UNIVERSIDAD CATÓLICA DE SANTA MARIA

ESCUELA DE POSTGRADO

MAESTRÍA EN DERECHO PENAL

“LOS DELITOS INFORMÁTICOS EN EL CÓDIGO PENAL”

TESIS PRESENTADA POR EL BACHILER:
JORGE ALBERTO VEGA AGUILAR
Para optar el Grado Académico de:
Magíster en Derecho Penal

AREQUIPA – PERÚ

2010

DEDICATORIA:

A Dios Todopoderoso, por guiarme y fortalecerme en todo momento

A mi esposa Luisa, por estar en todo momento a mi lado

A mis hijos Daniella y Sebastián, por dar inspiración a mi vida

A mis padres y hermanos, por su permanente apoyo.

EPÍGRAFE

"En otros tiempos el peligro era que los hombres se conviertan en esclavos. El peligro del futuro es que los hombres lleguen a convertirse en robots."

Erick Fromm

INDICE

RESUMEN

El propósito del presente trabajo de investigación reside, en el estudio de los delitos informáticos en el Código Penal, y su implicancia en nuestra sociedad, lo cual nos permitirá tener un panorama más amplio sobre estos delitos de nueva data.

En estos tiempos a nadie escapa la enorme influencia que ha alcanzado la informática en la vida diaria de las personas y organizaciones, siendo de gran importancia para el desarrollo y progreso de un país. Por tanto, junto al avance de la tecnología informática y su influencia en casi todas las áreas de la vida social, nos hemos visto en la obligación de realizar el presente trabajo de investigación que nos va a permitir hacer frente a este fenómeno informático y así tener un material bibliográfico de consulta de suma importancia, para los estudiantes y operadores del derecho interesados conocer sobre el tema materia de investigación.

Resulta de suma importancia, el presente tema de investigación debido a que hasta la fecha los tratadistas no han definido, estos delitos de nueva data, motivo por el cual es importante precisar que en la actualidad los juristas y especialistas en el tema materia de investigación, definen a los delitos informáticos como: delitos computacionales, delitos a través de medios informáticos y finalmente criminalidad informática.

Asimismo, destaca la importancia jurídico-penal, del presente trabajo de investigación, debido a que nuestros legisladores, han incluido en forma poco acertada dentro del Código Penal a los delitos informáticos, dentro de los delitos contra el patrimonio, motivo por el cual en la actualidad los legisladores se encuentran en la disyuntiva de seguir incluyendo esta nueva forma de criminalidad dentro de los tipos penales ya existente o crear una ley especial contra los delitos informáticos, como ya lo han realizado otros países y organizaciones internacionales.

Finalmente, nos parece poco acertada la inclusión de los “Delitos Informáticos” como un Capítulo dentro del Título de los Delitos Contra el Patrimonio en nuestro Código Penal vigente, por lo que se colegiría solo la existen Delitos Informáticos Contra el Patrimonio, lo cual no se ajusta a la realidad que estamos viviendo en la actualidad, debido a que la gama de esta nueva forma de criminalidad, no solo afecta al patrimonio, sino también: el honor, la intimidad, el pudor, la libertad Informática, la vida el cuerpo y la salud entre otros bienes jurídicos protegidos.

ABSTRACT

The purpose of this research lies in the computing crimes contained in the Criminal Code, and their implications in our society. This research will allow us to have a wider view on these newly appeared crimes.

Nowadays nobody escapes from the enormous influence that computing has reached over above us and over organizations, becoming highly important in the development and progress of a country. Therefore, considering the advance of technology and computing and their influence in almost all the areas of social life, we felt forced to do the present research so that we can face this computing phenomenon and thus have library material of great importance to consult, for students and law operators interested in knowing about the subject of this research.

The subject of this research is of the highest importance because up to now the authors have not defined these newly appeared crimes. It is necessary to precise that currently jurists and specialists on this theme define these crimes as: computing crimes, computational crimes, crimes via computing means, and finally computing criminality.

The legal and criminal importance of this investigation stands out due to the fact that our legislators have included inappropriately this kind of crimes into the Criminal Code within the crimes against patrimony which that has caused that the legislators are now in the disjunctive of keep including this new form of criminality into the already existenting criminal types or creating a special law against those so called computing crimes, just like other countries and international organizations have already done.

Finally, we do not consider pertinent to include the “Computing Crimes” as a chapter within the Crimes against Patrimony Title in our current Criminal Code since this would take us to infer that only computing crimes against patrimony exist, something that does not fit our reality. This is because of the variety of forms in which this new crime affects not only patrimony but also the honor, privacy, modesty, computing freedom, life, body and health of people, amongst other protected juridical goods.

INTRODUCCIÓN

El presente trabajo es investigación analítica, descriptiva y comparativa, orientada a un estudio conociendo del problema existente y que ha sido originado en la actualidad la por el avance de la ciencia, las nuevas tecnologías y la informática las mismas que han originado una nueva disciplina dentro de las ramas del derecho, como es el Derecho Informático, y por otro lado han originado nuevas formas de criminalidad, llamadas por algunos autores como: delitos informáticos, delitos computacionales, delitos a través de medios informáticos y siendo estos delitos de nueva data, es necesario realizar un estudio riguroso del tema. Es así que dentro del cúmulo de pensamientos, desarrollamos la presente tesis intitulada **"LOS DELITOS INFORMÁTICOS EN EL DERECHO PENAL".**

El análisis de la información lograda acerca del tema de investigación, nos permite que se pueda establecer una definición más aproximada a esta nueva forma de criminalidad, así como establecer el tema de investigación es poco estudiado tanto a nivel nacional e internacional; asimismo, que nuestra legislación penal no se encuentra acorde con el avance de la ciencia, nuevas tecnologías, informática y esta nueva forma de criminalidad.

El procesamiento de las respuestas al cuestionario, referentes a los delitos informáticos en el Código Penal, determina que se puede concluir que se viene incrementando la comisión de estos delitos por medios informáticos y que no es conocida en su totalidad por los miembros de la policía nacional, jueces, fiscales y abogados. Por ello la importancia jurídico – penal que adquiere la presente investigación; asimismo, aporte doctrinario con la finalidad que nuestros legisladores tengan las herramientas necesarias para legislar con relación a la criminalidad informática.

La presente investigación esta organizada en Cinco Capítulos, desarrollándose en el **PRIMER CAPÍTULO** el Marco Histórico, donde trataremos el origen y evolución del fenómeno informático; asimismo, como ha interactuado el Derecho Penal frente al fenómeno informático.

En el **SEGUNDO CAPÍTULO** se ha realizado el Marco Conceptual, de la manera más rigurosa, donde incluiremos términos utilizados en el llamado Ciberespacio, así como términos que tienen estrecha relación con el presente trabajo de investigación.

En el **TERCER CAPÍTULO** se ha desarrollado el Marco Teórico, donde se dilucidan algunas precisiones sobre los Delitos Informáticos como una nueva forma de criminalidad; asimismo, se ha tratado respecto a la caracterización de delincuente Informático, así como los bienes jurídicos afectados por estos delitos de nueva data. Cabe resaltar que respecto al Marco Jurídico, en el presente Capítulo, se ha tratado a los Delitos informáticos en el Código Penal vigente.

En el **CUARTO CAPÍTULO** se ha realizado un estudio de la legislación comparada de los Delitos Informáticos, teniendo como referencia países tanto de Europa, América y algunas instituciones que han legislado sobre delitos informáticos.

En el **QUINTO CAPÍTULO** se ha desarrollado la Verificación de las Hipótesis, contrastándolas, se realizó también la interpretación de los resultados y estadísticas. Asimismo, lo referente a la contrastación de las hipótesis se ha incluido casos donde se han cometido delitos informáticos recientemente.

Posteriormente, se establecen las conclusiones, recomendaciones y propuesta legislativa correspondiente al estudio, en las que se busca destacar situaciones relevantes, que serán de gran importancia para todo operador del Derecho y demás personas que deseen profundizar sobre el tema de investigación.

Finalmente, se presenta la bibliografía que sirvió de soporte teórico para el desarrollo del presente trabajo de investigación y los anexos correspondientes.

Se expresa, por último el agradecimiento al señor Director de la Escuela de Post-Grado y los Docentes de la Maestría de Derecho Penal de la Universidad Católica de Santa María.

El Autor

CAPÍTULO I:

MARCO HISTÓRICO

En el presente Capítulo desarrollaremos el marco histórico del presente trabajo de investigación donde trataremos el origen y evolución del fenómeno informático y el derecho penal frente al fenómeno informático; en este orden de ideas podemos precisar que esta nueva forma de criminalidad denominada delitos informáticos, es un fenómeno informático, siendo su principal problema el buscar formulas efectivas de control, motivo por el cual los legisladores tienen una función importante con la finalidad de regulador las relaciones y mecanismos sociales para el mantenimiento de un orden social en nuestro país.

1.1 Origen y evolución del fenómeno informático

El hombre desde la antigüedad buscó simplificar sus actividades, orientando su búsqueda en dicho sentido perfeccionó progresivamente sus métodos, sus técnicas. Para efectuar estos actos eran necesario manejar abundante información y transmitirla, siendo su primera invención el Ábaco "... herramienta que sirvió para el cómputo de las actividades comerciales, habiéndose utilizado en las civilizaciones más antiguas de la historia desde hace aproximadamente cuatro mil años." [1]

En el Siglo XVII el sabio francés Pascal idea la primera calculadora, obviamente de composición mecánica, aunque por lo primitivo de sus componentes sus operaciones resultaban básicas (sumas y restas). Posteriormente, en 1694, el notable científico Leibnitz, elabora otro modelo de máquina, aunque con ella era posible realizar operaciones más complejas que con el modelo de Pascal, su celeridad seguía siendo bastante objetable. Luego, en 1835, el británico Charles Babbge con la ayuda moral y económica de Ada Byron, elabora una compleja máquina capaz de realizar operaciones de carácter analítico, constituyendo el antecedente más lejano del trabajo con computadoras en el mundo.[2]

Es importante precisar que "…recién en 1890, aparece la informática en los Estados Unidos de América, cuando ante la necesidad del manejo adecuado de la información estadística propia del censo poblacional en ese país Hans

---

1 DICCIONARIO DE LA LENGUA ESPAÑOLA: Editorial Mediterraneo S.A. Volumen I,Madrid, 1983; pág. 5.

2 REYNA ALFARO, Luis Miguel, *"Los Delitos Informáticos – Aspectos Criminológicos, Dogmáticos y de Política Criminal"*, JURISTA Editores. Lima , 2002. pág. 111.

Hollerith elabora una computadora, aunque su capacidad era en extremo limitada".[3]

Así recién en la década de los 70, surge el primer microprocesador, se busca a partir de entonces mayor velocidad en las unidades y la miniaturización de las mismas. Aparece en consecuencia un nuevo mercado a explotar; Aple, Commodore, Microsoft, entre otras empresas, inician su conquista. Asimismo, a partir de la década de los 80 la meta es el perfeccionamiento, se diseñan herramientas que hoy en día resultan indispensables para quien quiera hacer uso adecuado de la computadora, de discos flexibles, discos duros, ratones, lapiceros ópticos, módem.

La informática, es definida como la "….. ciencia del tratamiento de la información que se ocupa de los fundamentos y la utilización de las instalaciones de procesamiento de datos, asistida por computadoras u otros procesadores informáticos. La informática ha sido la tecnología que ha evolucionado más rápidamente en la historia de la humanidad. Desde la presentación pública de la primera computadora electrónica (ENIAC), a mediados del Siglo XX, los cambios que ha experimentado la informática han sido enormes. La cantidad de datos que podemos conocer, recordar y manejar gracias a la informática es infinitamente superior que la que podemos conseguir por nuestros propios medios o leyendo una biblioteca. Desde siempre la mente humana ha buscado simplificar las tareas. Así en la antigüedad los cálculos matemáticos se hacían mentalmente, lo cual representaba un grave problema cuando tenían que hacer operaciones complicadas. A medida que avanzó la historia en la humanidad, se fueron ideando aparatos para agilizar la tarea de contar, desde el ábaco hasta la computadora…"[4]

Cabe mencionar que "… el hombre en el devenir de la historia ha perfeccionado los sistemas de contratación desde el trueque, pasando por la contratación tradicional hasta llegar a la contratación electrónica, la que se viene mejorando y masificando por el uso intensivo de las redes abiertas, que al ser de acceso público son inseguras. [5]

[3] REYNA ALFARO, Luis Miguel (2002) pág. 111.

[4] CHIRINOS SOTO Francisco, Código Penal Comentado, Editorial RODHAS Segunda Edición 2005 Lima, Pág. 458

[5] BLOSSIERS HUME, Juan José, *"Criminalidad Informática"*, Editorial Librería Portocarrero. Lima, 2003. pág. 147.

El siglo XX y comienzo del presente siglo, han traído lo que se ha denominado la *revolución de la información* y *revolución digital,* caracterizada ésta última por el desarrollo de tecnología en todas sus formas y, por ello nos encontramos ante un complejo y laberíntico entramado de cables, satélites, redes, computadoras, fibra óptica, televisores e impulsos eléctricos que constituyen la infraestructura del cyberespacio. Esta revolución, que encuentra en Internet su máxima expresión, es posible gracias al fenómeno de la convergencia, es decir, en el uso combinado de las computadoras y las redes de comunicación.

Los efectos de la *revolución digital* se hacen sentir en los distintos sectores de la sociedad como lo es en la economía, la política, la educación, el entretenimiento entre otras. Así pues, la sociedad encontró nuevas formas de interrelacionarse (compras on-line, chats, e-mail, educación a distancia, foros de discusión, etc.), y este fenómeno ha traído y traerá cambios profundos, por lo que es imprescindible estar preparados para enfrentar una evolución tecnológica acelerada, para que no se produzcan los efectos negativos.

Es indudable que así como la computadora se presenta como una herramienta muy favorable para la sociedad, también se puede constituir en un instrumento u objeto en la comisión de verdaderos actos ilícitos. Este tipo de actitudes concebidas por el hombre (y no la máquina, como algunos pudieran supones) encuentra sus orígenes desde el mismo surgimiento de la tecnología informática, ya que es lógico pensar que de al no existir las computadoras, estas acciones no existirían; por otra parte, la misma facilitación de labores que traen consigo dichos aparatos proporcionan que, en un momento, dado, el usuario se encuentre ante una situación de ocio, la cual canaliza a través de las computadoras, cometiendo, sin darse cuenta, una serie de ilícitos.

Por el mismo egoísmo humano se establece una especie de “duelo” entre el hombre y la máquina, lo cual, en última instancia, provoca el surgimiento de ilícitos, en su mayoría no intencionados, por ese “deseo” del hombre de demostrar su prioridad frente a las máquinas, y en este caso específico, las computadoras. De esta forma, podemos decir que estas acciones, más que resultado de una situación socioeconómica, se derivan de una actitud

antropopsíquica, aunque en el terreno de los hechos son una realidad sociológica bien determinada y que requiere, por ende, de un tratamiento jurídico específico.[6]

En la actualidad los denominados delitos informáticos, vienen afectando bienes jurídicos materia de protección por el Código Penal, el patrimonio, la intimidad, el honor, propiedad intelectual y derechos de autor, etc.

Luego del inicio de la comisión de los delitos informáticos, denominados de nueva data, en sus inicios eran investigados por la División de Estafas de la Dirección de Investigación Criminal de la Policía Nacional – DIRINCRI-PNP, hasta que se creó en agosto del año 2005 la División de Investigación de Delitos de Alta Tecnología – DIVINTAD, esta División es adscrita a la Dirección de Investigación Criminal de la Policía Nacional – DIRINCRI-PNP, siendo Jefe de dicha División el General PNP Eduardo Montero Romero; asimismo, durante el 2005 se registraron 456 denuncias, de ellas 243 casos se resolvieron, quedando pendientes de resolver 213 casos[7].

La División de Investigación de Delitos de Alta Tecnología, al igual que en muchos otros países se creó con la finalidad que un grupo de especialistas se dediquen exclusivamente a la investigación de los denominados delitos informáticos; asimismo, a esta División se debe de brindar mayor apoyo en lo que respecta a la logística, económico, tecnológico y efectuar capacitaciones al personal policial, con la finalidad de que se especialicen, para así poder hacer frente a esta nueva forma de criminalidad.

