Estados Unidos, se calcula que los consumidores pierden unos 500 millones de dólares al año debido a los piratas que les roban de las cuentas online sus números de tarjeta de crédito y de llamadas. Dichos números se pueden vender por jugosas sumas de dinero a falsificadores que utilizan programas especiales para codificarlos en bandas magnéticas de tarjetas bancarias y de crédito, señala el Manual de la ONU.

Los delincuentes cibernéticos al acecho también usan el correo electrónico para enviar mensajes amenazantes especialmente a las mujeres. De acuerdo al libro de Barbara Jenson "Acecho cibernético: delito, represión y responsabilidad personal en el mundo online", publicado en 1996, se calcula que unas 200.000 personas acechan a alguien cada año.

En Singapur El número de delitos cibernéticos detectados en el primer semestre del 2000, en el que se han recibido 127 denuncias, alcanza ya un 68 por ciento del total del año pasado, la policía de Singapur prevé un aumento este año en los delitos por Internet de un 38% con respecto a 1999. En relación con Internet y la informática, la policía de Singapur estableció en diciembre de 1999 una oficina para investigar las violaciones de los derechos de propiedad y ya ha confiscado copias piratas por valor de 9,4 millones de dólares.

Noelia García Noguera, en su artículo titulado “ESTADÍSTICAS DE ESTAFAS Y DELITOS EN ESPAÑA DURANTE 2002”, habla de las cifras de delitos informáticos cometidos en España en el año 2002. Explica que la Guardia Civil española reportó más de 9000 denuncias por delitos informáticos, de los cuales 7 820 estaban relacionados con la pornografía infantil. Por su parte, el Cuerpo Nacional de Policía abrió el año pasado 1100 investigaciones por fraudes o delitos relativos a Internet. Más de 24 000 españoles fueron víctimas de algún tipo de fraude durante el año pasado. Entre los fraudes detectados están: Casinos en Internet, donde la ruleta virtual suele estar trucada; conexiones a teléfonos 906; fraudes mediante tarjetas de

crédito; ventas fraudulentas y subastas online; timos donde se piden dinero mediante correo electrónico (para niños enfermos, negocios en Nigeria, entre otros); medicamentos milagrosos; oportunidades de negocio (compra de maquinaria y otros artículos a un menor costo); presuntos sorteos (de paquetes de vacaciones, artículos informáticos, entre otros.)[46]

Si bien es cierto que estos datos deben ser analizados con cautela, por cuanto los delitos informáticos solo se denuncian en muy raras ocasiones, las cifras que han podido ser detectadas son alarmantes. A ellas, se debe añadir la denominada cifra negra, que consta de aquellos delitos informáticos que no han podido ser detectados, o que, por miedo al descrédito público, no han sido denunciadas. En fin, los delitos informáticos se expanden exponencialmente en lo referente a su capacidad de lesionar los bienes jurídicos de terceros y son capaces de producir inpensables daños económicos. Por ello, es necesario y urgente que se encuentre una respuesta penal a este problema.

En el Ecuador, lamentablemente, no se han encontrado durante esta investigación, estadísticas que nos permitan visualizar la profundidad del problema local.

II.2 BIEN JURÍDICO PROTEGIDO

Determinar el bien jurídico a proteger es esencial para poder tipificar un delito. Es necesario que exista un bien jurídico que esté siendo vulnerado, o que se encuentre en riesgo de ser vulnerado, para que exista un motivo jurídico para tipificar la conducta que atenta contra éste, como un delito penal. Como consecuencia de ello, es necesario conocer cuáles son dichos bienes jurídicos para poder analizar,

[46] http://www.delitosinformaticos.com/estafas/estadisticas_2002.html.

posteriormente, cuán completa es la protección penal que brinda el Ecuador frente a la delincuencia informática.

II.2.A DESARROLLO HISTÓRICO

La teoría del bien jurídico es producto del temprano liberalismo del siglo XIX; antes de este momento histórico, el ilícito penal aparecía en una concepción absolutamente teológica, ya que era considerado una desobediencia a la voluntad divina.