En la actualidad se viene incrementando las víctimas mortales, debido a lo vulnerable que son los menores de edad frente a los peligros del Internet, el uso de la red sirve en muchos casos para difundir pornografía, asesinatos, violencia, agresión y suicidio, exponen a nuestra población de niños, que están en la etapa más vulnerable de su vida, a una serie de estímulos que aún son incapaces de manejar y discriminar como nocivos para su salud mental; en el mes de setiembre 2007, han fallecido dos menores de 10 años a causa del juego denominado **"shocking game",** que circula por las diferentes páginas de Internet; asimismo, un reporte del Hospital Delgado Noguchi, en lo

6 TELLEZ VALDEZ, Julio, *"Derecho Informático"*, Universidad Nacional Autónoma de México, 1991.pág. 81.

7 Estadística Publicada el la Página Web de la División de Investigación Delitos de Alta Tecnología – DIVINTAD http:/www.policiainformatica.gob.pe de fecha 07 de marzo 2006.

que va del año 32 niños se han suicidado, 5 de ellos han sido inducidos directamente por Internet.[8] Según los últimos estudios del Instituto Guestalt de Lima, el 76% de los menores de 11 a 17 años que navegan por Internet, lo hacen sin supervisión de un adulto. Esta libertad sería la causa de los últimos suicidios con el "juego del ahorcamiento". Para el Director de ésta Institución, Manuel Saravia Oliver, esto resulta preocupante, pues los chicos se exponen a toda clase de contenidos no apto para los adolescentes y niños.[9]

Si bien es cierto, que el Estado viene realizando denodados esfuerzos para hacer frente a estos delitos de nueva data, incluyendo en el Código Penal vigente a los Delitos Informáticos y la creación de la División de Investigación de Delitos de Alta Tecnología - DIVINTAD, no es suficiente para hacer frente a esta nueva forma de criminalidad, con la finalidad de hacer frente de una forma más eficiente, es recomendable la creación de una ley especial contra los delitos informáticos, donde se encuentre tipificado las diferentes formas de criminalidad, así como las sanciones correspondientes y atribuciones de la Policía Nacional al momento de realizar las investigaciones en una forma más rápida y eficiente.

1.2 El Derecho Penal frente al fenómeno informático

La eclosión de la red constituye uno de los problemas jurídicos más candentes en el panorama jurídico actual. El fenómeno de las nuevas autopistas de la información suscita un enjambre de cuestiones de fondo, cuya elucidación requiere que se opere en varias direcciones. Se trata, pues, de abordar el significado multidireccional de la red en el ámbito jurídico como cuestión previa e ineludible al análisis jurídico-penal de las conductas ilícitas en Internet y a la formulación de propuestas de política-criminal. Esto explica el carácter multidisciplinario del problema, en el que están implicados cuestiones técnicas de seguridad en Internet, las relaciones y fronteras entre responsabilidad civil y penal, la problemática jurídica general de la tutela de datos personales y cuestiones relativas a la tutela de la propiedad intelectual e industrial en las redes telemáticas o, por último, cuestiones que afectan a la reglas del tráfico jurídico en el mercado virtual; como es fácil de comprobar se trata de un elenco de problemas que trascienden, con mucho, a la estricta disciplina del Derecho Penal.[10]

---

8 Diario Expreso de fecha 07 de setiembre 2007, Lima, pág. 15

9 Diario Trome de fecha 03 de setiembre 2007, Lima, pág. 05

10 ZUÑIGA Rodríguez Laura: "Derecho Penal, Sociedad y Nuevas Tecnologías", editorial Colex, 2001, pág. 115

En el Perú la toma de conciencia sobre el desarrollo de la nueva rama del derecho, denominada Derecho Informático, nace como consecuencia de la aparición de la computadora, la misma que hace posible el acopio, uso, manipulación y transmisión de información por medio de soportes electrónicos y redes que cada día son más y de uso masivo de la población. De allí que existen conductas novedosas que implican una nueva criminalidad o comportamiento delictivo. Con la expresión *"criminalidad mediante computadoras"* se alude a todos los actos antijurídicos según la ley penal vigente (o socialmente perjudiciales y por eso penalizables en el futuro), realizados por el empleo de un equipo automático de procesamiento de datos".[11]

Lo anteriormente expuesto hace posible afirmar que "…*el fenómeno informático,* es una realidad incuestionable y parece que también irreversible, la informática se ha instalado entre nosotros. El principal problema se traduce en buscar fórmulas efectivas de control, respecto a las cuales el Derecho ha de tener un marcado protagonismo, en su papel de regulador de las relaciones y mecanismo sociales para el mantenimiento de un orden social. Nadie duda que el fenómeno informático produce en distintas ramas del ordenamiento jurídico (Derecho Civil, Derecho Procesal, Derecho Mercantil, etc.) un cierto trastorno a la hora de enfrentar tales hechos".[12]

El uso de las computadoras, y su interconexión, ha dado lugar a un fenómeno de nuevas dimensiones: el delito de instrumentado mediante el uso del computador. Si bien no existe aún una medida exacta de estas transgresiones, es probable que su incidencia se acentúe con la exacción del uso de computadoras y redes telemáticas. Los tipos penales tradicionales resultan en muchos países inadecuados para encuadrar las nuevas formas delictivas tal como la interferencia a una red bancaria para obtener, mediante una orden electrónica el libramiento ilegal de fondos o la destrucción de datos. El tema plantea, además, complejos perfiles para el derecho internacional cuando el delito afecta a más de una jurisdicción nacional.[13]

---

11 DAVARA, Miguel Angel: *"Derecho Informático"* Editorial Aranzandi. Madrid 1993; págs. 318-319.

12 BRAMONT-TORRES, Luis Alberto: *"Delitos Informáticos en el Código Penal Peruano"*, Fondo Editorial de la Pontificia Universidad Católica. Lima, 1997. pág. 17.

13 CORREA, Carlos y otros: *"Derecho Informático",* Ediciones de Depalma, Buenos Aires, 1987. pág. 295

Así "…es innegable, el uso las nuevas tecnologías conduce a la ampliación y creación de nuevos delitos en todas partes del mundo. Dichas conductas delictivas son producto del adelanto tecnológico del que somos usuarios y como señalan los tratadistas, que el moderno Derecho Penal necesita asumir y afrontar los conceptos y estrategias de la criminalidad sobre todo en conexión con nuevos fenómenos delictivos…"[14], por lo que el estudio de la criminología de estos nuevos ilícitos resulta muy importante. Así en la actualidad los problemas de carácter metodológico y operativos que la informática plantea al jurista contemporáneo puede definirse como "… los problemas de una frontera nueva del derecho, que aún ha de trazarse, ya que el nuevo territorio se extiende al futuro, … la sociedad tecnológica, cuya protagonista es la computadora, esta se caracteriza por la rapidez de su desarrollo y de sus innovaciones que obligan al observador a proceder en el sentido mismo de una experiencia en formación".[15]

Es tan importante y trascendente este *fenómeno informático* que innovar el Derecho Penal frente a los llamados Delitos Informáticos, Delitos Computacionales, o Delitos cometidos a través de medios informáticos de "… tal es la problemática generada por este fenómeno que ha motivado, en la actualidad, la necesidad de recurrir al Derecho Penal a fin de disuadir del abusivo al que lleva el empleo de computadoras, lo cual se ha plasmado ya en varias legislaciones extranjeras. No obstante, ante estas situaciones no puede olvidarse el principio del Derecho Penal como *ultima ratio*, lo cual significa que la intervención penal solo está justificada cuando otras ramas del ordenamiento jurídico ya no puedan resolver los problemas que genera el fenómeno informático en la sociedad, de ahí que el Derecho Penal actúe como última instancia de control social".[16]

Por consiguiente, "… este nuevo reto para los juristas, como es obvio, debe, a su vez, analizado desde una perspectiva de solución internacional, pues las soluciones estrictamente estatales está abocadas al fracaso por acrónicas"; asimismo, "…. se detecta la necesidad, pero también la complejidad, de elaboración y desarrollo de un estatuto jurídico para las nuevas autopistas de la información. Las líneas de política jurídica adecuadas en ningún caso deberán desconocer los principios de proporcionalidad y racionalidad de las

14 BLOSSIERS HUME, Juan José. (2003) págs. 139 –140.

15 FROSSINI, Vittorio: *"Informática y Derecho"*, Editorial Temis S.A. Bogota 1988. pág. 49.

16 BRAMONT-TORRES, Luis Alberto (1997) pág. 17 y 18.

respuestas normativas, por cuanto el enjambre de intereses contradictorios que subyacen en la red, puede convertir en infructuosas e inadecuadas soluciones jurídicas por unidireccionales.[17]

Motivo por el cual "…en suma, se le plantean al Derecho peruano grandes desafíos, frente a los que sólo resta una radical, urgente y tenaz decisión: Innovar. Innovar con un nuevo Derecho, un Derecho que aprenda de los errores del pasado y mire hacia delante; un Derecho que vea fortificados sus máximos valores: la justicia y la seguridad. Asimismo, se hace imprescindible un Derecho que responda satisfactoriamente a las demandas de la nueva Sociedad de la Información, es decir, un Derecho que se adapte a la realidad, un Derecho actual, para de este modo cumplir a cabalidad con su rol regulador." [18]

La importancia en nuestros días de la informática y de Internet, con su constante desarrollo, con su utilidad e incluso la imposibilidad de prescindir de ellos en múltiples aspectos de la vida diaria, y asimismo la vulnerabilidad que padecen, han dado lugar a una profusión de normas, informes y declaraciones de principios que pretenden conjurar los ataques y peligros que pueden afectar a estas nuevas tecnologías. Además, la procedencias de tales textos es frecuentemente de carácter supranacional, circunstancia totalmente lógica si tenemos en cuenta que el radio de expansión de los sistemas informáticos y de Internet supera las fronteras nacionales, y consecuentemente los ataques a ellos puede provenir de cualquier parte del planeta.[19]

Por tanto es importante precisar que hoy en día el fenómeno de la informática ha ingresado a todas las actividades humanas, como una realidad latente, el Derecho y la actividad jurídica en general no son una excepción. El uso de las computadoras se difunde cada vez más en toda la actividad del abogado, el jurista, el juez, el fiscal y el notario.

---

17 ZUÑIGA Rodríguez Laura (2001) pág. 116

18 Revista Electrónica de Derecho Informático: *"El Derecho Peruano Frente a los Desafíos del Nuevo Milenio: Conciliación, Tecnología e Innovación"*, César Antonio MAITA AZPIRI, Abril 2001.

19 FAJARDO CABANA Patricia: "*Nuevos retos del Derecho Penal en la era de la Globalización"*, Editorial Tirant lo Blanch, Valencia, 2004. pág. 381.

De igual forma han ingresado en los estudios jurídicos, en el Poder Judicial, en las Fiscalías, en las Notarías, en la Administración Pública, en los Registros Públicos y en general en todas las instituciones públicas y privadas se vienen utilizando sistemas informáticos. En suma se le plantea al Derecho Penal Peruano grandes desafíos, frente a los que resta una radical, urgente y tenaz decisión, la cual debe de innovarse, aprendiendo de sus errores del pasado, la doctrina y la jurisprudencia tanto nacional como extranjera, y mirar hacia delante; un Derecho Penal que se adapte a la realidad actual para de este modo cumpla su rol regulador.

Por lo antes expuesto, podemos afirmar que estamos ante un derecho penal de la globalización, por lo que nos aunamos al indicar que "la globalización requiere de unos determinados estándares de certeza y seguridad jurídica en la protección de los intereses que se pretende lograr a través de un marco regulatorio. De esta forma, es posible concebir que se recurra a todos los órdenes de regulación y protección jurídica, tanto civiles, administrativas, fiscales y, desde luego penales. Si esto último ocurre, es decir, que la globalización logre la protección de sus intereses a través del derecho penal de la globalización"[20]. Asimismo, podemos indicar que en la actualidad, "un intento por relacionar el derecho penal con el fenómeno de la globalización debe incluir el análisis, en primer lugar, de los aspectos constitutivos a nivel de principios por los que se construye el modelo normativo y, posteriormente, el descenso a la concreta regulación de las partes general y especial del derecho penal[21].

[20] FAJARDO CABANA Patricia (2004). pág. 159

[21] FAJARDO CABANA Patricia (2004). pág. 160

CAPÍTULO II:

MARCO CONCEPTUAL

En el presente Capítulo desarrollaremos el marco conceptual, donde desarrollaremos diversos términos técnicos y jurídicos con la finalidad de comprender y estar acorde con el avance de la ciencia y tecnología, y así poder hacer frente a esta nueva forma de criminalidad; asimismo podemos apreciar que en la vida de todas las personas, en todo momento deben de enfrentar diariamente el uso de términos especializados propios del conocimiento jurídico los mismos que se vienen perfeccionando en su contenido, o cayendo en desuso, a medida que la realidad social los ha ido superando o complementando, debido al avance de la ciencia y la tecnología.

En este orden de ideas, a continuación en el presente Capítulo vamos a definir las palabras utilizadas en el presente trabajo de investigación con la finalidad de tener conocimiento y un panorama más amplío con relación a esta nueva forma de criminalidad como son los delitos informáticos.

2.1 ATAQUES: Un ataque no es más que la realización de una amenaza, entendiéndose por amenaza, como una "… una condición del entorno del sistema de la información (persona, máquina, suceso o idea), que dada una oportunidad, podría dar lugar a que se produjese una violación de la seguridad confidencialidad, integridad, disponibilidad o uso legítimo)".

La política de seguridad y el análisis de riesgos identifican las amenazas que han de ser contrarrestadas, dependiendo del diseñador del sistema de seguridad especificar los servicios y mecanismos de seguridad necesarios. Las amenazas a la seguridad de una red pueden caracterizarse modelando el sistema como un flujo de información desde una fuente, como por ejemplo un archivo o una región de la memoria principal, a un destino como por ejemplo otro archivo o un usuario.[1]

2.2 ATAQUES ACTIVOS: Estos ataques incluyen alguna modificación del mensaje o la creación de mensajes falsos. Existen varias formas de ataques como:

Cambiar la identidad del emisor o receptor, ocurre cuando una entidad pretende hacerse pasar por otra persona.

Manipulación de datos, consiste en la alteración o eliminación de datos.

Repetición, consiste en capturar una información, guardarla un tiempo y volverla a enviar, produciendo un efecto de no autorización.

[1] INSTITUTO NACIONAL DE ESTADISTICA E INFORMATICA (INEI), Colección de Seguridad de la Información: *"Delitos Informáticos"*. Lima, 2001.pág. 38

Denegación de servicios, consiste en impedir una comunicación, una respuesta, causar un repudio de usuarios.

Encaminamiento incorrecto, ocurre cuando atacan a los nodos dentro de la red, pues no están tan protegidos como los terminales[2].

2.3 ATAQUES PASIVOS: Son simplemente observaciones de datos reservados durante una transmisión. La finalidad del intruso es la obtención de la información transmitida. Dentro de ellos encontramos dos tipos de ataque: *la observación del contenido del mensaje*, el mismo que sería el entendimiento por parte de un intruso del contenido de una transmisión que contiene información confidencial, como una conversación telefónica, o correo electrónico y *el análisis del trafico,* sería la observación por parte del intruso sobre la longitud del mensaje, la identificación de sus usuarios y la frecuencia de transmisión, pero en ningún caso puede entender la información, pues va encriptada. Estos ataques, son difícilmente detectables porque no producen una alteración de la información, no obstante son factibles de prevenir.[3]

2.4 BIEN JURÍDICO: En su acepción general, todo aquel que se encuentra protegido o amparado dentro de los diversos aspectos del derecho. En Derecho penal, se emplea este concepto para referirse al interés tutelado frente a la comisión de los delitos, llamándosele "bien jurídico protegido" o "bien jurídico tutelado"[4]

De igual forma, se entiende que "... el *bien jurídico* es una viga de maestra del nuevo sistema punitivo. El bien jurídico, como los hemos señalado, constituye un principio garantizador de carácter informativo. La sociedad en general, y cada miembro de ella en particular, debe saber lo que realmente se está amparando, y, sobre todo, tener la posibilidad democrática de revisar y discutir las bases sobre las cuales se asienta dicha protección o amparo. En consecuencia, el injusto y todo el delito en si, giran en torno del bien jurídico. El *"corpus"* legal tiene la virtud de haber construido bines jurídicos que constituyen los intereses y aspiraciones de las grandes mayorías nacionales que siempre han sido marginadas del amparo del Estado...."[5]

---

2 INSTITUTO NACIONAL DE ESTADISTICA E INFORMATICA (2001) Ob cit. págs. 40 - 41

3 INSTITUTO NACIONAL DE ESTADISTICA E INFORMATICA (2001) Ob cit. págs. 39 – 40

4 FLORES POLO Pedro, Diccionario de Términos Jurídicos, Editores Importadores, Lima. Tomo I, pág. 202

5 PEÑA CABRERA, Raúl: *"Tratado de Derecho Penal – Estudio Programático de la Parte Especial"*, Editora Jurídica Grijley. 3ra. Edición. Lima, 1999. pág. 63.

2.5 CATEGORÍA DE ATAQUES: Las cuatro categorías de ataques o amenazas son: la interrupción, intercepción, modificación y fabricación.[6]

Interrupción, la información de sistema destruido o llega a ser inutilizable. Este es un ataque sobre la disponibilidad. En este ataque se pueden incluir ejemplos de destrucción de una pieza de hardware, como un disco duro o el corte de una línea de comunicación.

Modificación, es una sin autorización, pero que no sólo accediendo a la información sino que también alterándola. Este es un ataque sobre la integridad. Los ejemplos incluidos podrían ser los cambios de valores en archivos y programas o la modificación de mensajes transmitidos en una red.