Como explica Blossiers Hüme, "la época de la ilustración, arraigada al contrato social, si bien no tan favorable para la constitución de un concepto autónomo de bien jurídico, determinó una visión totalmente distinta de lo social, y como consecuencia, de lo penal. La laicización y la humanización del Derecho, significaron en el orden penal que los valores supremos de la legislación se encuentren en el plano sobrenatural, orientándose la tutela hacia el individuo."[47] Desde ese mismo momento del contrato social, nace un derecho a ser respetado y un deber de respetar. El delito aparece como lesión a ese derecho subjetivo que se centraba en la libertad como derecho. De ello se infiere que el objeto del delito deberían ser solo los derechos subjetivos de los demás y como consecuencia de ello, donde no existía alguna lesión de un derecho subjetivo, no existiría ningún delito.

"Es necesario que la conducta lesiva contraviniera la relación jurídica que vincula un objeto a un sujeto o el contenido propio de un derecho personal del que se derivan a favor de su titular atribuciones de carácter intersubjetivo. Por este motivo que se pudo encontrar en el concepto de derecho subjetivo el instrumento para el establecimiento del individualismo, la defensa del particular frente al Estado. Esta corriente de proteger un derecho subjetivo en Derecho Penal responde a las dos

[47] Blossiers Hüme, Juan José; CRIMINALIDAD INFORMÁTICA; 2003; página 167.

exigencias consustanciales al liberalismo clásico: igualdad y libertad, elementos que resultarían puramente ficticios, pues el sujeto es considerado en abstracto, desconociéndose las diferencias que se derivan de la situación del individuo dentro del cuerpo social."[48]

En 1834, Birnbaum expone, como novedad, la concepción material del objeto de protección penal desde una perspectiva intrasistémica. Su visión radica en la idea de que el delito debe apreciarse de acuerdo a la naturaleza de las cosas o conforme a la razón. Tiende a considerar a los bienes como poseedores de valor en sí mismos y no por su relación con un sujeto, superándose de este modo las limitaciones del derecho subjetivo; al tiempo que clarifica que la lesión del bien penalmente tutelado carece de relación directa con la concepción de la infracción de un derecho, ya sea objetivo o subjetivo.

Las teorías posteriores a Birnbaum se caracterizan por darle mayor relevancia al aspecto formal y material del bien jurídico. Entre las más relevantes están la teoría constitucionalista sobre el bien jurídico penal y la teoría sociológica sobre el bien jurídico penal, las cuales son analizadas a continuación.

II.2.A.1 Teoría Constitucionalista Sobre el Bien Jurídico Penal

Esta teoría basa sus ideas en la comparación jerárquica de normas, ya que la Constitución, como texto fundamental, tiene la capacidad de imponer los intereses que el ordenamiento penal debe acoger. Dentro de estas teorías existen dos orientaciones; una de contenido restringido y una de contenido amplio.

---

[48] Blossiers Hume, Juan José; CRIMINALIDAD INFORMÁTICA: 2003; Página 168.

Las teorías constitucionales restringidas sostienen como intereses jurídicos penalmente relevantes sólo aquellos expresamente contenidos en el texto constitucional, con lo cual el proceso de elaboración de la ley penal alcanzará sus orígenes en la decisión del constituyente.

Esta teoría plantea la dificultad de crear nuevos tipos penales, que se vuelven necesarios como consecuencia de la normal evolución social. Bajo la visión de esta teoría, cualquier tipificación de un nuevo delito constituiría una violación de la Constitución, por no estar previamente calificado como delito por el constituyente. Esta norma tipificada no estaría amparada como un interés penalmente relevante, dentro del radio de protección penal que se ha establecido constitucionalmente.

Las teorías Constitucionales amplias se bifurcan. El primer enfoque plantea que "la vinculación que debe mediar entre la norma penal y una norma constitucional se limita a la característica básica del Estado, en este caso, como hemos señalado, Social y Democrático de Derecho, por tal razón atendiendo a ello la Constitución debe servir de marco referencial obligado al legislador penal en la configuración de bienes jurídicos"[49] Esta concepción, a mi parecer es obvia, por cuanto plantea un respeto jerárquico del ordenamiento jurídico existente, lo cual es evidente para mantener un Estado de Derecho, y como consecuencia no plantea ninguna innovación a los principios generales que rigen el Estado de Derecho.

La segunda tesis sostiene que el Derecho Constitucional es el fin al que se debe llegar, y no el punto de partida. De esta manera, el Derecho Penal se rige por principios constitucionales y apunta a su cumplimiento, mediante la creación de normas que persigan el cumplimiento de los principios constitucionales.

II.2.A.2 Teorías Sociológicas Sobre el Bien Jurídico Penal

[49] Blossiers Hüme, Juan José; CRIMINALIDAD INFORMÁTICA; 2003; página 173.

Dentro de ésta teoría se destacan dos corrientes: una monista individualista y otra relacionada al perjuicio social, las cuales son explicadas de forma breve, a continuación.

II.2.A.2.a Teorías Monistas Individualistas

Bajo esta óptica, el bien jurídico es en esencia, “un interés individual indispensable”, con lo cual los bienes jurídicos individuales trascienden a primer plano, sin dejar de darle importancia a los bienes jurídicos colectivos. Estos teoría considera que los bienes jurídicos deben acomodarse a la función de protección de los individuos y deben ser delimitados con base en esa función.

Esta teoría busca evitar la desmesurada ampliación de la intervención penal, tomando como base el interés humano necesitado de protección jurídico penal, pero aceptando adicionalmente aquellos intereses colectivos que, de manera cercana, protejan valores individuales.

II.2.A.2.b Teorías Relativas al Perjuicio Social

Quienes apoyan esta teoría sostienen que los intereses que pueden ser elevados a la categoría de bienes jurídico penales son aquellos cuya lesión o riesgo produzca un daño social importante. Dentro de esta teoría se identifican claramente dos vertientes bien definidas: el funcionalismo sistémico y el interaccionismo.

II.2.A.2.b.1 Funcionalismo Sistémico

Esta teoría basa sus planteamientos en la disfuncionalidad del comportamiento con relación al sistema social. Bajo esta teoría, el bien jurídico tutelado penalmente será "la validez fáctica de las normas añadiendo como filtro del mismo el concepto de la "dañosidad social" de la conducta a fin de configurar el contenido material del concepto y evitar a la vez su estancamiento en la teoría de las normas."[50]

Sin embargo, Guillermo Portilla, citado por Blossiers Hüme explica que "el lugar de determinación de los efectos socialmente dañosos del delito no reside ya en los procesos de interacción perturbados por el hecho como suceso externo, sino sólo en la validez de la norma".[51]

II.2.A.2.b.2 Teorías Interaccionistas

Esta teoría entiende al grupo social como un variado sistema de interacciones sociales en el cual el delito, como lesión o como riesgo de daño de un bien jurídico , afecta a esta estructura social de interacción.

Es interesante la opinión de Erlinda Eva Berrier, en su trabajo " Y Dónde está el Delito?", quien sostiene que "el bien jurídico es algo estático, preexistente al Derecho, sino algo dinámico, diferente según el desarrollo de la sociedad sometido a cambio, y acorde con la Constitución."[52]

Por su parte, Diego Sánchez explica que "El bien jurídico puede presentarse como objeto de protección de la ley o como objeto de ataque contra el que se dirige el delito y no debe confundirse con el objeto de la acción que pertenece al mundo de

[50] Blossiers Hüme, Juan José; CRIMINALIDAD INFORMÁTICA; 2003; página 179-180.
[51] Ibidem; Página 180.
[52] Berrier, Erlinda Eva; "Y DÓNDE ESTÁ EL DELITO?"; www.monografías.com ; página 20.

lo sensible. Siguiendo el ejemplo más común: en el hurto el objeto de la acción es la cosa sustraída; el objeto de la protección, la propiedad."[53]

II.2.B CLASIFICACIÓN DE LOS BIENES JURÍDICOS PROTEGIDOS

El campo de acción de todo precepto penal puede estar referido al resguardo de intereses individuales o colectivos. Se denominan bienes jurídicos individuales aquellos bienes cuya lesión o riesgo de lesión vulnera de manera directa a las personas. Entre ellos se pueden destacar la vida, la libertad y el honor, entre otros. Por su parte, son bienes jurídicos colectivos aquellos en los cuales prevalecen los intereses comunitarios; son aquellos cuya lesión o peligro de lesión afecta directamente a intereses colectivos. Entre ellos se puede mencionar el medio ambiente, la administración pública, el orden socio-económico, entre otros.