Intercepción, es una sin autorización por parte de una persona, computadora o programa en una comunicación. Este es un ataque sobre la confidencialidad. Un ejemplo incluido podría ser la copia ilegal de programas o archivos.

Fabricación, es la introducción de objetos falsificados en un sistema sin autorización. Este es un ataque sobre la autenticidad. Un ejemplo sería la introducción de mensajes falsos en la red.

2.6 CRACKER: es denominado al pirata, delincuente que tiene como objetivo introducirse en ordenadores ajenos para destruir programas. Se ha de pronunciar cracker. Se encuentra adaptado como salteador[7].

Según lo indicado en la definición anterior podríamos afirmar que el cracker es aquel hacker fascinado por su capacidad de romper sistemas y software y que se dedica única y exclusivamente a Crackear sistemas. Para los grandes fabricantes de sistemas y la prensa este grupo es el más rebelde de todos, ya que siempre encuentran el modo de romper una protección. Pero el problema no radica ahí, si no en que esta rotura es difundida normalmente a través de la Red para conocimientos de otros, en esto comparten la idea y la filosofía de los Hackers. En la actualidad es habitual ver como se muestran los Cracks de la mayoría de Software de forma gratuita a través de Internet.

2.7 CRACKING: Es el ingreso sin autorización a un sistema con el objetivo de destruir la información; La persona que realiza estas conductas es denominada craker, el término viene de la palabra Crack, que significa romper algo o

---

6 INSTITUTO NACIONAL DE ESTADISTICA E INFORMATICA (2001) págs. 38 – 39.

7 Enciclopedia Universal Salvat, Editorial Salvat, Madrid 2009. Volumen 9, pág. 4314

descifrar un código, es alguien que entra subrepticiamente en el sistema informático de otra persona con frecuencia en una red, lo que puede realizar por ganancias materiales, malintencionadamente, por algún propósito o causa altruista o por placer del desafío[8].

Para las acciones nocivas existe la más contundente expresión, "Cracker" o "rompedor", sus acciones pueden ir desde simple destrucciones, como el borrado de información, hasta el robo de información sensible que se puede vender, es decir, presenta dos vertientes, el que se cuela en un sistema informático y roba información o produce destrozos en el mismo, y el que se dedica a desproteger todo tipo de programas, tanto de versiones shareware para hacerlas plenamente operativas como de programas completos comerciales que presentan protecciones anticopia[9].

2.8 CRIMINALIDAD INFORMÁTICA: se entiende como criminalidad a la calidad que tipifica una acción u omisión como criminal. También tiene sentido de "índice o estadística sobre delincuencia" y como tal se emplea en la criminología para precisar con datos estadísticos la frecuencia de crímenes en un país, en forma global o clasificada por delitos, y atendiendo a diversos factores que concurren en su comisión[10].

Así, se entiende a "... la *Criminología* como la disciplina que ocupa del estudio del delito como fenómeno social, psíquico y biológico, en cuanto trata de averiguar la etiología del delito. Esta disciplina, a través de un método empírico (causal - explicativo), investiga las causas del delito, que a su vez se sirve de diversas fuentes, constituyendo por ello un saber interdisciplinario. Así, se nutre de la psicología, la antropología criminal, la biología, la sociología, la economía, etc. Contemporáneamente, se ha planteado un cambio al paradigma etiológico, y en ello ha contribuido indudablemente los aportes de la de la Criminología Crítica, que ha rechazado la criminalidad tradicional. La Criminología Crítica y las demás vertientes actuales de la criminología moderna, ha criticado el proceso de criminalización al mismo tiempo que han ampliado su objeto de estudio, lejos del Derecho positivizado y más cerca del contexto social[11].

---

8 BLOSSIERS HUME, Juan José, *"Criminalidad Informática"*. Editorial Librería Portocarrero. Lima, 2003.

9 INSTITUTO NACIONAL DE ESTADISTICA E INFORMATICA (2001). Ob cit. pág. 30

10 FLORES POLO Pedro (1984) Tomo I, pág. 377

11 PEÑA CABRERA, Raúl (1999) pág. 184

La expresión criminalidad informática comprende aspectos patrimoniales en el orden económico y del propio sistema informático y por lo tanto difiere de otras formas de criminalidad común, y así tanto en lo social como en lo económico llega a tener una singular connotación[12].

Finalmente Klaus Tiedeman cita a Gunter KAISER quien "... describe la criminalidad informática como "un fenómeno sometido constantemente a cambios a través del desarrollo técnico y social", en cuyo ámbito nuclear se encuentran "manipulaciones a las computadoras" con el objeto de conseguir una ventaja patrimonial a favor del autor o un tercero. Pese a las considerables dudas en la comprensión estadística de la criminalidad informática y de una elevada cifra oscura, imposible de estimar en particular[13]..."

2.9 DELITO: Etimológicamente la palabra delito proviene, de la similar latina "dellictum". En general, *delito* es culpa, crimen, quebrantamiento de una ley imperativa. Proceder o abstención que lleva anejo una pena. Mas técnicamente, cumplimiento del presupuesto contenido en la ley penal, que el delincuente, autor del delito o participe de él no viola, sino que observa.

El delito es un concepto que varía a través del tiempo, según los países y las costumbres y en relación con las diversas legislaciones vigentes. La acción delictuosa se considera voluntaria, a no ser que conste expresamente lo contrario. Características esenciales: el delito es un acto humano, antijurídico, por la oposición de la conducta al derecho vigente; tipificado ya que el hecho delictuoso encaja con un tipo subsumido en un artículo del código penal; culpable, porque puede imputarse a un autor, intencionado o negligente, del delito cometido, dada la relación de causalidad existente entre el agente y su acción; punible, es decir, sancionable con una pena expresamente señalada en el código penal[14].

Según indica Raúl Peña Cabrera, "... la teoría del delito ha elaborado un sistema de conceptos para conceptuar al delito en atención a la variedad de la acción humana y en la necesidad de diferenciar estas acciones para poder ser tratadas bajo una pena o medida de seguridad. Para cumplir con los objetivos fijados el

---

12 BLOSSIERS HUME, Juan José. Ob cit. págs. 137-138.

13 TIEDEMAN, Klaus: "Derecho Penal y Nuevas Formas de Criminalidad", Editorial IDEMSA, Lima, 2000.

14 Enciclopedia Universal Salvat, Editorial Salvat, Madrid 2009. Volumen 9, pág. 4314

estudio debe ser ordenado, pues su seriedad va a permitir que se compruebe las exigencias de la ley penal; en otras palabras, verificar la asistencia de la tipicidad, antijuricidad y culpabilidad. Por otro lado, "... el concepto jurídico - penal del delito realiza su misión de ordenar la aplicación de la ley penal a un nivel Intermedio, entre la ley penal y el supuesto de hecho, para hacerla más transparente y posibilitar mejor su control. Esta ordenación transparente de la aplicación eleva, al mismo tiempo, la capacidad de praxis del Derecho penal para recoger, aplicar y elaborar complejas reglas de decisiones configurando así un rico derecho judicial."[15]

2.10 DELITO INFORMÁTICO: Julio Téllez Valdés, define a *Los Delitos Informáticos* como "…actitudes ilícitas en que se tienen a las computadoras como instrumento o fin" (concepto atípico) o las "conductas típicas, antijurídicas y culpables en que se tienen a las computadoras como instrumento *o* fin…'' (concepto típico); asimismo, el citado tratadista, indica que "…entre los contados tratadistas penales que han incursionado en el tema, tenemos al italiano Carlo Sarzana, que menciona que los delitos informáticos son *"cualquier comportamiento criminógeno en que la computadora está involucrada como material, objeto o mero símbolo".*[16]

2.11 DELITO COMPUTACIONAL: Luis Miguel Reyna Alfaro indica "… que si bien existen diferencias claras entre ambos conceptos -delitos computacionales y delitos informáticos- ambos forman parte de un mismo fenómeno criminal cuya denominación correcta sería la de "criminalidad mediante computadoras" y por la cual debe de entenderse a todas las conductas criminales para cuya comisión se emplee los ordenadores o en las cuales resulte afectada la información contenida en los sistemas informáticos."[17]

2.12 DELITO CIBERNÉTICO: Los delitos cibernéticos, son aquellos delitos cometidos en el ciberespacio, como "…un mundo virtual en que los defectos, miserias y malos hábitos del ser humano, se reproducen con la misma facilidad que las virtudes. El efecto de aldea global generado por el entramado de redes y la proliferación de nodos en todo el planeta ayuda a la

---

15 PEÑA CABRERA, Raúl (1999) . pág. 63.

16 TELLEZ VALDEZ, Julio. *"Derecho Informático"*, Universidad Nacional Autónoma de México, 1991. pag. 82.

17 REYNA ALFARO, Luis Miguel: *"Los Delitos Informáticos – Aspectos Criminológicos, Dogmáticos y de Política Criminal*", JURISTA Editores. Lima, 2002. pág. 139.

difusión de inmediata de los mensajes y permite el acceso a cualquier información introducida en la red." [18]

2.13 DERECHO PENAL ECONÓMICO: En primer termino precisaremos que "... el *Derecho Penal* es fruto de las teorías penales existentes en Europa, cuyo contenido cambiaba conforme variaban las tendencias en Europa. Como ha ocurrido con otras ramas ajenas al Derecho penal, nuestra legislación penal ha estado influenciada por las y escuelas penales europeas. Cada institución jurídica lleva en si misma sus propios principios –actos simbólicos, formas de expresión- el cual es logrado a través de una selectiva evolución. Esta sistematización es un proceso lento que casi podríamos decir dura el mismo tiempo que dura la evolución de su propia cultura; una sistematización que muchas veces no llega a realizarse a plenitud... " [19]

De esta manera, se entiende que "... el *Derecho Penal Económico* constituye una nueva área jurídica actual, interdisciplinaria y, pese a concepciones históricamente antiguas, nueva, que todavía tiene un papel subordinados en los estudios –sobre todo los universitarios- que incluso son esporádicos. En cambio en la práctica, la importancia del derecho penal económico es cada vez más fuerte: aproximadamente uno de cada tres fiscales se ocupa de asuntos relacionado con el derecho penal económico...", es así que en un sentido más amplio: se consideran como delitos económicos a la evasión fiscal y fraude de subvenciones, a los delitos contra los bancos y las empresas de seguro, a los delitos de quiebra y falsificación de balance, así como a los delitos de adulteración de productos alimenticios y vinos, los delitos contra la competencia y a las violaciones contra embargos relacionados con el comercio exterior."[20]

2.14 DELITO CONTRA EL HONOR: El *honor*, en antropología social, gloria y buena reputación de las que goza el individuo. Para algunos autores, el concepto exacerbado de honor constituye no sólo un valor esencial sino un tópico propio de la antropología de los países mediterráneos; asimismo, el honor forma parte de la ética del individuo que se contempla a sí mismo a través de los ojos de los demás. Se relaciona con la reputación, la respetabilidad o la gloria, valores que se obtienen a partir del juicio de terceros frente a los que se quiere ocupar una posición superior, ya que se establece una lucha de poder mientras se cuestiona

[18] INSTITUTO NACIONAL DE ESTADISTICA E INFORMATICA (2001). Ob cit.

[19] PEÑA CABRERA, Raúl (1999). pág. 144

[20] TIEDEMAN, Klaus. . Ob cit. págs. 13 - 14

si los demás disfrutan de la misma integridad. No se goza de gloria ni de buena o mala reputación a menos que haya un tercero que así lo certifique. [21]

Asimismo, "... al respecto adquiere importancia la tesis expuesta por BERDUGO, la cual seguimos íntegramente. Este autor constituye el concepto de honor partiendo de un modelo de sociedad personalista, otorgándole un contenido que se acomoda a la participación del individuo en la sociedad, que sea respetuoso con el principio de igualdad..." [22]

2.15 DERECHO A LA INTIMIDAD: Con relación a la Intimidad, es definida como amistad intima. Parte personalísima, comúnmente reservada, de los asuntos, designios y afecciones de un sujeto o de su familia[23].

Es así que "... el principio de un *derecho a la intimidad* de la vida privada, como una forma de la libertad personal digna de protección jurídica es una conquista... de la conciencia humana... el *"right to privacy"...* comprende el respeto a una esfera amplia de la vida privada: No solo las relaciones intimas, sino también ciertos comportamientos personales, elementos distintivos de una personalidad biosíquica, las opiniones religiosas o políticas." [24] Así para el resguardo de los derechos a la intimidad, a la información, a la rectificación, a la voz, a la propia imagen, al honor y la buena reputación la Constitución Política de 1993, ha contemplado la garantía constitucional del Habeas Data.

De igual forma, podemos apreciar que "... con el desarrollo de la sociedad, el legislador se ha visto obligado a proteger penalmente la intimidad de las personas, teniendo en cuenta sobre todo el avance tecnológico alcanzado." [25]

En estos términos podemos afirmar que "... las controversias no solo se presentan cuando se transmiten datos calificados como "sensibles", es decir, cuando se refieren a la vida privada del sujeto, sin que este tenga el más mínimo conocimiento y, por tanto, carezca de su asentimiento. Es necesario retroceder un paso para evitar que la búsqueda - y no sólo posterior

---

21 BIBLIOTECA DE CONSULTA ENCARTA 2003.

22 BRAMONT - ARIAS TORRES, Luis Alberto y GARCIA CANTIZANO, María del Carmen, *"Manual de Derecho Penal Parte Especial",* Editorial San Marcos – Cuarta Edición. Lima, 1998. pág. 135 – 136.

23 Enciclopedia Universal Salvat (2009) Volumen 17, pág. 8202

24 NUÑEZ PONCE, Julio. *"Derecho Informático",* MARSOL Perú Editores S.A., Lima, 1996. pág. 64.

25 BRAMONT - ARIAS TORRES, Luis Alberto y GARCIA CANTIZANO, María del Carmen (1998) pág. 196.

transferencia de la información que se apetece - suponga violación de la privacidad de la persona." [26]

Considerando que, los ataques a la intimidad derivados de la tecnología informática, medios de comunicación escrita, radial, televisiva colocan a la persona en una situación de absoluta indefensión, por ello se ha se tiene que regular urgentemente ciertas conductas que se presentan como una nueva forma de criminalidad informática, en lo que se refiere las alteraciones en la información, la protección de los datos personales, los contratos informáticos, etc. La privacidad de las comunicaciones es objetivo constante de las nuevas tecnologías que amenazan, y que quizá también incentivan, el progreso de la humanidad.

Asimismo, respecto al Derecho a la Intimidad, también "…observamos a diario en las informaciones televisivas, cómo se utilizan aparatos avanzados de la llamada era 'Tecnológica' en las investigaciones policiales y persecución a los delincuentes. No menos instrumentos avanzados utilizarán en las investigaciones secretas y para fines de espionaje. Así también, existen instituciones privadas que realizan costosas investigaciones, creándose aparatos de alta tecnología que permiten la detección de la imagen o la palabra a largas distancias y que por su precio a veces diminuto es de fácil acceso al público. Existen pequeñísimos receptores que permiten escuchar conversaciones realizadas a grandes distancias de donde se halla quien espía, o facilitan conocer diálogos celebrados en el interior de habitaciones cerradas, o conversaciones telefónicas…" [27]

Es preciso resaltar que en la actualidad "…el ciudadano de la *sociedad tecnológicamente avanzada* se siente atemorizado porque presume que las conquistas del progreso se ven contrapuntadas por graves amenazas para su libertad, su identidad o incluso para su propia supervivencia. Esta amenaza latente para el ejercicio de las libertades, que obedece a las condiciones en que se desarrolla la vida colectiva de nuestra época se ha hecho particularmente acuciante en relación con el derecho a la intimidad. En etapas anteriores el respeto a la vida privada podía ser fácilmente tutelado por su titular. Para proteger la intimidad de sus propias acciones bastaba

[26] IUS ET PRAXIS, Revista de la Facultad de Derecho y Ciencias Políticas, Fondo de Desarrollo Editorial de la Universidad de Lima, Nro. 26 Enero – Diciembre, Lima, 1996. pág. 147.

[27] REVISTA ELECTRÓNICA DE DERECHO INFORMÁTICO. "*Breve ensayo sobre delitos de violación de la intimidad en la legislación Peruana*, C.J. VILLON MEDINA y M.P. VALDIVIA LUQUE, Abril 2003.

autoexcluirse del trato social de forma natural. Los muros de una casa, la soledad de un lugar desierto, incluso el tono expresivo oral del susurro eran suficientes para asegurar la protección de la intimidad y para excluir el conocimiento y la difusión de las acciones y de las palabras." [28]

2.16 ESPIONAJE INFORMÁTICO: "El *Espionaje*, consiste en la obtención secreta de información que la fuente informativa no desea revelar. El término se puede emplear en referencia a los ámbitos militar, económico o político, pero en general se relaciona con la política exterior y de defensa. De acuerdo con el Derecho internacional el espionaje es una actividad delictiva, y suele estar tipificado como delito de especial gravedad merecedor de máximas penas, especialmente cuando afecta a la seguridad del Estado. Tal es el caso de España, cuyo Código Penal sanciona su comisión con la reclusión mayor en su máximo grado. No obstante, la gran mayoría de los países cuentan con organismos oficiales, encargados de la consecución de información valiosa para su gobierno, que suelen ser denominados servicios de inteligencia del Estado.