II.2.C EL BIEN JURÍDICO PROTEGIDO EN LOS DELITOS INFORMÁTICOS

La determinación del bien jurídico protegido es necesario para la determinación del delito penal informático por cuanto delimita el campo dentro del cual pueden ejercitarse las conductas delictivas. De esta determinación, es posible conocer cuando una conducta puede ser considerada penalmente relevante y la motivación que lleva a tipificarla; una vez que se conoce el interés jurídico que vulnera, existe una razón para tipificar como delito dicha conducta. Si no vulnera o pone en riesgo que se vulnere dicha conducta, no es factible que se la tipifique como delito.

Una de las mayores dificultades que se presentan al momento de legislar sobre los delitos informáticos es la falta de precisión y vaguedad que existe en la doctrina

[53] Sánchez, Diego; "BIENES JURÍDICOS A SER PROTEGIDOS POR EL AVANCE DE LOS DELITOS INFORMÁTICOS" (ponencia presentada dentro del Congreso Mundial de Derecho Informático, realizado en Ecuador en el año 2001.

para determinar los intereses jurídicos que el legislador debe amparar, al tipificar las conductas que puedan vulnerarlos. Adicionalmente, los delitos informáticos se han catalogado por la doctrina como pluriofensivos, debido a su gran capacidad de afectación, que ha llegado a lesionar a varios bienes jurídicos en un mismo acto delictivo.

De esta manera, esta especialidad del Derecho Penal, debe construir un nuevo grupo de bienes jurídicos, dentro de los cuales consten todos aquellos que no alcancen a ser amparados por los tipos tradicionales.

El objeto jurídico es "el bien lesionado o puesto en peligro por la conducta del sujeto activo" y "está constituído por aquellos bienes públicos o intereses colectivos asumidos por el Estado que, por ser precisamente tales, el derecho debe proteger" [54] "Es la persona o cosa que constituye la materia sobre la cual recae la conducta del delincuente; que pertenece al mundo fáctico, que es un elemento del tipo, y que no existe en los delitos formales o de mera actividad" [55] El objeto del delito informático, como consecuencia, es un intangible, es un objeto inmaterial, es la información.

Concuerdo con Jijena Leiva en que el objeto de amparo son los contenidos informativos de un sistema; es decir, la información en sí misma, que vaya a ser objeto de tratamiento automatizado, que se encuentre almacenada en bancos de datos o que vaya a ser procesada. De ella, se debe realizar un análisis para identificar aquella información que necesita ser protegida, porque su vulneración signifique un atentado directo contra algún bien jurídico protegido. De este grupo de información, se deberá decidir la clase de protección que será necesaria, dentro de la cual, se obtendrá la información que deba ser protegida por el campo penal.

[54] Jijena Leiva, Renato Javier; CHILE, LA PROTECCIÓN PENAL DE LA INTIMIDAD Y EL DELITO INFORMÁTICO: 1992; página 91.
[55] Ibidem. Página 93.

Jijena Leiva ha encontrado tres bienes jurídicos que pueden ser afectados mediante el mal uso de la información; así, “si la información es nominativa o relacionada con las personas se atenta contra la intimidad; de ser económica o representar valores, se atenta contra el patrimonio y la propiedad, y si es estratégica o relacionada con la seguridad o la soberanía de un Estado- en cuanto esté inserto en la comunidad internacional-, contra lo que hemos denominado la intimidad nacional”.[56]

Para el Doctor Santiago Acurio del Pino, en su artículo publicado en la Revista “Ruptura por la legalidad” del año 2001, explica que la identificación de los bienes jurídicos protegidos debe realizarse desde la perspectiva tradicional, re interpretando, de forma teleológica, los delitos tradicionales, con la finalidad de subsanar las lagunas originadas por los novedosos comportamientos delictivos. Como consecuencia de ello, los bienes jurídicos protegidos serán los mismos que existen para los delitos tradicionales, con la diferencia de elementos agregados que faciliten la persecución y sanción de los delitos informáticos.

En general, los bienes jurídicos protegidos son: el patrimonio, que se ve afectado en los fraudes informáticos y en las manipulaciones de datos; la reserva, intimidad y confidencialidad, que se vulnera en caso de agresiones informáticas relacionadas con la intimidad y con los bancos de datos en particular; la seguridad o fiabilidad del tráfico jurídico y probatorio, en el caso de falsificación de datos y documentos probatorios por medios informáticos; y la propiedad cuando recae sobre la información o sobre elementos físicos y materiales de un sistema informático, que es afectado por los daños y que se denomina terrorismo informático.

Por otro lado, el peruano Blossiers Hüme ha identificado los siguientes bienes jurídicos, entre individuales y colectivos: la intimidad, el patrimonio, el honor, la libertad informática y la seguridad informática.

---

[56] Jijena Leiva, Renato Javier; CHILE, LA PROTECCIÓN PENAL DE LA INTIMIDAD Y EL DELITO INFORMÁTICO: 1992; página 91

Para Berrier, los bienes jurídicos que son suceptibles de protección penal son: la información, el derecho a la privacidad, y la seguridad.

Para fines pedagógicos, a continuación realizo una descripción de los bienes jurídicos que, la mayoría de la doctrina, ha considerado que deben ser tomados en consideración como bienes jurídicos protegidos. En esta descripción, tomo aquellos que, a mi parecer, son los más relevantes para el estudio de los delitos informáticos.

II.2.C.1 La Intimidad

Para lograr un correcto entendimiento del alcance de este bien jurídico protegido, es necesario aclarar la diferencia existente entre dos conceptos, que muchas veces se confunden: el concepto de privacidad, frente al de intimidad. La intimidad se refiere a aquellas circunstancias internas, que constituyen la esencia del ser humano y que éste mantiene como núcleo de su personalidad. El diccionario de la Real Academia de la Lengua Española define a la intimidad como "Zona espiritual íntima y reservada de una persona o de un grupo, especialmente de una familia" [57]. Por su parte, Diego Sánchez ejemplifica los datos sensibles diciendo que "datos como por ejemplo el estado de salud, constituye un dato íntimo y que la doctrina más calificada lo ubica dentro de la categoría de datos sensibles, incluyendo dentro de éstos los referidos a la salud, costumbres, hábitos sexuales y creencias religiosas o filosóficas de una persona."[58]

La privacidad se define por Dávara Rodriguez, citado por Blossiers Hüme, como "término al que podemos hacer referencia bajo la óptica de la pertenencia de los

[57] http://buscon.rae.es/diccionario/drae.htm
[58] Sánchez, Diego; "BIENES JURÍDICOS A SER PROTEGIDOS POR EL AVANCE DE LOS DELITOS INFORMÁTICOS" (ponencia presentada dentro del Congreso Mundial de Derecho Informático, realizado en Ecuador en el año 2001.

datos de una persona, su titular, y que en ellos se puedan analizar aspectos que individualmente no tienen mayor trascendencia, pero que al unirlos a otros pueden configurar un perfil determinado sobre una o varias características del individuo que éste tiene derecho a exigir que permanezcan en su esfera interna, en su ámbito de privacidad". Por su parte, el Diccionario de la Real Academia de la Lengua Española define a este concepto como "Ámbito de la vida privada que se tiene derecho a proteger de cualquier intromisión."[59]

González Guitián, citado por Jijena Leiva, explica que la jutificación para tipificar este delito reside en que la falta total de dicha protección significa el absoluto e inmediato acceso, lo cual se traduce en una constante observación de un individuo, con lo cual se lo priva de su individualidad y, en cierto modo, de su dignidad humana.

En el ámbito supranacional, este derecho ha sido recogido en el numeral 12 de la Declaración Universal de los Derechos Humanos de las Naciones Unidas de 1948, en el numeral 8.1 de la Convención Europea para la protección de los Derechos Humanos y las Libertades Fundamentales de 1950 y en el numeral 17.1 del Pacto Internacional de Derechos Civiles y Políticos de 1966.