Todas las formas y técnicas de espionaje actuales se apoyan en las cada vez más eficientes tecnologías de las comunicaciones y en dispositivos de medida y cálculo. Las cámaras miniaturizadas y el microfilm han hecho más fácil a las personas involucradas en cualquier forma de espionaje la obtención de fotografías de documentos secretos y la ocultación de las películas. Los satélites artificiales también suelen utilizarse en el espionaje realizando fotografías aéreas para detectar instalaciones militares secretas. Los piratas informáticos, independientes o contratados, pueden conseguir información o programas localizados en ordenadores. La vanguardia de todos estos desarrollos es secreta, pero se sabe que los teléfonos pueden ser interceptados sin intervención física, que se pueden colocar dispositivos electrónicos de escucha y grabación en una habitación sin entrar en ella y que se pueden tomar fotografías en la oscuridad". [29]

Así "... los *delitos de espionaje informático* se refieren principalmente a la obtención – generalmente por parte de competidores – de resultados de investigación, direcciones de clientes, etc. Pueden ser cometidos introduciendo programas copiadores, o por otros métodos (la radiación

[28] REVISTA ELECTRÓNICA DE DERECHO INFORMÁTICO.*"El derecho a la intimidad en una sociedad informatizada"*, María Barberá Fraguas Enero de 2002

[29] BIBLIOTECA DE CONSULTA ENCARTA 2003. Microsoft Corporation. © 1993-2002.

electrónica que emite una terminal de computación puede ser captada y registrada sin mayor complicación hasta cerca de un kilómetro de lugar de la instalación). Es cuestionable si la figura del "robo" – que requiere de privación permanente de un bien a la víctima – se adecua a esta acción delictual." [30]

Por otro lado se entiendo por *espionaje informático* a "...la actividad de obtener sin autorización datos o programas o divulgar los obtenidos legítimamente. En el ámbito del procesamiento de datos, el espionaje económico se ve favorecido por el hecho de que las informaciones se encuentran archivadas en un espacio mínimo y pueden ser transferidas sin problema alguno a otro soporte. Además, dentro del uso indebido de datos, figura siempre el llamado hurto de software; es decir, el empleo indebido de programas de computación, los cuales requieren mucho esfuerzo y dedicación, afectándose también comercialmente por el mal uso que algunas personas les dan al realizar la llamada piratería." [31]

2.17 ESTAFA INFORMÁTICA: la estafa se consume cuando el bien sustraído pasa a manos del culpable, aunque no se haya todavía el lucro. Elementos: 1) una defraudación real o efectiva, y no la mera posibilidad de un perjuicio, de naturaleza económica y valorable, ya que el importe del valor de la estafa es la base de la sanción penal que corresponda; 2) engaño, que es su primordial característica; 3) conexión o relación de causalidad entre la defraudación y sus efectos, y 4) ánimo de lucro, o propósito de obtener beneficio gracias a la defraudación de la cosa ajena, ya se trata de bienes muebles o inmuebles[32].

Respecto al fraude por manipulaciones de un computador contra un sistema procesamiento de datos, "... incluye el cambio de datos o informaciones para obtener un beneficio económico. Estos delitos pueden afectar datos que representen activos (depósitos monetarios, créditos, etc.), o bien objetos materiales (manejo de inventarios). Su perpetración puede acrecentarse en la medida que se difunden los cajeros automáticos, puntos de venta (POS) y otras máquinas electrónicas. La acción criminal puede basarse en la introducción de datos falsos por la computadora (diversos casos de este tipo

30 CORREA, Carlos y otros: *"Derecho Informático"*, Ediciones de Depalma, Buenos Aires, 1987.

31 RIOS ESTAVILO, José Luis. *"Derecho e Informática en México – Informática Jurídica y Derecho de la Informática"*, Universidad Nacional Autónoma de México., 1997 pág. 124.

32 Enciclopedia Universal Salvat (2009) Volumen 12. pág. 5619

se han dado en entidades bancarias), o bien en la modificación de los resultados." [33]

2.18 GLOBALIZACIÓN: El término globalización es utilizado en la actualidad en esferas tan diferentes (la de los negocios, la de los medios de comunicación, la del hombre de la calle, la de la sociología) y con matices y connotaciones tan distintas que ha perdido parte de su poder de definición convirtiéndose muchas veces en fuente de ambigüedad y de incomprensión entre diferentes grupos. El citado sistema mundial único de relaciones económicas, políticas, etc., corresponde al denominado sistema-mundo capitalista, en la terminología del sociólogo estadounidense I. Wallerstein[34].

La globalización es un fenómeno principal, pero no excluyentemente económico que caracteriza por la creación a escala casi mundial de redes de intercambio como nunca antes las habíamos conocido, sobre la base de una nueva compresión de las dimensiones temporal y espacial. La novedad de esta nueva ordenación del mundo no se encuentra en la existencia del intercambio, porque éste siempre a existido; por el contrario, lo novedoso radica tanto en la calidad, escala y cantidad de estos intercambios, que ya no sólo recaen sobre bienes tangibles, sino que, además, sobre personas, capitales y servicios[35].

2.19 HACKER: Experto en informática capaz de entrar en sistemas cuyo acceso es restringido. No necesariamente con malas intenciones. Originalmente, término utilizado para referirse a un aficionado a los ordenadores o computadoras, totalmente cautivado por la programación y la tecnología informática, persona que disfruta explorando detalles de los sistemas programables.

Es quien intercepta dolosamente un sistema informático para dañar, apoderarse, interferir, desviar, difundir, y/o destruir información que se encuentra almacenada en computadoras pertenecientes a entidades públicas o privadas. El término hacker en castellano significa "cortador". Los "Hackers", son fanáticos de la informática, generalmente jóvenes, que tan solo con un computador personal, un módem, gran paciencia e imaginación son capaces

33 CORREA, Carlos y otros (1987). pág. 296.

34 Enciclopedia Universal Salvat (2009) Volumen 15. pág. 6921

35 FAJARDO CABANA Patricia: "*Nuevos retos del Derecho Penal en la era de la Globalización"*, Editorial Tirant lo Blanch, Valencia, 2004. pág. 157-157.

de acceder a través de una red pública de transmisión de datos, al sistema informatizado de una empresa o entidad pública, saltándose todas las medidas de seguridad, y leer la información, copiarla, modificarla, preparando las condiciones idóneas para llamar la atención sobre la vulnerabilidad de los sistemas informáticos, o satisfacer su propia vanidad.[36]

Asimismo, "... originalmente, término utilizado para referirse a un aficionado a los ordenadores o computadoras, totalmente cautivado por la programación y la tecnología informática. En la década de 1980, con la llegada de las computadoras personales, y posteriormente con la posibilidad de conexión a los grandes sistemas de ordenadores a través de Internet, este término adquirió una connotación peyorativa y comenzó a usarse para denominar a quien se conecta a una red para invadir en secreto computadoras, y consultar, alterar o eliminar los programas o los datos almacenados en las mismas, aunque a eso es a lo que dedican su atención los denominados crackers. También se utiliza para referirse a alguien que, además de programar, disfruta desensamblando sistemas operativos y programas para entender su lógica de funcionamiento, para lo que utiliza programas que desensamblan el código y realizan operaciones de ingeniería inversa. [37]

2.20 INFORMÁTICA: Antes pasar a definir la informática jurídica, definiremos a *la informática,* la misma que es definida por La Real Academia de la Lengua Española, como: "el conjunto de conocimientos científicos y técnicas que hacen posible el tratamiento automático de la información por medio de ordenadores". De igual forma la Enciclopedia de Consulta de Encarta 2003, define a la Informática o Computación, "como el conjunto de conocimientos científicos y de técnicas que hacen posible el tratamiento automático de la información por medio de computadoras. La informática combina los aspectos teóricos y prácticos de la ingeniería, electrónica, teoría de la información, matemáticas, lógica y comportamiento humano. Los aspectos de la informática cubren desde la programación y la arquitectura informática hasta la inteligencia artificial y la robótica".[38]

---

36 BIBLIOTECA DE CONSULTA ENCARTA 2003.

37 INSTITUTO NACIONAL DE ESTADISTICA E INFORMATICA (2001). Ob cit. pág. 30

38 BIBLIOTECA DE CONSULTA ENCARTA 2003

2.21 INFORMÁTICA JURÍDICA: Es definida por Julio TELLEZ VALDÉZ "...como un conjunto de aplicaciones de la informática en el ámbito jurídico; de tal forma que en términos conceptuales entendemos por informática jurídica a la técnica interdisciplinaria que tiene por propósito la aplicación de la informática (entiéndase computadoras) para la recuperación de información jurídica, así como la elaboración y aprovechamiento de los instrumentos de análisis y tratamiento de dicha información, necesarios para una toma de decisión con repercusiones jurídicas".[39]

De igual forma Julio NUÑEZ PONCE, define a la informática jurídica como "la aplicación de la Informática al Derecho permitiendo que exista una base de datos computarizada, se automatice la gestión de un estudio, secretaría de juzgados, notaria, etc. y se sistematice el conocimiento jurídico a través de la inteligencia artificial".[40]

Por otro lado, el Dr. Juan José BLOSSIERS HUME, señala que: "... existen otros términos para denominar a la informática jurídica; para evitar confusión adoptamos este nombre más explicativo de una de las sub áreas del derecho informático, la cual puede considerarse como una tecnología aplicada a la automatización a un conjunto de datos jurídicos pertinente, según el criterio usado. De una forma más simple: es automatizar la información jurídica."[41]

2.22 INSTRUMENTO O MEDIO: Es todo medio probatorio que conste por escrito, en papel u otro medio material similar. Algunos autores le confieren un sentido más amplio; instrumento es todo lo que sirve para instruir una causa, todo cuanto da luz la existencia de un hecho o convenio. Asimismo, instrumento del delito, son todos los objetos o elementos materiales utilizados por los autores de un evento criminal antes, y después del mismo[42].

2.23 INTERNET: Conocida como, red de redes. Sistema mundial de redes de computadoras interconectadas. Fue concebida a fines de la década de 1960 por el Departamento de Defensa de los Estados Unidos; más precisamente, por la ARPA. Se la llamó primero ARPANET y fue pensada para cumplir funciones de investigación. Su uso se popularizó a partir de la creación de la

---

39 TELLEZ VALDEZ, Julio (1991) pág. 14.

40 NUÑEZ PONCE, Julio. (1996) págs. 21 y 22.

41 BLOSSIERS HUME, Juan José, *"Informática Jurídica".* Editorial Librería Portocarrero. Lima, 2003.pág. 57

42 FLORES POLO Pedro (1984) Tomo II, pág. 98-99

World Wide Web. Actualmente es un espacio público utilizado por millones de personas en todo el mundo como herramienta de comunicación e información.

En el año 1983, el crecimiento de la red llevó al ejército a dividir la red en dos partes: ARPANET, para usos civiles y el MILNET, para usos militares, esta segunda red quedo restringida y a salvo del acceso privado. La primera red se convirtió en la actual Internet y quedo abierta a cualquiera que desease acceder a la misma. Así, progresivamente, se ha ido configurando el Internet como un conjunto de redes conectadas en el ámbito mundial. Internet comprende redes de casi todos los países. Se ha creado de esta forma un gran entramado donde cualquier computadora conectada a cualquier subred de Internet, está a la vez conectada a cualquier otra subred[43].

Asimismo, se entiende por Internet, a "... la interconexión de redes informáticas que permite a los ordenadores o computadoras conectadas comunicarse directamente, es decir, cada ordenador de la red puede conectarse a cualquier otro ordenador de la red. El término suele referirse a una interconexión en particular, de carácter planetario y abierto al público, que conecta redes informáticas de organismos oficiales, educativos y empresariales. También existen sistemas de redes más pequeños llamados intranets, generalmente para el uso de una única organización, que obedecen a la misma filosofía de interconexión. La tecnología de Internet es una precursora de la llamada "superautopista de la información", un objetivo teórico de las comunicaciones informáticas que permitiría proporcionar a colegios, bibliotecas, empresas y hogares acceso universal a una información de calidad que eduque, informe y entretenga. A finales de 1998 estaban conectados a Internet unos 148 millones de ordenadores, y la cifra sigue en aumento." [44]

2.24 NOMBRES DE DOMINIO: Los nombres de dominio no son otra cosa que la dirección de Internet consignada en palabras, de forma tal que resulta fácilmente comprensible para el usuario de Internet. El funcionamiento de este sistema de nombres de dominio ("domain names system" - DNS) es a través de bases de datos con lista de los nombres de dominio y sus respectivas direcciones IP. El "domain name", se compone de dos elementos, uno identificador (ejemplos

[43] CARRETERO, Jesús y otros: "Descubre Internet" , editorial PEARSON EDUCACION S.A., Madrid. 2004, pág. 4
[44] BIBLIOTECA DE CONSULTA ENCARTA 2003

conocidos hay muchos: "yahoo", "terra", etc.) y otro que sirve de referencia al nivel al que pertenecen ("com.", "edu", "gob" entre otros"). [45]

Cuando *"... una empresa que desea hacer negocio en Internet debe, en primer lugar, necesariamente debe identificarse como tal en la red. La atribución de un nombre de dominio simbolizará para la empresa su acta de nacimiento y existencia en el mundo virtual, así como el medio como el medio para identificar su actividad, sus productos y/o servicios. La elección de un nombre de dominio es, por tanto, una de las principales y primeras decisiones que deben de tomar a la hora de crear un negocio virtual. Además, su protección deberá ser de gran importancia. Cada computadora, o servidor, conectado a Internet es identificado por un número único llamado Dirección de Protocolo de Internet (IP address). Este número IP se presenta bajo la forma de cuatro números (cada uno entre 0 y 225) separados por un punto del tipo: 192.52.5.16 Un nombre de dominio presentará una estructura del tipo: http://www.nombrededominio.com/*". [46]

2.25 OFENSAS CONTRA EL PUDOR PÚBLICO: Como bien indica Bramont – Arias Torres y García Cantizano al referirse que: "El Capítulo IX del Título IV del Libro II del Código Penal, al igual que en el Código Penal anterior, se denomina "Ofensas contra el pudor público", por lo que se identifica el bien jurídico protegido con el pudor público. Según la moderna doctrina penal, el Derecho penal no puede proteger meros contenidos morales, si es que se quiere aceptar la idea de que solo han de perseguirse conductas que posean una apreciable nocividad social" [47]

El Internet, avance tecnológico de enorme potencial en beneficio de la educación, que puede ser empleado con magníficos resultados, pero que desafortunadamente es utilizado también para promocionar la pornografía infantil. El aumento vertiginoso de las computadoras y el uso de Internet, plantea el desafío de contar con normas que sancionen como delito, la transmisión de pornografía infantil a través de Internet o de cualquier otro medio de archivo de datos, reconociendo que el desarrollo de nuevas tecnologías para la producción y transmisión de la pornografía es muy rápido y que se podrán presentar otras formas más sofisticadas de transmisión. Tipo penal que deberá sancionar el uso de un sistema de cómputo o de cualquier

45 REYNA ALFARO, Luis Miguel (2002) pág. 117

46 IASONI Marie: "Comercio Electrónico, Aspectos Legales", Editorial Librería Portocarrero. Lima, 2002. 25 – 26

47 BRAMONT - ARIAS TORRES, Luis Alberto y GARCIA CANTIZANO, María del Carmen. (1998) págs. 277 – 278.

otro mecanismo de archivo de datos con la finalidad de exhibir a menores de edad realizando actos de exhibicionismo corporal, lascivos, agregándose el término pornográfico, por considerarse más aplicable.

Es en este sentido que la Congresista de la República Enith CHUQUIVAL SAAVEDRA, pretende contemplar y precisar un nuevo tipo penal relacionado con el uso del Internet, la misma que va acorde con el avance de la tecnología, pretende cautelar la condición vulnerable que presentan los niños y las niñas, principales víctimas de explotación sexual no sólo en la modalidad de prostitución infantil, sino en pornografía infantil, turismo sexual y/o venta de niños. El Estado les debe protección, por ello, debe combatir a los que los explotan al utilizarlos para sacar ventaja o provecho de carácter sexual y/o económico a la infancia. Asimismo, indica que debe ser considerado también dentro del tipo penal las conductas de elaboración, producción, ofrecimiento, distribución y de accesibilidad del material pornográfico a través de un sistema de cómputo o cualquier otro mecanismo de archivo de datos. Siendo importante que el texto penal cuente con una definición amplia sobre pornografía que permita al juzgador su plena identificación. Dicho proyecto presentaba los siguientes Artículos que se incorporarían al Código Penal, en Materia de Pornografía Infantil en Internet (Art. 183-B y 183-C):

Articulo 1°. *- Adicionase los artículos 183-B y 183-C al Capítulo XI -Ofensas al Pudor Público- del Código Penal, con el siguiente texto:*

*"**Artículo 183-B**. - Al que procure o facilite por cualquier medio el que uno o más menores de dieciocho años, con o sin su consentimiento, lo o los obligue o induzca a realizar actos de exhibicionismo corporal, lascivos, o pornográficos con el objeto y fin de videograbarlos, fotografiarlos o exhibirlos mediante medios impresos, electrónicos o de un sistema de datos a través de cómputo o de cualquier otro mecanismo de archivos de datos, con o sin el fin de obtener un lucro, se le impondrán la pena privativa de libertad no menor de cinco ni mayor de doce años y con trescientos sesenta y cinco días multa".*

"Al que fije, grabe, imprima actos de exhibicionismo corporal, lascivos o pornográficos, en que participen uno o más menores de dieciocho años, se le impondrá la pena de cinco a doce años de pena privativa de la libertad y de trescientos sesenta y cinco días multa. La misma pena se impondrá a quien con fines de lucro o sin él, elabore, produzca, reproduzca, ofrezca, venda, arriende, exponga, publicite, haga accesible, distribuya o trasmita a través de un sistema de computo o cualquier otro mecanismo de archivo de datos, el material a que se refiere el presente artículo".

*"**Artículo 183-C**. - Para los efectos de estos artículos se entiende por pornografía*

infantil, toda representación de un menor de edad dedicado a actividades explícitas reales o simuladas de carácter sexual, realizada a través de escritos, objetos, medios audiovisuales, electrónicos, sistemas de cómputo o cualquier medio que pueda utilizarse para la comunicación y que tienda a excitar sexualmente a terceros, cuando esta representación no tenga valor artístico, literario, científico o pedagógico."

***Artículo 2°.** - La presente ley entrará en vigencia al día siguiente de su publicación en el Diario Oficial "El Peruano".* [48]

2.26 PATRIMONIO: el patrimonio es definido, "…desde el punto de vista jurídico, es la universalidad constituida por el conjunto de derechos y obligaciones que corresponden a una persona y pueden ser apreciables en dinero (Osorio)". Cable resaltar que "…la controversia sobre la naturaleza jurídica del patrimonio se ha extendido al campo del derecho penal, en el cual habría sido preferible que no entrara, dice Raniere, sosteniendo que generalmente en este campo el patrimonio no se tiene en cuenta como unidad distinta de los elementos que lo componen, esto es, como "universitas", sino como conjunto de derechos que el sujeto individualiza pero que la ley no unifica, creando una unidad autónoma. Si esto es exacto -agrega- lo que queda de la disputa mencionada es poca cosa y de tan poca monta que no puede justificar la distinción de los delitos contra el patrimonio en dos grandes grupos, como sostiene Edmund Mexguer."[49]

Asimismo, la "... concepción mixta o jurídico – económico del patrimonio: es esta la posición que actualmente asume la doctrina con carácter mayoritario. Desde esta concepción, el patrimonio está constituido por la suma de valores económicos puestos a disposición de una persona, bajo la protección del ordenamiento jurídico. Un aspecto digno de ser resaltado es el grado de reconocimiento jurídico requerido en los bienes de contenido económico para constituir el patrimonio..." [50]

2.27 PIRATA INFORMÁTICO: Es aquella persona que copia, reproduce, vende, entrega un programa de software que no le pertenece o que no tiene licencia de uso, a pesar de que el programa está correctamente registrado como propiedad intelectual en su país de origen o en otro país, esta persona adultera su estructura, su procedimiento de instalación, copiándolo directamente y

---

48 Diario Oficial "El Peruano", de fecha de Publicación 09 de Mayo del 2002

49 FLORES POLO, Pedro. "*Diccionario de Términos Jurídicos",* Editores Importadores, Lima 1984. págs. 283 – 284

50 BRAMONT - ARIAS TORRES, Luis Alberto y GARCIA CANTIZANO, María del Carmen. (1998) Ob cit. pág. 285.

reproduciendo por cualquier medio la documentación que acompaña al mismo programa. [51]

2.28 **PHREAKER:** Este grupo es bien conocido en la Red por sus conocimientos en telefonía. Un Phreaker posee conocimientos profundos de los sistemas de telefonía, tanto terrestres como móviles. En la actualidad también poseen conocimientos de tarjetas prepago, ya que la telefonía celular las emplea habitualmente. Sin embargo es, en estos últimos tiempos, cuando un buen Phreaker debe tener amplios conocimientos sobre informática, ya que la telefonía celular o el control de centralitas es la parte primordial a tener en cuenta y/o emplean la informática para su procesado de datos.

Persona que ingresa al sistema telefónico, teniendo o no equipo de computación, con el propósito de apoderarse, interferir, dañar, destruir, conocer, difundir, hacer actos de sabotaje, o hacer uso de la información accediendo al sistema telefónico, provocando las adulteraciones que en forma directa, conlleva este accionar, con su consecuente perjuicio económico. Estos tipos con unos conocimientos de telefonía insuperables, conocen a fondo los sistemas telefónicos incluso más que los técnicos de las compañías telefónicas. La modernización de las redes hizo necesario que los phreakers utilizaran técnicas menos éticas, como robar números de *calling cards,* los obtenían colocándose cerca de un teléfono público y memorizando el número de tarjeta que marcaba un usuario descuidado. Una vez obtenida la clave, la información era esparcida de tal manera que en un caso se llegaron a realizar 600 llamadas internacionales en dos minutos antes de que los operadores de seguridad del sistema la cancelaran. [52]

2.29 **SABOTAJE INFORMÁTICO:** Es defendido como: "… cualquier actividad encaminada a la inhabilitación temporal o permanente, parcial o total de los medios informáticos con la finalidad de vulnerar la capacidad productiva de la empresa propietaria de esos medios u organismo público." [53]

De igual formas "... el sabotaje informático puede referirse a los datos y los programas (por ejemplo, una "bomba de tiempo" que destruye el programa, o una "rutina de cáncer" que destruye el funcionamiento de aquel mediante

[51] Ibidem. pág. 32

[52] INSTITUTO NACIONAL DE ESTADISTICA E INFORMATICA (2001), pág. 31

[53] INSTITUTO NACIONAL DE ESTADISTICA E INFORMATICA (2001), pág. 112.

instrucciones que se autoreproducen), o bien al equipamiento en si. En algunas legislaciones, como se ha visto, y otras propuestas de ley en Francia, Suiza, Portugal, etc., se han elaborado para paralizar el daño cometido aun sólo cuando abarque bienes intangibles (datos y programas)." [54]

Por otro lado se entiende por sabotaje informático a "... las conductas que persiguen la destrucción o incapacidad de los sistemas informáticos o de algún elemento que la compone (hardware y software), así tenemos el sabotaje al procesamiento de datos; este resulta favorecido por la gran concentración de información en un mínimo espacio." [55]

2.30 **TELEMÁTICA:** Se entiendo que la telemática se origina de una contracción de teleinformática, es un concepto tan vivo aunque engloba una gran cantidad de servicios operativos o proyectos, hoy telemática es correo electrónico, facsímil, teleconferencias, telemedicina, televenta, transferencia electrónica de datos, entre otros servicios e igualmente es enlaces de datos entre computadoras como Internet y otras redes extranet, intranet etc.

De igual forma, telemática, es definido como el conjunto de servicios y técnicas que asocian las telecomunicaciones y la informática. La telemática ofrece posibilidades de comunicación e información, tanto en el trabajo como en el hogar y otros ámbitos personales. Agrupa servicios muy diversos, por ejemplo, la telecopia, el teletexto, las redes telemáticas como Internet y las comunicaciones inalámbricas, una de cuyas aplicaciones más visibles es el Sistema de Posicionamiento Global o GPS. [56]

2.31 **VIRUS:** Programa que se duplica a si mismo en un sistema informático incorporándose a otros programas que son utilizados por varios sistemas. Este tipo de programas puede actuar de diversas maneras:

a) Solamente advertir al usuario de su presencia, sin causar daño aparente.
b) Tratar de pasar desapercibidos para causar el mayor daño posible.
c) Adueñarse de las funciones principales (infectar los archivos de sistema)[57].

---

54 CORREA, Carlos y otros (1987) pág. 297.

55 RIOS ESTAVILO, José Luis.(1997) pág. 124.

56 BIBLIOTECA DE CONSULTA ENCARTA 2003

57 GIL ALBARRAN Guillermo, "Derecho Informático" Grupo Editorial Megabyte, Lima – 2007, pág. 752 - 753

CAPÍTULO III:

MARCO TEÓRICO

A continuación al desarrollaremos el Capítulo Tercero, en el cual trataremos el marco teórico del presente trabajo de investigación, donde realizaremos algunas precisiones sobre la criminalidad informática y las diversas definiciones de los llamados "delitos informáticos" realizado por juristas nacionales y extranjeros, arribando finalmente a una posición personal con relación a la definición de estos delitos de nueva data.

Asimismo, en este Capítulo trataremos sobre las características y clasificación de los delitos informáticos; así como las características del delincuente informático y sobre los bienes jurídicos afectados por estos delitos de nueva data.

3.1 Algunas precisiones sobre la criminalidad informática y la definición de los "delitos informáticos"

En estos últimos años el mundo entero ha experimentado un sorprendente y explosivo avance en el desarrollo de la *ciencia informática, telemática y el Internet*; no cabe duda que la "era digital" ha otorgado y seguirá proporcionado innumerables beneficios a nuestra sociedad, sin embargo no podemos desconocer que este desarrollo tecnológico ha propiciado, también, la aparición de nuevas modalidades delictivas, las que hasta hace poco eran desconocidas en nuestro ordenamiento jurídico.

El cambio social operado en las últimas décadas, resulta íntimamente vinculado a la *evolución tecnológica* operada en ese transcurso de tiempo, generándose problemas para la protección de intereses sociales no convencionales y para la represión de las conductas delictivas realizadas a través de medios no convencionales, pues como bien precisa ZAFFARONI: "…el impacto de la explosión tecnológica es un problema de *política criminal* que conoce sobradamente. La técnica siempre es un arma y cada avance fue explotado criminalmente, en forma tal que siempre el criminal está más tecnificado que la prevención del crimen".[1]

De igual forma por su parte Luis Miguel Bramont-Arias Torres, señala que "…el fenómeno informático es una realidad incuestionable y parece que también irreversible, la informática se instalado entre nosotros. El principal problema se traduce en buscar fórmulas efectivas de control respecto a las

[1] REYNA ALFARO, Luis Miguel. *"Los Delitos Informáticos – Aspectos Criminológicos, Dogmáticos y de Política Criminal"*, JURISTA Editores E.I.R.L. Lima, 2002. pág.125.

cuales el Derecho ha de tener un marcado protagonismo, en su papel de regulador de las relaciones y mecanismos sociales para el mantenimiento de un orden social". [2]

Muchas discusiones se han planteado en torno al concepto del delito informático – computer crime ó computer kriminalitat- para algunos autores es no es más que el delito cometido bajo el empleo de medios informáticos, es decir, constituyen nuevas formas de comisión de conductas ya descritas en sede penal, rechazando la existencia de un bien jurídico autónomo para esta clase de delitos. Para otro sector de la doctrina el delito informático tiene un contenido propio, afectando así un nuevo interés social cuyo reconocimiento legislativo urge, diferenciando así entre delitos computacionales –como nuevas formas comitivas de delitos- y delitos informáticos, aquellos que afectan el novísimo bien jurídico penal propuesto. Finalmente, existe una vertiente, defendida por la doctrina de habla inglesa, que hace una diferencia tripartita en que la informática aparece como medio para cometer delitos tradicionales, como fin en si misma y como medio de prueba.[3]

A continuación procederemos a definir a los delitos informáticos, teniendo en consideración que en la actualidad no existe una definición de carácter universal, motivo por el cual citaremos algunas de las definiciones por parte de juristas expertos en el tema de investigación tanto nacionales, como extranjeros.

Luis Miguel Bramont – Arias Torres, indica que: "... en realidad no existe un bien jurídico protegido en el delito informático, porque en verdad no hay como tal un delito informático. Este no es más que una forma o método de ejecución de conductas delictivas que afectan a bienes jurídicos que ya gozan una específica protección por el Derecho Penal".[4]

Juan José Blossiers Mazzini y Sylvia Calderón García, precisan que "Parece ser lo que en realidad vulnera esta novedosa tipología es una violación mixta de valores jurídicos, que en algunos casos compromete tanto al patrimonio como la libertad de las personas o el sistema informático y la

[2] BRAMONT–ARIAS TORRES, Luis Alberto, *"El Delito Informático en el Código Penal Peruano"*, Fondo Editorial de la Pontificia Universidad Católica del Perú. Lima, 1997. pág. 17

[3] REYNA ALFARO, Luis Miguel, (2002) pág. 237 – 239.

[4] BRAMONT - ARIAS TORRES, Luis Alberto Ob. cit. pág. 58

protección de datos. No solo se vulneran valores de carácter económico sino de carácter tan valioso como la intimidad, lo que hace imposible negar su existencia."[5]

Luis Miguel Reyna Alfaro, manifiesta que: " … resulta evidente que si bien existen diferencias claras entre ambos conceptos –delitos computacionales y delitos informáticos-, ambos forman parte de un mismo fenómeno criminal cuya denominación correcta sería la de criminalidad mediante computadoras" y por la cual debe entenderse a todas las conductas criminales para cuya comisión se emplee los ordenadores o en las cuales resulte afectada la información contenida en los sistemas informáticos."[6]

Juan José Blossiers Hume, con relación a la definición de esta nueva forma de criminalidad indica que es "…innegable, el uso las nuevas tecnologías conduce a la ampliación y creación de nuevos delitos en todas partes del mundo. Dichas conductas delictivas son producto del adelanto tecnológico del que somos usuarios y como señalan los tratadistas, que el moderno Derecho Penal necesita asumir y afrontar los conceptos y estrategias de la criminalidad sobre todo en conexión con nuevos fenómenos delictivos…"[7].

Julio Nuñez Ponce, precisa que: "En plano de la dogmática jurídico – penal, la criminalidad informática puede suponer una nueva versión de delitos tradicionales."[8]

Renato Javier Jijena Leiva, lo define como: "... toda acción típica, antijurídica y culpable, para cuya consumación se usa la tecnología computacional o se afecta a la información contenida en un sistema de tratamiento automatizado de la misma."[9]

Julio Téllez Valdés, define a *Los Delitos Informáticos* como "…actitudes ilícitas en que se tienen a las computadoras como instrumento o fin"

---

5 BLOSSIERS MANZZINI, Juan José y CALDERON GARCIA Silvia B., *"Delitos Informáticos en la Banca".* Editora ROA SRL. Lima, 2000

6 REYNA ALFARO, Luis Miguel Ob. cit.. pág. 138 – 139.

7 BLOSSIERS HUME, Juan José. (2003) págs. 139 –140.

8 NUÑEZ PONCE, Julio. Los Delitos Informáticos, en REDI Nro. 15

9 JIJENA LEIVA Renato Javier, "La criminalidad informática: Situación de Lege ferenda en Chile". En Actas del III Congreso Iberoamericana de Informática y Derecho", Mérida, 1992. pág. 508

(concepto atípico) o las "conductas típicas, antijurídicas y culpables en que se tienen a las computadoras como instrumento *o* fin…'' (concepto típico)[10].

María de la Luz Lima, define el "delito electrónico" "en un sentido amplio como cualquier conducta criminógena o criminal que en su realización hace uso de la tecnología electrónica ya sea como método, medio o fin y que, en un sentido estricto, el delito informático , es cualquier acto ilícito penal en el que las computadoras, sus técnicas y funciones desempeñan un papel ya sea como método, medio o fin"[11].

Rafael Fernández Calvo, el delito informático es "la realización de una acción que reuniendo las características que delimitan el concepto de delito, se ha llevado a cabo, utilizando un elemento informático o telemático contra los derechos y libertades de los ciudadanos"[12]

Organización para la Cooperación Económica y el Desarrollo (OCDE)[13], define la delincuencia informática en un sentido amplio, como referido a todo delito que implique la utilización de las tecnologías informáticas. Los conceptos de «delincuencia informática», «delincuencia relacionada con la informática», «delincuencia de alta tecnología» y de «delincuencia cibernética» tienen el mismo significado en la medida que todos se refieren a: a) la explotación de las redes de información y comunicación sin ninguna dificultad geográfica y b) la circulación de datos intangibles y volátiles.

Luego de efectuar las diferentes definiciones de los denominados delitos informáticos, por parte de autores tanto nacionales como extranjeros, nos ha permitido realizar una aproximación a la definición de estos delitos de nueva data como los denominados delitos informáticos, donde hemos podido apreciar que no hay una definición común entre autores.