Explica Diego Sánchez que "sobre el derecho a la intimidad, la doctrina y jurisprudencia española, han trasladado el contenido esencial del referido derecho desde la facultad de aislamiento *(ius solitundinis*) al poder de control sobre las informaciones relevantes para cada sujeto, observándose entonces, una evolución positiva de este derecho configurado originalmente en sentido negativo. Para los españoles, el derecho a la intimidad presenta hoy un doble aspecto: por un lado, un

[59] http://buscon.rae.es/diccionario/drae.htm

derecho de defensa de la persona y por el otro, el control de las informaciones que la afectan, entendido éste como un derecho de intervención."[60]

La Constitución Política de la República del Ecuador, en su Art. 23, numeral 8 establece que " Sin perjuicio de los derechos establecidos en esta Constitución y en los instrumentos internacionales vigentes, el Estado reconocerá y garantizará a las personas los siguientes: 8. El derecho a la honra, a la buena reputación y a la intimidad personal y familiar. La ley protegerá el nombre, la imagen y la voz de la persona". Igualmente, este artículo se refiere al derecho de mantener la correspondencia y las convicciones religiosas en secreto. Así, establece: "13. La inviolabilidad y el secreto de la correspondencia. Esta sólo podrá ser retenida, abierta y examinada en los casos previstos en la ley. Se guardará el secreto de los asuntos ajenos al hecho que motive su examen. El mismo principio se observará con respecto a cualquier otro tipo o forma de comunicación; y 21. El derecho a guardar reserva sobre sus convicciones políticas y religiosas. Nadie podrá ser obligado a declarar sobre ellas. En ningún caso se podrá utilizar la información personal de terceros sobre sus creencias religiosas y filiación política, ni sobre datos referentes a salud y vida sexual, salvo para satisfacer necesidades de atención médica."

Dentro de este orden de ideas, existe el concepto de intimidad nacional, el cual fue explicado en el capítulo I y que se relaciona con el flujo de datos transfronteras. En este campo, se debe tener en cuenta que todos los Estados deben poder mantener informaciones reservadas y, en consecuencia, sancionar la comisión de los delitos en los que estén envueltos sus antecedentes relevantes.

Para Blossiers Hüme, "la intimidad es un bien jurídico posible de afectación a través del ciberespacio, sin embargo, la conducta atentatoria por sí misma no

[60] Sánchez, Diego; "BIENES JURÍDICOS A SER PROTEGIDOS POR EL AVANCE DE LOS DELITOS INFORMÁTICOS" (ponencia presentada dentro del Congreso Mundial de Derecho Informático, realizado en Ecuador en el año 2001.

representaría la tipificación de un delito informático, en la medida que lo único que variaría respecto del tipo básico del delito contra la intimidad es la modalidad empleada..."[61] Luego explica que estos delitos deberían denominarse "delitos contra la intimidad de las personas mediante el uso de la informática y de las comunicaciones", por cuanto el bien jurídico protegido sigue siendo la intimidad.

II.2.C.2 El Patrimonio

El patrimonio se constituye como uno de los principales objetos de protección en ciberespacio, debido a la expansión del comercio electrónico como una nueva manera de contratación, por lo cual su protección adquiere gran importancia dentro de la criminalidad informática.

Sin embargo, es importante resaltar que si bien el patrimonio es un valor a ser preservado y salvaguardado en el ciberespacio, no constituye el bien jurídico protegido en los delitos informáticos, ya que no responde a la propia naturaleza de la red que está en función del acceso y transmisión de la información.

II.2.C.2.a Propiedad de la Información

En este punto es necesario reconocer la propiedad sobre los bienes inmateriales, lo que ya se ha logrado dentro de nuestro ordenamiento jurídico.

---

[61] Blossiers Hüme, Juan José; CRIMINALIDAD INFORMÁTICA; 2003; página 191-192.

II.2.C.3 El Honor

Durand Valladares, citado por Blossiers Hüme, define al honor como “el derecho que cada ser humano tiene al reconocimiento y respeto, ante él mismo y ante las demás personas, de su dignidad humana y de los méritos y cualidades que ha ido adquiriendo como fruto de su desarrollo personal y social”[62]

Existe una aparente proximidad entre los bienes jurídicos honor e intimidad; sin embargo, jurídicamente representan diferentes bienes jurídicos a tutelar, que pueden ser lesionados en un mismo acto por su gran proximidad conceptual. El derecho al honor es el derecho al respeto que merece toda persona en su dignidad humana.

Blossiers Hüme explica, que al igual que en el derecho a la intimidad, no es necesario ninguna modificación de este bien jurídico protegido para que sea adaptado a los delitos informáticos, por cuanto solamente varía el medio de cometimiento de los mismos.