En tal sentido, podemos arribar a la conclusión de que no existe una definición formal y universal del delito informático, por lo que se han formulado conceptos respondiendo a realidades nacionales concretas "… no

10 TELLEZ VALDEZ, Julio. *"Derecho Informático"*, Universidad Nacional Autónoma de México. México - 1991. pag. 82.

11 LIMA de la LUZ, María. Criminalia N° 1-6 Año L. Delitos Electrónicos. Ediciones Porrua. Enero-Julio 1984

12 Fernández Calvo Rafael. El tratamiento del llamado delito informático en el proyecto de ley orgánico del Cód. Penal: Reflexiones y propuestas de la C.L.I.- Comisión de libertades e informática

13 http://europa.eu/legislation_summaries/justice_freedom_security/fight_against_organised_crime/l33193b_es.htm

es labor fácil dar un concepto sobre delitos informáticos, en razón de que su misma denominación alude a una situación muy especial, ya que para hablar de "delitos" en el sentido de acciones típicas, es decir tipificadas o contempladas en textos jurídicos penales, se requiere que la expresión "delitos informáticos" esté consignada en los códigos penales, lo cual en nuestro país, al igual que en otros muchos no han sido objeto de tipificación aún."[14]

Entre los autores nacionales tenemos a Luis Miguel Bramont – Arias Torres, quien indica que no existe un delito informático, que esta nueva forma de criminalidad solo es una forma o método de ejecución de conductas delictivas que afectan bienes jurídicos que ya gozan de protección por nuestra legislación penal vigente; por otro lado la posición antes mencionada es contradecida Juan José Blossiers Mancini y Silvia Calderón García, quienes precisan que parece ser lo que en realidad vulnera esta novedosa tipología es la violación mixta de valores jurídicos; asimismo, otro autor como Luis Miguel Reyna Alfaro indica que la denominación correcta sería la de criminalidad mediante computadora; motivo por el cual podemos precisar que autores como Julio Nuñez Ponce y Juan José Blossiers Hume indican que estos delitos de nueva data tienen como definición correcta la de criminalidad informática, siendo estos delitos una nueva versión de los delitos tradicionales.

Con relación a los autores extranjeros de igual forma como en el caso de los autores nacionales no existe una definición en común, como es el caso de la definición realizada por Renato Javier Jijena Leiva, quien indica estos delitos de nueva data es toda acción típica, antijurídica y culpable, para cuya consumación se usa la tecnología computacional; asimismo, Julio Téllez Valdés indica estos delitos son actitudes ilícitas en que se tienen a las computadoras como instrumento o fin" o las "conductas típicas, antijurídicas y culpables en que se tienen a las computadoras como instrumento o fin.

Asimismo, María de la Luz Lima indica que este delito de nueva data es una conducta criminógena o criminal que en su realización hace uso de la tecnología electrónica ya sea como método, medio o fin, esta posición es respaldada por Rafael Fernández Calvo quien indica quien indica que para realizar este delito de nueva data se utilizando un elemento informático o

[14] TÉLLES VALDEZ, Julio. Derecho Informático. 2° Edición. Mc Graw Hill. México D.F. 1996 Pág. 103-104

telemático; asimismo, Julio Téllez Valdés precisa que las actitudes ilícitas en que se tienen a las computadoras como instrumento o fin" o las "conductas típicas, antijurídicas y culpables en que se tienen a las computadoras como instrumento *o* fin.

Finalmente, luego de analizar las diferentes definiciones y posiciones adoptadas por los juristas nacionales y extranjeros con relación a la correcta definición éstos delitos de nueva data denominados delitos informáticos, nos ha permitido arribar a una posición personal, debiendo ser la definición e identificación más apropiada de estos delitos de nueva data es la de **"**Criminalidad Informática***",*** debido a que estos ilícitos son una nueva forma de criminalidad, nuestra posición es reafirmada cuando Luis Bramont Arias – Torres precisa que esta estos delitos de nueva data son una forma o método de ejecución de conductas delictivas que afectan bienes jurídicos que ya gozan de protección por nuestra legislación penal.

3.2 Características de los Delitos Informáticos

Con relación a las características de estos delitos de nueva data, hemos tomado en cuenta las características indicadas por el jurista mexicano Julio Téllez Valdez[15], al ser quien define en forma más completa y son las siguientes:

a) Son conductas *criminales de cuello blanco* (White collar crime), en tanto que sólo un de terminado número de personas con ciertos conocimientos (en este caso técnicos) puede llegar a cometerlas.
b) Son *acciones ocupacionales*, en cuanto a que muchas veces se realizan cuando el sujeto se halla trabajando.
c) Son *acciones de oportunidad*, ya que se aprovecha una ocasión creada o altamente intensificada en el mundo de funciones y organizaciones del sistema tecnológico y económico.
d) Provocan serias *pérdidas económicas*, ya que casi siempre producen "beneficios" de más de cinco cifras.
e) Ofrecen *posibilidades de tiempo y espacio*, ya que en milésimas de segundo y sin una necesaria presencia física pueden llegar a consumarse.
f) Son *muchos los casos y pocas las denuncias*, y todo ello debido a la misma falta de regulación por parte del Derecho.
g) Son *muy sofisticados* y relativamente frecuentes en el ámbito militar.

[15] TELLEZ VALDEZ, Julio, *"Derecho Informático"*, Universidad Nacional Autónoma de México 1991. págs. 82 – 83.

h) Presentan grandes *dificultades para su comprobación*, esto por su mismo carácter técnico.

i) En su mayoría *son imprudencias* y no necesariamente se cometen con intención.

j) Ofrecen *facilidades para su comisión* los menores de edad.

k) Tienden a proliferar cada vez más, por lo que requieren una urgente regulación.

l) Por el momento *siguen siendo ilícitos* impunes de manera manifiesta ante la ley.

3.3 Clasificación de los Delitos Informáticos

Muchas son las clasificaciones que se han dado sobre delitos informáticos, por lo que consideramos que el jurista mexicano Julio Téllez Valdez[16], clasifica a los delitos informáticos de acuerdo a dos criterios:

3.3.1 Como instrumento o medio

En esta categoría se encuentran las conductas criminales que se valen de las computadoras como método, medio o símbolo en la comisión del ilícito, por ejemplo:

a) Falsificación de documentos vía computarizada (tarjetas de crédito, cheques, etc.)

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

c) Planeamiento y simulación de delitos convencionales (robo, homicidio, fraude, etc.)

d) Lectura, sustracción o copiado de información confidencial.

e) Modificación de datos tanto en la entrada como en la salida.

f) Aprovechamiento indebido o violación de un código para penetrar a un sistema introduciendo instrucciones inapropiadas.

g) Variación en cuanto al destino de pequeñas cantidades de dinero hacia una cuenta bancaria apócrifa.

h) Uso no autorizado de programas de cómputo.

i) Introducción de Instrucciones que provocan “interrupciones” en la lógica interna de los programas.

j) Alteración en el funcionamiento de los sistemas, a través de los virus informáticos.

[16] TELLEZ VALDEZ, Julio, *“Derecho Informático”,* Universidad Nacional Autónoma de México 1991. pág..83

k) Obtención de información residual impresa en papel luego de la ejecución de trabajos.
l) Acceso a áreas informatizadas en forma no autorizada.
m) Intervención en las líneas de comunicación de datos o teleproceso.

3.3.2 Como fin u objetivo

En esta categoría, se enmarcan las conductas criminales que van dirigidas contra las computadoras, accesorios o programas como entidad física, como por ejemplo:

a) Programación de instrucciones que producen un bloqueo total al sistema.
b) Destrucción de programas por cualquier método.
c) Daño a la memoria.
d) Atentado físico contra la máquina o sus accesorios.
e) Sabotaje político o terrorismo en que se destruya o surja un apoderamiento de los centros neurálgicos computarizados.
f) Secuestro de soportes magnéticos entre los que figure información valiosa con fines de chantaje (pago de rescate, etc.)

Asimismo, a continuación indicaremos la clasificación efectuada por Uhlrich Seiber[17], quien los clasifica en las siguientes categorías:

a) Fraude por manipulación de un computador contra un sistema de procesamientos de datos;
b) Espionaje informático y robo de software;
c) Sabotaje informático;
d) Robo de servicios;
e) Acceso no autorizado a sistemas de procesamiento de datos; y
f) Ofensas tradicionales en los negocios asistidos por computador.

3.4 Caracterización del delincuente informático

Es importante precisar que en la práctica se comprueba como la *delincuencia informática* es realizada por personas vinculadas de algún modo a las empresas, es decir, por sujetos que tienen acceso a la unidad central de procesamiento de datos *–hackers-*. Puesto que dichas personas, por su, propio trabajo, llegan a conocer de manera completa el sistema informático, tienen mayor facilidad para burlar la seguridad implantada.[18]

[17] CORREA, Carlos y otros: *"Derecho Informático",* Ediciones de Depalma, Buenos Aires, 1987. pág. 296

[18] BRAMONT - ARIAS TORRES, Luis Alberto Ob. cit. pág. 23

.

Las principales características que presentan los sujetos activos de esta conducta delictiva son las siguientes:

a) En general, son personas que *no poseen antecedentes delictivos.*

b) La mayoría de sexo masculino.

c) Actúan en forma individual.

d) Poseen una *inteligencia brillante* y alta capacidad lógica, ávidas de vencer obstáculos; Actitud casi deportiva en vulnerar la seguridad de los sistemas, características que suelen ser comunes en aquellas personas que genéricamente se las difunde con la denominación “hackers”.

e) Son jóvenes con *gran solvencia en el manejo de la computadora*, con coraje, temeridad y una gran confianza en sí mismo.

f) También *hay técnicos no universitarios, autodidactas, competitivos*, con gran capacidad de concentración y perseverancia. No e trata de delincuentes profesionales típicos, y por eso, son socialmente aceptados.

g) En el caso de los *“hackers”*, realizan sus actividades como una especie de deporte de aventura donde el desafío está allí y hay que vencerlo. *Aprovechan la falta de rigor de las medidas de seguridad* para obtener acceso o poder descubrir deficiencias en las medidas vigentes de seguridad o en los procedimientos del sistema. A menudo, los piratas informáticos se hacen pasar por usuarios legítimos del sitio. Eso suele suceder con frecuencia en los sistemas en que los usuarios emplean contraseñas comunes o de mantenimiento que están en el propio sitio.

h) Dentro de las organizaciones, las personas que cometen fraude *han sido destacadas en su ámbito laboral* como muy trabajadoras, muy motivadas (es el que siempre está de guardia, el primero en llegar y el último en irse).

i) Con respecto a los que se dedican a estafar, nos encontramos ante especialistas. Algunos estudiosos de la materia lo han catalogado como *“delitos de cuello blanco”,* (se debe a que el sujeto activo que los comete es poseedor de cierto status socio-económico.)

El diario El Comercio, informó que en la actualidad los delincuentes informáticos[19] dejan el "phishing" y ahora corrompen sitios legítimos; asimismo, indicó que el envío de correos “spam” fue dejado de lado para atacar páginas web desde donde roban datos de miles de usuarios (Washington - Reuters). El número de virus cibernéticos crece rápidamente y

[19] Diario el Comercio 14 abril 2009 http://elcomercio.pe/noticia/272990/delincuentes-informaticos-dejan-phishing-y-ahora-corrompen-sitios-legitimos

ahora en lugar de transmitirse por correo electrónico están ocultos en sitios web aparentemente seguros, dijo el martes la compañía de seguridad en Internet Symantec Corp en un reporte. Se ha registrado en Internet un enorme incremento en la cantidad de virus y gusanos, también llamados "códigos maliciosos", y han trepado a 1,6 millones el año pasado contra los 624.267 identificados en el 2007, de acuerdo a Symantec. "El 60% de todas la amenazas (por códigos maliciosos) en los últimos 20 años se produjeron sólo en los últimos 12 meses", dijo Vincent Weafer, vicepresidente de contenidos de seguridad y datos de inteligencia de Symantec. Los atacantes se están alejando del uso de la técnica de envío de correo "spam" -conocida como "phishing"- para obtener información personal de los usuarios, y han pasado a dedicarse a corromper sitios web legítimos, por ejemplo de un negocio local, y usarlos para robar datos, indicó el reporte.

Asimismo, informó que existen sitios proclives que los atacantes tienden a permanecer lejos de grandes sitios web corporativos manejados por compañías que repararían pronto el sitio, dedicándose en cambio a sitios más pequeños no manejados por profesionales, como el de recintos que ofrecen alojamiento y desayuno ("bed and breakfast"). El reporte de Symantec citó otros ejemplos de páginas de internet infectadas, como sitios de la ONU y del Gobierno británico. "Los tipos malos están buscando sitios web legítimos y comprometiéndolos", explicó Weafer. El objetivo de los virus es robar, y la diseminación de la banda ancha en distintos continentes hace más fácil que existan áreas sin control que alberguen sin proponérselo a los piratas informáticos. "En el 2008, el 78% de las amenazas a la información confidencial exportó datos de los usuarios y 76% usó un componente de pulsación de teclas para robar información sobre cuentas bancarias on line", indicó el reporte.

Una vez que se han robado los números de tarjetas de crédito, nombres de usuario y contraseñas, se los vende en el mercado negro. "El artículo más popular para la venta en la economía subterránea en el 2008 fue la información de tarjetas de crédito, que representó el 32% del total", dijo el reporte. "El precio por cada tarjeta puede llegar a un mínimo de hasta 6 centavos cuando son compradas en un grupo", agregó. Los datos de cuentas bancarias fueron el segundo artículo más vendido, con un 19%, y por cada paquete de datos de un cliente se pagó entre 10 y 1.000 dólares. Los

nombres de usuarios y contraseñas de cuentas de correo electrónico estuvieron en el tercer puesto con el 5%, y se los vendió por entre 10 centavos y 100 dólares. “Si puedo controlar tu dominio (...) Puedo usarlo para conectarme y enviar “spam”. Puedo usarlo para hacerme pasar por ti u otra persona”, dijo Weafer. “Existe la posibilidad de que la información que usas para ingresar a tu correo sea la misma que usas para ingresar a tu cuenta de banco”, agregó. Weafer dijo que los usuarios ya no pueden confiar exclusivamente en el software de protección de seguridad, e instó a la cooperación internacional para enfrentar al crimen organizado que opera en ambientes sin control. “Mientras la banda ancha se extiende y vuelve más barata, eso mueve los virus”, señaló el experto. “Hay desafíos genuinos”, concluyó.

Del mismo, modo en un editorial del Diario El Comercio, manifestaron lo siguiente: “Resulta intolerable que los delitos informáticos sigan propagándose cual plaga bíblica, sin que los culpables rindan cuentas ante la justicia. Peor aun, las fechorías cada vez son más sofisticadas y temerarias, llegando al nivel de la burla. Como lo reveló El Comercio en su edición de ayer, han osado usurpar los emblemas de la Policía Nacional para, vía e-mail, infectar computadoras e invadir distintas bases de datos personales con el fin de robar información. En suma, no solo enfrentamos a los maliciosos hackers que penetran páginas web y difunden información falsa, como la inventada embolia de la esposa del jefe de Estado, sino que estamos ante un grupo de avezados delincuentes que conocen del manejo informático y de la manipulación en la red, por la cual despojan de toda reserva al usuario y comenten toda suerte de tropelías delincuenciales. Ante la grave dimensión del problema, y pese a la dificultad que implica identificar y sancionar a quienes operan a través de distintas cabinas de Internet, es imperativo que las fuerzas del orden, los fiscales y jueces estén a la altura de las circunstancias y presenten resultados concretos contra esta modalidad delictiva. En este caso, las leyes existen y están perfectamente vigentes pues hay todo un capítulo en el Código Penal dedicado a los delitos informáticos. El punto es empezar a capturar a estos bandidos y aplicar sanciones ejemplares y públicas. De lo contrario, la impunidad hará que la plaga continúe con todos los perjuicios que ello significa para los usuarios, su privacidad y su seguridad.”[20]

[20] Diario El Comercio 31 julio 2008. http://elcomercio.pe/edicionimpresa/html/2008-07-31/sanciones-ejemplares-delincuentes-informaticos.html

3.5 Los bienes jurídicos afectados por los delitos informáticos

Es importante resaltar que el estudio de los bienes jurídicos en los delitos de nueva data, son el punto de partida obligado para determinar los tipos penales en los llamados Delitos informáticos, debido a que determina el marco dentro del cual pueden realizarse; así "... el derecho positivo peruano es tajante a vincular el Derecho penal con la protección de bienes jurídicos. En efecto, el ordenamiento penal se concreta en proteger *"bienes vitales"*: vida, integridad corporal, libertad, salud, seguridad, patrimonio, etc. lo importante es que los bienes vitales sean indispensables para la convivencia humana en sociedad; por eso mismos deben ser protegidos por el poder coactivo del Estado a través de la pena pública". [21]

Con relación al bien jurídico, podemos afirma que es todo aquel que se encuentra protegido o amparado dentro de los diversos aspectos del derecho; asimismo, es empleado en el derecho penal para referirnos al interés tutelado frente a la comisión de los delitos, llamados como "bien jurídico protegido" o "bien jurídico tutelado", de igual forma podemos afirmar el bien jurídico protegido surge como consecuencia de los intentos por controlar el desmedido avance del derecho penal, debido a que no había forma como limitar las conductas necesarias para proteger a la sociedad como ultima ratio.

Finalmente podemos colegir que con relación a los bienes jurídicos protegidos en los delitos informáticos según los diversos autores que tienen posiciones encontradas quienes indican que "… no hay unanimidad en orden al contenido del *bien jurídico* en el delito informático. La mayoría de legislaciones establecen que estos delitos afectan al patrimonio, pero, de lege ferenda, también hay autores que afirman que el bien jurídico protegido es bien el orden económico, bien la intimidad de las personas".[22] Asimismo, podemos apreciar que los bienes jurídicos protegidos en los delitos informáticos afectan bienes jurídicos individuales y bienes jurídicos colectivos, y que "…el delito informático es un *delito pluriofensivo*; ya que lesiona más de un bien jurídico…". [23]

---

21 BRAMONT - ARIAS TORRES, Luis Alberto Ob. cit. pág. 51.

22 BLOSSIERS HUME, Juan José Ob. 2003. pág. 187.

23 PEÑA CABRERA, Raúl: "TRATADO DE DERECHO PENAL – ESTUDIO PROGRAMÁTICO DE LA PARTE ESPECIAL", Editora Jurídica Grijley. 3ra. Edición. Lima,1999. pág. 49.

3.5.1 El patrimonio como bien jurídico protegido

El patrimonio, en cuenta a su concepto no presenta un contenido claro capaz de resolver todos los problemas que plantean estos delitos; por esto se han mantenido diferentes posiciones que tratan de esclarecer su significado. Quienes sostienen que el patrimonio es el bien jurídico protegido en el delito informático tienen como fundamento básico el hecho que ofrece la realidad en la comisión de estas conductas, mediante las cuales, casi siempre se ocasiona un perjuicio *cuantificable económicamente.* Desde este punto de vista, se estaría afectando a un *bien jurídico individual* como, como es el patrimonio, con independencia de la cuantía del perjuicio y de la capacidad económica de la empresa afectada, que sería por lo tanto, el único sujeto pasivo afectado por la conducta.

Por otro lado, existen autores como Bramont Arias, quien señala que "... comprendemos que el hecho de que a través del uso de un sistema informático pueda afectarse el patrimonio, no significa que dicho comportamiento configure *per se* un delito informático ni que el patrimonio sea el bien jurídico en los delitos empleo de sistemas informáticos deberían ser comprendidos como nuevas modalidades de los delitos patrimoniales y no como delitos informáticos autónomos..." [24]

3.5.2 El orden económico bien jurídico protegido

Los autores reconocen el surgimiento y la importancia de una nueva rama jurídica que han denominado como Derecho Penal Económico, respecto a la cual, no obstante, no puede decirse que hay un concepto único -ante todo falta de precisión-, que sirva para, marcar los limites conceptuales de un objeto de estudio en sí reacio a una definición dogmática; incluso hay discrepancia en la denominación de la materia. Quienes mantienen esta tesis en el ámbito de la delincuencia informática han de partir del hecho que con estas conductas afectan, no ya el patrimonio particular de una empresa, sino en realidad, todo el orden económico establecido en una concreta sociedad, por lo que los perjudicados no serían solo la empresa, sino toda la colectividad imbuida en el mundo de las relaciones socioeconómicas. Estaríamos ante un bien jurídico de carácter macrosocial. [25]

---

[24] BRAMONT - ARIAS TORRES, Luis Alberto Ob. cit. págs. 51 - 54.

[25] BRAMONT - ARIAS TORRES. Ob. cit. págs. 55 - 56.

En tal sentido podemos colegimos cuando se afirma que "... en el complicado proceso de hoy en día, se mueven numerosos bienes jurídicos intermedios mediatizados entre los intereses del Estado y los intereses del agente económico individual, así como de los consumidores. Así, el interés supraindividual en el funcionamiento del tráfico de crédito y del comercio de capitales, tiene en el ordenamiento económico actual, un lugar legítimo, reconocido por el derecho económico desde hace mucho tiempo." [26]

3.5.3 La intimidad como bien jurídico protegido

El derecho a la intimidad está reconocido constitucionalmente como un derecho fundamental de la persona en el artículo 2, numeral 7 de la Constitución Política de 1993. Al respecto, no puede olvidarse como en la actualidad se tiene a la concentración relativa a todos los aspectos posibles de la persona, cuyo acceso es restringido a un grupo reducido, en el cual, mediante la manipulación de la información informática de tales datos puede llegar a tener un excesivo control sobre el individuo. La frase conocida de que la información es poder, ha llevado a varios Estados a la creación de organismos especiales encargados del control del empleo correcto de toda información que el Estado pueda tener almacenada respecto a la intimidad de la persona[27].

De igual forma podemos afirmar que el derecho a la intimidad es un derecho fundamental, inherente a la persona, secundado por la prohibición del suministro de información personal que afectan la intimidad personal y familiar, por ello es necesario el otorgamiento de un marco jurídico en el ámbito de la ley a fin de posibilitar una efectiva protección del derecho a la intimidad considerando los avances en materia informática.

En tal sentido, podemos apreciar que la norma constitucional ha establecido con proyección un marco conceptual donde se pueden reglamentar a través de leyes, políticas de protección a la intimidad frente al avance tecnológico sin embargo el Estado debe establecer políticas a fin de salvaguardar la información de tipo personal de acceso público que forma alguna pudiera perjudicar a la intimidad del ciudadano. Es decir una adecuada regulación de protección de datos personales.

---

[26] TIEDEMAN, Klaus: "Derecho Penal y Nuevas Formas de Criminalidad", Editorial IDEMSA, Lima, 2000. pág. 22.

[27] BRAMONT - ARIAS TORRES, Luis Alberto Ob. cit. pág. 57.

Finalmente en relación a la intimidad como bien jurídico protegido nos aunamos a la afirmación vertida por los juristas Bramont - Arias Torres, Luis Alberto y García Cantizano, María del Carmen, quienes señalan que "... con el desarrollo de la sociedad, el legislador se ha visto obligado a proteger penalmente la intimidad de las personas, teniendo en cuenta sobre todo el avance tecnológico alcanzado. Con esta rubrica se está protegiendo la intimidad de las personas y la intimidad familiar; se trata de la protección de hechos o actividades propias o destinadas a la persona o a un círculo de personas..." [28]

3.5.4 La libertad informática como bien jurídico protegido

Con relación a la libertad informática la cual ha sido llamada por la doctrina española como "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 banco de datos, lo que se denomina habeas data por su función análoga en el ámbito de la libertad de la información y cuanto supuso el tradicional habeas corpus en lo referente a la libertad personal, controlar su calidad, lo que implica la posibilidad de corregir o cancelar los datos inexactos o indebidamente procesados y disponer sobre su transmisión." Asimismo, otros autores con relación a la libertada informática afirman que en "... en conclusión la libertad informática se erige como 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 esta información, derechos comprendidos en lo denominados derechos de "Tercera Generación". Se trata de un bien jurídico de naturaleza individual y personal." [29]

Cabe resaltar que las tendencias actuales con relación a la libertad informática otros autores consideran "… que la autodeterminación informativa deberá subordinarse al derecho a controlar la información personal, consistente en la facultad de toda persona a controlar la utilización de su información personal por parte de terceros (públicos o privados) a través de medios informáticos, para que dicho control permita al titular de los datos el determinar dicha información personal conforme a los derechos y legítimos intereses que enfrente a la misma, llegando, eventualmente, a poder exigir su supresión. [30]

---

28 BRAMONT - ARIAS TORRES, Luis Alberto Ob. cit. pág. 196.

29 BLOSSIERS HUME, Juan José Ob. cit. pág. 198 - 200.

30 *"El derecho a controlar la información personal"*. Esteban RUÍZ MARTÍNEZ. Revista Electrónica de Derecho Informático. Nro. 49 Agosto 2002

3.5.5 El honor como bien jurídico protegido

Con relación al derecho al honor como bien jurídico protegido podemos afirmar que "… el derecho al honor, jurídicamente constituye 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 demás méritos y cualidades que han ido adquiriendo como fruto de su desarrollo personal y social. El honor como objeto de protección penal ha sido concebido desde muy diversas perspectivas, sin embargo, para una concepción estrictamente jurídica, dignidad de la persona, sujeto de derecho, constituye la esencia misma del honor y determina su contenido. Debemos precisar, que al igual que otros bienes jurídicos tutelados por el Derecho Penal, el derecho al honor puede verse conculcado ya sea por algún envío masivo de determinado grupo de personas de mensajes difamatorios, como publicaciones en páginas web con información que atente contra el honor de una determinada persona." [31]

Asimismo, "... está admitido por la mayoría de la doctrina que el bien jurídico protegido en este grupo de delitos es el honor. En principio "... el *honor subjetivo* puede entenderse como la auto evaluación del sujeto, es decir, el juicio que tiene toda persona de si mismo en cuanto sujeto de relaciones sociales. El *honor objetivo* es la valoración que otros hacen de la personalidad ético – social de un sujeto. Coincidirá con la reputación de la que disfruta cada persona frente a los demás sujetos que conforman una comunidad social." [32]

3.5.6 La Información como bien jurídico protegido

Con relación a la información como bien jurídico, autores como Luis Miguel Reyna Alfaro[33], indica que hoy en día no resulta suficiente poseer la información, es necesario además tener la capacidad de almacenarla, tratarla y trasmitirla eficientemente, de allí que "la información" debe ser entendida como un proceso en el cual se englobe los tres supuestos (almacenamiento, tratamiento y transmisión).

El almacenamiento, tratamiento y transmisión de datos mediante los sistemas de procesamiento e interconexión conceden el novísimo significado al término "información", colocando a su poseedor en privilegiada situación de ventaja

31 BLOSSIERS HUME, Juan José Ob. cit. pág. 194 - 195.

32 BRAMONT - ARIAS TORRES, Luis Alberto y GARCIA CANTIZANO, María del Carmen, *"Manual de Derecho Penal Parte Especial",* Editorial San Marcos – Cuarta Edición. Lima , 1998. pág. 135.

33 REYNA ALFARO, Luis Miguel, (2002) pág. 237 – 239.

respecto al resto de individuos. Así podemos decir que el interés digno de tutela penal sería la "información" (almacenamiento, tratada y transmitida a través de sistemas informáticos), como valor económico de la actividad de la empresa. Ahora bien, habrá que determinar si estamos ante un bien jurídico penal individual o si más bien el interés tutelado es de carácter colectivo. Si tenemos en consideración que estamos ante un interés social vinculado a la actividad empresarial, todas veces que la información se convierte en un valioso instrumento de la actividad de empresa, el bien jurídico "información" se encontraría encaminado dentro de los llamados delitos socioeconómicos y por ello sus repercusiones trascenderían a las propias bases del sistema socioeconómico, esto es, está a través del bien jurídico colectivo.

Sin embargo, ello no obstante que puedan resaltar implicados, en determinados supuestos, intereses patrimoniales individuales, con lo cual surge el inconveniente adicional de diferenciar entre delitos patrimoniales y los referidos al orden socioeconómico, para ello debemos dejar en claro que el bien jurídico propuesto está dirigido a resguardar interese colectivos, cercanamente relacionados al orden público económico, aunque puedan concurrir a su vez intereses individuales, que en éste específico caso serían los de los titulares de la información contenido en los sistemas de tratamiento autónomo de datos.

Finalmente autores como Juan José Blossiers Hume, refiere en relación a la informática como bien jurídico protegido que "... el derecho a la autodeterminación informativa o libertad informática se encuentra inefablemente vinculado al concepto de intimidad, ya que se trata de ofrecer al individuo la seguridad de sus datos de carácter personal ante el factible vinculado al concepto de intimidad, ya que se trata de ofrecer al individuo la seguridad de datos de carácter personal ante el factible uso mediante la informática u otro sistema automatizado; no obstante, es necesario que los datos utilizados sean íntimos o permanezcan al núcleo esencial de la personalidad del individuo, sino, simplemente, que sean datos que puedan revelar sus hábitos y comportamientos. Así, el individuo tendría el derecho a decidir que información personal se podrá difundir y el destino sobre esta información dentro de la informática." [34]

[34] BLOSSIERS HUME, Juan José Ob. cit. pág. 194 - 195.

3.6 El Derecho Penal y los problemas actuales de la Política Criminal[35]

El jurista José Hurtado Pozo[36], con relación a la terminología del Derecho Penal que: "Desde los inicios del siglo XIX, se le denomina, de manera predominante, a la materia que estudiamos, derecho penal. Mucho tiempo, fue designada con la expresión de derecho criminal. Ambas expresiones no son del todo satisfactorias, en la medida en que sólo ponen en evidencia uno de los aspectos fundamentales de la materia. La primera, se refiere a la pena (*poena*, comprendida en sus orígenes en el sentido religioso de expiación). La segunda, alude al crimen, comportamiento generador de la reacción social, la misma que se ha diversificado progresivamente. Actualmente, se prefiere hablar de derecho penal aun cuando no refleja plenamente el contenido que se le da. Junto a la infracción (crimen, delito o contravención) y a la sanción (penas privativas de libertad, multa, trabajo comunitario, medidas de seguridad), es considerar, de manera destacada, tanto al delincuente como a la víctima. Esta última ha sido descuidada mucho tiempo en las reflexiones sobre los diversos aspectos de la reacción punitiva del Estado".

Según el jurista alemán Claus ROXIN[37] refiere que: "La criminalidad es un problema de todas las sociedades. Ello explica la internacionalización de la ciencia penal. Sin embargo, pese a la larga experiencia con ese fenómeno, en ninguna parte se ha conseguido llegar a eliminar a la criminalidad y ni siquiera alcanzar su marginación; tampoco existe acuerdo sobre el camino razonable para reducirla. Las tendencias de la política criminal cambian como la moda. Por una parte existe en un primer plano el esfuerzo por la reintegración social del autor; por otra, se busca hacer frente a la criminalidad mediante la firmeza y la disuasión. De momento se extiende esta segunda tendencia —que parte de Norteamérica—, la cual se erige en todo el mundo como un medio para dar popularidad a los políticos, pues partiendo de un conocimiento profano resulta creíble que el endurecimiento de las penas disminuye la criminalidad.

---

35 Conferencia traducida de la versión alemana "Aktuelle Probleme der Kriminalpolitik" por Enrique Díaz Aranda, dictada el 4 de septiembre de 2000, en el ciclo "Puntos de discusión de vanguardia en las ciencias penales" , en el auditorio " Jaime Torres Bodet" del Museo Nacional de Antropología e Historia, Organizado por la PGR y el INACIPE. ** Catedrático de derecho penal de la Universidad de Munich (LMU).

36 HURTADO POZO José "NOCIONES BASICAS DE DERECHO PENAL DE GUATEMALA", pág. 1.

37 CLAUS ROXIN Y OTROS "PROBLEMAS FUNDAMENTALES DE POLITICA CRIMINAL Y DERECHO PENAL", Editorial de la Universidad Autónoma de México, 2002 pág. 87 y 88.

Por consiguiente, con semejante política se pueden ganar votos y al mismo tiempo demostrar firmeza. También en Alemania, donde la pena privativa de la libertad ha retrocedido ampliamente —sólo el cinco por ciento de todas las penas se cumplen como pena privativa de libertad— resuena la llamada hacia la construcción de nuevas prisiones; contra eso, una medida afable de resocialización, como es la remuneración del trabajo en prisión, sólo puede conseguirse paso a paso por nuestro tribunal constitucional en contra de la tenaz resistencia de los políticos.

Desde mi punto de vista, las penas rigurosas —sobre todo las privativas de libertad— son en verdad imprescindibles para los delitos capitales; pero no son un medio de reacción adecuado en contra de la criminalidad pequeña y mediana, la cual es numéricamente preponderante…."; asimismo, ROXIN explica sus ideas en forma de tesis y son las siguientes:

Primera tesis: las penas no son de ninguna manera un medio adecuado para luchar contra la criminalidad.

Segunda tesis: las penas privativas de libertad son además un medio particularmente problemático en la lucha contra la criminalidad.

Tercera tesis: la prevención es más efectiva que la pena.

Cuarta tesis: el sistema de reacción penal se debe ampliar y, sobre todo, complementarlo con sanciones penales similares de carácter social constructivo.

Finalmente, es importante precisar que según la problemática de la estigmatización del delincuente ante el derecho penal, según Miguel Reyna Alfaro, señala que es evidente que la sociedad, a través de sus diversas instituciones, ha internalizado en sus miembros una concepción bastante parcializada del delincuente así como de las características que éste posee, es así que tanto la Criminología como el Derecho Penal orientaron sus discusiones y debates hacia este "estereotipo de delincuente" y a las conductas que podían ejecutarse por su parte. De esta manera queda establecido un prototipo, el mismo que resulta íntimamente asociado a las características sociales de la persona ya su nivel cultural-económico, según dicho prototipo el delincuente será, como indican Feest/Blankenburg "aquel que fundamentalmente pertenezca a las clases bajas, dejando en claro la amplia brecha marcada en función a la realidad social del individuo[38].