II.2.C.4 La Libertad Informativa

Es el derecho del individuo a controlar el uso de sus datos personales, tratados o insertos en un programa informático. La doctrina española la ha denominado “un nuevo derecho fundamental”, que tiene por objeto garantizar la facultad de las personas para conocer y acceder a las informaciones que les conciernen, archivadas en bancos de datos.

---

[62] Blossiers Hüme, Juan José; CRIMINALIDAD INFORMÁTICA; 2003; página 194 y 195.

La libertad informativa se construye a partir de que es un objeto de protección dentro de la red, caracterizado por el derecho que tiene el individuo a decidir qué información personal se podrá difundir y el destino de la misma.

Blossiers Hüme aclara que "no se debe considerar a la libertad informática como un bien jurídico que requiere de protección penal en forma autónoma de la intimidad, ya que quien disponga de los datos que se encuentren almacenados en sistemas informáticos y los utilice en perjuicio del titular, estará afectando el derecho a la intimidad o al honor, según sea el caso."[63] Dichos bienes ya están siendo protegidos, sin necesidad de la introducción de figuras penales específicas, destinadas a combatir la criminalidad informática.

II.2.C.4.a Información Personal Registrada

La protección jurídica ha de brindarse a la información personal, con lo cual, la protección de datos queda encuadrada en un concepto más amplio: el de la regulación jurídica de la información.

II.2.C.5 La Seguridad Informática

No cabe duda que la seguridad en el ciberespacio es fundamental. Esta seguridad depende de que dos áreas fundamentales estén protegidas: el acceso, asegurando que no accedan quienes no han sido autorizados y el tránsito, certificando que la información viaje segura.

La seguridad informática se verá vulnerada en cuanto se atente al uso y funcionamiento de redes o sistemas informáticos. Existe una gran gama de

[63] Blossiers Hüme, Juan José; CRIMINALIDAD INFORMÁTICA; 2003; página 201.

conductas que se cometen a través del ciberespacio, en donde el inicio de estos medios de ejecución de posteriores delitos se basa específicamente en el acceso o ingreso indebidos a un determinado sistema informático.

Blossiers Hüme considera que la seguridad informática se torna en un bien jurídico que debe primar como objeto de protección en los delitos informáticos por su autonomía y por constituir una característica principal del uso de medios informáticos.

II.2.C.5.a Acceso

El acceso no está solamente en relación con la información almacenada, sino también de la información en tránsito. El acceso debe ser considerado dentro de la seguridad informática, por cuanto a partir del acceso, el agente toma contacto con la información del titular del sistema, lo cual representa la llave de otras puertas que pueden conducir a conductas típicas contra el honor, el patrimonio y la intimidad. Para evitar este tipo de intromisiones, se han planteado soluciones tecnológicas como los passwords, que permiten el acceso solamente a aquel que lo posea.

II.2.C.5.b Tránsito

Una vez que la información está en la red, los protocolos de seguridad y las aplicaciones de criptografía le proporcionan al usuario seguridad en las transacciones. Las firmas electrónicas permiten comprobar la autenticidad del mensaje de datos.

En síntesis, los delitos informáticos vulneran más de un bien jurídico protegido, por lo cual la doctrina los ha denominado como pluriofensivos. Esta denominación se

produce en razón de que no solo vulnera el sistema informático, sino también el patrimonio y el orden económico. Blossiers Hüme lo considera que debe ser tratado, en muchas ocasiones, como un delito continuado, por no existir coincidencia de intención tiempo y lugar. En el delito continuado existe una misma intención, que une a actos sucesivos producidos en distinto tiempo y lugar.

II.3 CRIMINALIDAD INFORMÁTICA

Como explica Pérez Luño, desde el punto de vista de la dogmática jurídico penal, la criminalidad informática puede agrupar a dos categorías de delitos distintos: por un lado, la aparición de una nueva versión de delitos tradicionales, o la aparición de nuevos delitos que eran impensables antes del descubrimiento de las nuevas tecnologías. Desde este punto de vista, el delito informático obliga a revisar los elementos constitutivos de gran parte de los tipos penales tradicionales.

Esta clase de delitos son efímeros y cambiantes, debido a que están sometidos a constantes fluctuaciones e innovaciones tecnológicas. Asimismo, se caracteriza por las dificultades que presentan al momento de descubrirlos, perseguirlos y probarlos. A continuación se analizan las características propias de los delitos informáticos.

II.3.A DELINCUENCIA ECONÓMICA

Con la aparición del Delito Informático, ha aparecido en el campo del Derecho Penal un fenómeno criminal sui géneris. Son delitos que se caracterizan por no depender del uso de la fuerza física, son cometidos por personas de respetabilidad y de alto estatus social en el curso de la actividad que realiza; por lo cual se los ha denominado por la generalidad de la doctrina, aunque no cumplen con todas las

características que necesarias, como “delitos de cuello blanco”, término introducido por primera vez en el año 1943 por el criminólogo norteamericano Edwin Sutherland.

Sutherland, citado por Blossiers Hüme, define al delito de cuello blanco como: “el delito cometido por una persona de responsabilidad y status social alto en el curso de su ocupación.” Por lo cual, es necesario que concurran tres aspectos: la comisión de un delito, el status social superior que ostenta el agente y el aprovechamiento de su profesión con fines delictivos.[64]

Los delitos informáticos se caracterizan por presentar ventajas en relación al tiempo y al espacio. Son delitos que se consuman en milésimas de segundo y que no necesariamente implican la presencia física de los autores.

Son delitos muy difíciles de detectar y pocas veces denunciados. La detección de estos delitos se dificulta por las especiales condiciones del delincuente, como por la apariencia de normalidad que presentan. Existe una zona oscura, debido a que el porcentaje de delitos descubiertos es muy bajo en relación con los cometidos; al igual que existe una brecha entre los que son descubiertos y los que son puestos a conociemiento de los jueces. La propia precariedad y anacronismo del sistema jurídico penal refuerza la tendencia existente de no denunciar estos delitos, con el fin de evitar el escándalo social y el consiguiente desprestigio que puede derivarse por considerar a esa empresa como carente de medidas de seguridad básicas. Adicionalmente, son delitos que presentan un alto grado de dificultad probatoria.

Pablo Palazzi comenta un informe presentado en 1980 por el Law Enforcement Assistance Administration (LEAA), en el cual se manifiesta que según expertos del FBI, solamente se detectan el 1% de los delitos informáticos; y que de ese 1%,

[64] Blossiers Hüme, Juan José; CRIMINALIDAD INFORMÁTICA; 2003; página 66.

solamente el 14% es denunciado, y de ese 14%, solo el 3% concluye con sentencias condenatorias.[65]

Otro problema es la diversidad de las conductas. Se producen no solo conductas típicas, sino otras atípicas, que son de gran poder lesivo, ya sea a bienes individuales o colectivos, y que deben ser enfrentados por el Derecho. Existe gran originalidad en la perpetración y calidad del delito, debido a la gran creatividad y sofisticación que exigen.

Son delitos que se producen en masa; es decir, mediante una sola acción, o mediante una acción que se ejecuta varias veces, individualmente en cada computador, tiene efectos que lesionan los bienes jurídicos de varias personas. Es decir, existe una nueva figura de sujeto pasivo, el cual no es determinable porque se determina como la masa de personas afectadas por dicha acción delictiva.

Las consecuencias económicas son considerables, a tal punto que, como explica la argentina Patricia Lorenzo, en una monografía, sin título, ofrecida en el Internet[66], las pérdidas económicas son inmensas.[67] Para demostrarlo basta con presentar algunas cifras. A principios de los noventa, el Instituto Suizo de Seguros ha informado que las Compañías aseguradoras sufrían pérdidas anuales equivalentes a 4 mil millones de francos por medio de actos delictivos informáticos. En Francia, en 1984, el resultado de los actos delictivos relacionados con medios informáticos ascendió a 700 millones de francos, lo que fue equivalente a un monto diez veces mayor al emergente de asaltos bancarios tradicionales perpetrados en todo el país durante el mismo período de tiempo. Existe, sin embargo, una dificultad de valoración del perjuicio, lo que constituye otro de los grandes problemas existentes en la actualidad.

---

[65] Palazzi, Pablo; DELITOS INFORMÁTICOS; 2000; página 64

[66]

ERROR: syntaxerror
OFFENDING COMMAND: --nostringval--

STACK:

86
11824
3