[38] REYNA ALFARO, Luis Miguel, (2002) pág. 143 –144.

3.7 Marco Jurídico coadyuvante del Marco Teórico expresados en el Código Penal

La necesidad de tipificar y sancionar a los delincuentes de los denominados *"Delitos Informáticos"*, ha sido la preocupación de los investigadores en los últimos años, cabe resaltar que estos delitos de nueva data se iniciaron con la aparición de las computadoras, Internet y el avance de la tecnología. Es tal la trascendencia de estos delitos que se hacen presente en nuestra legislación penal al adicionar a nuestro Código Penal de 1991 mediante Ley Nº 27309, publicada en el Diario Oficial "El Peruano", de fecha 17 de junio del 2000, se incorpora al Título V del Libro Segundo del Código Penal vigente, el Capítulo X, "Delitos Informáticos", el artículo 207°-A "Acceso indebido de sistemas de información", el artículo 207°-B "Sabotaje Informático" y el artículo 207°-C "Agravantes", lo que surge evidentemente como un intento de poner hacer frente a los delitos informáticos, poniendo a la vanguardia nuestra legislación con relación a los avances tecnológicos.

En suma, se le plantea al Derecho peruano grandes desafíos, frente a los que sólo resta una radical, urgente y tenaz decisión: Innovar un nuevo Derecho, un Derecho que aprenda de los errores del pasado y mire hacia delante; un Derecho que vea fortificados sus máximos valores: la justicia y la seguridad. Asimismo, se hace imprescindible un Derecho que responda satisfactoriamente a las demandas de la nueva Sociedad de la Información, es decir, un Derecho que se adapte a la realidad, un Derecho actual, para de este modo cumplir a cabalidad con su rol regulador. [39]

Al respecto es importante acotar lo señalado por Luis Reyna Alfaro, al precisar que si bien el patrimonio resulta ser el valor genéricamente titulado, el interés social respaldado de manera específica parece ser "la información contenidas en los sistemas de tratamiento automatizado de datos", siendo esto así parece innegable que se otorgue a la "información" (almacenada, tratada y trasmitida a través de medios informáticos) un valor económico, con lo que la regulación lege lata guardaría cercana relación con la concepción del suscrito sobre el valor social digno de tutela, sin embargo, existen diferentes saltantes en la ubicación del bien jurídico penal, lo que tiene a su vez importantes consecuencias prácticas. Según entiende, la información como valor económico de la empresa, debería ser regulada en un título autónomo,

[39] *"El Derecho Peruano Frente a los Desafíos del Nuevo Milenio: Conciliación, Tecnología e Innovación"*, Revista Electrónica de Derecho Informático César Antonio MAITA AZPIRI, Abril 2001.

que dejaría en evidencia la especial naturaleza del bien jurídico penal tutelado y permitiría remarcar su carácter supraindividual, lo que no es posible hacer a partir de la concepción patrimonial acogida en nuestro texto penal[40].

3.7.1 Espionaje Informático

Con relación a este delito el cual fue adicionado a nuestro código penal vigente mediante el **artículo 207º-A** dispone lo siguiente:

"*El que utiliza o ingresa indebidamente a una base de datos, sistema o red de computadoras o cualquier parte de la misma, para diseñar, ejecutar o alterar un esquema u otro similar, o para interferir, interceptar, acceder o copiar información en tránsito o contenida en una base de datos, será reprimido con pena privativa de libertad no mayor de dos años o con prestación de servicios comunitarios de cincuenta y dos a ciento cuatro jornadas. Si el agente actuó con el fin de obtener un beneficio económico, será reprimido con pena privativa de libertad no mayor de tres años o con prestación de servicios comunitarios no menor de ciento cuatro jornadas.*"

Sujetos que intervienen en el delito de Espionaje Informático:

Sujeto Activo, la descripción típica del presente delito nos permite considerar como sujeto activo a cualquier persona natural que utilice o ingrese indebidamente a una base de datos, sistema o red de computadoras o cualquier parte de la misma, para diseñar, ejecutar o alterar un esquema u otro similar, o para interferir, interceptar, acceder o copiar información en tránsito o contenida en una base de datos; es importante precisar, si bien es cierto que en este delito el bien jurídico es el patrimonio por encontrarse dentro de los delitos contra el patrimonio, podemos apreciar que el bien jurídico protegido también es la información que tiene cualquier persona dentro de una computadora, cuando se indica: ***" … o copiar información en tránsito o contenida en una base de datos…."***

Sujeto Pasivo, en el presente caso es considerado a toda persona natural o jurídica titular de la información afectada.

3.7.2 Sabotaje Informático

Con relación a este delito el cual fue adicionado a nuestro código penal vigente mediante el **artículo 207º-B** dispone lo siguiente:

"*El que utiliza, ingresa o interfiere indebidamente una base de datos, sistema, red o programa de computadoras o cualquier parte de la misma con el fin de alterarlos, dañarlos o destruirlos, será reprimido con pena privativa de libertad no menor de tres ni mayor de cinco años y con setenta a noventa días multa.*"

Sujetos que intervienen en el delito de Sabotaje Informático:

Sujeto Activo, la descripción típica del presente delito nos permite considerar como sujeto activo a cualquier persona natural que utiliza, ingresa o interfiere

[40] REYNA ALFARO, Luis Miguel, (2002) pág. 257

indebidamente una base de datos, sistema, red o programa de computadoras o cualquier parte de la misma con el fin de alterarlos, dañarlos o destruirlos, pudiendo afectar tanto el software o hardware de una computadora, así como la información contenida en las computadoras.

Sujeto Pasivo, en el presente caso es considerado a toda persona natural o jurídica titular o propietaria del hardware o software de las computadoras, así como la base de datos, sistemas, red, programa, ordenador ó información.

3.7.3 Modalidad Agravada

Con relación a este delito el cual fue adicionado a nuestro código penal vigente mediante el **artículo 207º-C** dispone lo siguiente:

"*En los casos de los Artículos 207º-A y 207º-B, la pena será privativa de libertad no menor de cinco ni mayor de siete años, cuando:*

1. *El agente accede a una base de datos, sistema o red de computadora, haciendo uso de información privilegiada, obtenida en función a su cargo.*
2. *El agente pone en peligro la seguridad nacional."*

Sujetos que intervienen en la modalidad agravada de los delitos de Espionaje y Sabotaje Informático:

Sujeto Activo, la descripción típica del presente artículo, trata sobre la modalidad agravada de los delitos de espionaje y sabotaje informático, permitiéndonos considerar como sujeto activo a cualquier persona natural que tenga una vinculación con una base de datos, sistema o red de computadora haciendo uso el delincuente informático de información privilegiada, obtenida en función a su cargo; asimismo, según lo indicado en el segundo numeral el sujeto activo puede ser cualquier persona natural.

Sujeto Pasivo, en el presente caso de igual forma es considerado a toda persona natural o jurídica titular o propietaria del hardware o software de las computadoras, así como la base de datos, sistemas, red, programa, ordenador ó información.

Con relación a esta nueva forma de criminalidad es importante señalar que el desarrollo tan amplio de las tecnologías informáticas ofrece un aspecto negativo, originando conductas antisociales y delictivas que se manifiestan de formas que hasta ahora no era posible imaginar. Los sistemas de computadoras ofrecen oportunidades nuevas y sumamente complicadas de infringir la ley, y han creado la posibilidad de cometer delitos de tipo tradicional en formas no tradicionales.

Asimismo, hemos podido apreciar que en los últimos tiempos, ha sido evidente que la sociedad ha utilizado de manera benéfica los avances derivados de la tecnología en diversas actividades; sin embargo, es necesario que se atiendan y regulen las cada vez más frecuentes consecuencias del uso indebido de las computadoras y los sistemas informáticos en general, de igual forma es importante mencionar que en los casos de delitos cometidos por medios informáticos los cuales afectan a nuestra sociedad en general, perjudicando en especial a los menores de edad quienes son los más vulnerables y susceptible de ser afectados en su intimidad, pudor, estafados, extorsionados y chantajeados entre otras formas delictivas que pueden afectar a los menores.

Con relación a los delitos informáticos en nuestro Código Penal vigente, es importante precisar que la inclusión de estos delitos dentro de los delitos contra el patrimonio, a nuestro parecer ha sido poco acertada, debido a que se puede colegir que todos los delitos informáticos serían solo contra el patrimonio; asimismo, debemos tener en cuenta, si bien es cierto que esta inclusión es poco acertada, es un inicio por parte de los legisladores con la finalidad de hacer frente a esta nueva forma de criminalidad, siendo éste el punto de inicio para hacer frente a estos delitos que se vienen incrementando según avanza la ciencia y la tecnología en esta sociedad globalizada.

Respecto a los llamados delitos informáticos no son cometidos por la computadora, sino que es el hombre quien los comete con ayuda de aquella; en ese entendido, podemos afirmar que la mayoría de los tipos penales en nuestro Código Penal vigente pueden susceptibles a ser realizados por medios informáticos, motivo por el cual se puede apreciar que no existe un delito informático como tal, lo que si existe es la comisión de los tipos penales ya previstos en nuestro Código Penal por nuevas formas o métodos llamados criminalidad informática.

Finalmente, hemos podido apreciar durante la realización del presente trabajo de investigación respecto a los delitos informáticos previstos en los artículos 207 “A”, 207 “B” y 207 “C” de nuestro Código Penal vigente, son escasos los procesos judiciales en mérito a los artículos antes mencionados, por lo que dichos artículos serían letra muerta al no cumplir con el fina con que fueron promulgados.

3.8 Delitos que admiten la utilización de medios informáticos en el Código Penal Peruano

A continuación trataremos con relación a los delitos que admiten la utilización de medios informáticos en nuestro Código Penal vigente; asimismo, podemos afirmar que la mayoría de los delitos tipificados en nuestro código penal, son susceptibles de ser realizados a través de medios informáticos por lo que colegimos con la afirmación de Luis Reyna Alfaro, cuando refiere que prácticamente todos los delitos tipificados en nuestro ordenamiento sustantivo pueden ser cometidos por medios informáticos, sin embargo, cabe reafirmarnos en el hecho que para considerar un delito dentro los crímenes mediante computadoras, éste deberá ser cometido utilizando medios informáticos en su propia función, todos los componentes que no cumplan con dicho requisito deberán ser excluidos de dicha calificación[41].

3.8.1 Delitos Contra la Vida el Cuerpo y la Salud

De los tipos penales previstos en el presente Título denominado, “De contra la vida el cuerpo u la salud”, se encuentran el capítulo titulado “Lesiones”, se encuentra el **artículo 121º** el cual dispone lo siguiente: ***“El que causa a otro daño grave en el cuerpo o en la salud, será reprimido con pena privativa de libertad no menor de tres ni mayor de ocho años”.***

Los medios informáticos aunque parezca poco probable, pueden ser aplicados para la ejecución de actos destinados a lesionar la vida, el cuerpo y la salud de las personas. En este orden de ideas resulta perfectamente posible quien ingresa al sistema de información de una clínica de un hospital cambiar los datos contenidos en las hojas médicas de los pacientes de dicho centro médico y provocar que los actores médicos ejecuten diagnósticos que no se encuentren acordes con el real estado de salud de los pacientes y en consecuencia provoquen daños en la salud o peor aún su muerte, con lo que se configurarían los delitos de lesiones y homicidio, ya sea a título de dolo como culpa. En la casuística extranjera se ha demostrado lo perjudicial que pueden llegar a ser este tipo de conductas, en los Estados Unidos por ejemplo, un intruso ingresó a los archivos de un hospital y prescribió a un niño de nueve años que sufría de meningitis, drogas de carácter letal para su enfermedad, el menor salvó gracias a la intervención de la enfermera que se percató de la nocividad de dicho medicamento o piénsese por ejemplo la

[41] REYNA ALFARO, Luis Miguel, (2002) págs. 167

prescripción de antibióticos innecesarias a una persona mayor de sesenta años o incluso, lo que reviste mayor gravedad, conseguir tratamientos médicos que produzcan la muerte de los pacientes a fin de favorecer a la competencia o el caso de una adolescente que utilizó la computadora de su madre, quien trabajaba en un hospital, llamó a siete pacientes que se encontraban en la sala de cuidados intensivos de dicho centro médico para decirles que habían salido positivo en la prueba de VIH, esto es que eran portadores del virus del SIDA. [42]

En tal sentido podemos afirmar que: "... la vida humana es el bien jurídico principal en nuestra sociedad, al que toda persona tiene derecho; de esta forma es proclamado por nuestra Constitución en el inciso 1 del artículo 2. La vida se protege de modo absoluto, aunque según nuestra Constitución existen excepciones a la regla general: así el artículo 140 de la Constitución donde se prevé la pena de muerte para los delitos de traición a la patria en caso de guerra..." [43]

3.8.2 Delitos Contra el Honor

De los tipos penales previstos en el presente título, "De los Delitos Contra el Honor", se encuentran la injuria, la calumnia y la difamación, en los siguientes artículos:

"Artículo 130º.- "Injuria"; *El que ofende o ultraja a una persona con palabras, gestos o vías de hecho, será reprimido con prestación de servicio comunitario de diez a cuarenta jornadas o con sesenta a noventa días-multa".*

"Artículo 131º.- "Calumnia"; *El que atribuye falsamente a otro un delito, será reprimido con noventa a ciento veinte días-multa".*

"Artículo 132º.- "Difamación"; *El que, ante varias personas, reunidas o separadas, pero de manera que pueda difundirse la noticia, atribuye a una persona, un hecho, una cualidad o una conducta que pueda perjudicar su honor o reputación, será reprimido con pena privativa de libertad no mayor de dos años y con treinta a ciento veinte días-multa. Si el delito se comete por medio del libro, la prensa* ***u otro medio de comunicación social****, la pena será privativa de libertad no menor de uno ni mayor de tres años y de ciento veinte a trescientos sesenta y cinco días-multa".*

De los artículos antes mencionados se desprende la posibilidad de catalogar a la informática como medio idóneo para su comisión en las distintas formas de autoría. Incluso, el avance logrado en esta disciplina, el amplio alcance

[42] REYNA ALFARO, Luis Miguel, (2002) págs. 167 - 169

[43] BRAMONT - ARIAS TORRES, Luis Alberto y GARCIA CANTIZANO, María del Carmen, Ob. cit. pág. 35.

que viene teniendo los sistemas de interconexión, las redes de información, permiten que se le equipare a medio de comunicación social, lo que en atención a nuestro ordenamiento penal sustantivo constituye figura agravada del delito de Difamación, si entendemos como medio de comunicación social a las diversas instituciones informativas como la prensa, la radio, la televisión, el cine, la revistas, así como a través de las diversas páginas web, etc.

Por lo antes expuesto, concurrimos con la concepción de Luis Reyna Alfaro, quien afirma que: "... nuestra concepción se refuerza si tenemos en cuenta que la mayoría de medios de comunicación social tradicionales poseen paginas web en Internet en donde se contiene a la información que propalan, de todo lo cual es simple deducir que las redes en que estas paginas se ubican constituyen también medios de comunicación social no convencionales al reunir la exigencias correspondencia con el grupo social, más aún si antedichotas características del Internet tenemos que es posible establecer vínculos o contactos de carácter sonoro y visual con personas ubicadas en lugares geográficamente alejados en cuestión de segundos con un alcance masivo asombroso. En cuanto a la jurisprudencia en nuestro país se marco un precedente con la conocida querella interpuesta por un grupo de periodistas, contra el ciudadano argentino Héctor Ricardo FAISAL, a quien se le imputo el delito de Difamación Agravada por medio de prensa, pues a través de la pagina web de la "Asociación Pro Defensa de la Verdad" (APROVED) difundía contenidos lesivos contra el honor de los querellantes. Sin ingresar a analizar en el fondo del asunto, en dicho proceso en ningún momento se negó el carácter del medio de comunicación social de Internet. Asimismo, en la jurisprudencia extranjera, la Corte Suprema de los Estados Unidos en la conocida cauda RENO v. ACLU reconoce a la Internet con el "unique an wholly new médium of worlwide human comunication" ("el único y absoluto nuevo medio de comunicación humana.") [44]

3.8.3 Delito de Violación de la Intimidad

Del los tipos penales previstos en el presente capítulo titulado, **"Violación de la intimidad"**, se encuentra tipificado en ***artículo 154º*** *dispone los siguiente:* ***"****El que viola la intimidad de la vida personal o familiar ya sea observando, escuchando o registrando un hecho, palabra, escrito o imagen,* ***valiéndose de instrumentos, procesos técnicos u otros medios,*** *será reprimido con pena privativa de libertad no mayor de dos años. La pena será no menor de uno ni mayor*

[44] REYNA ALFARO, Luis Miguel, (2002) pág. 170 – 172

de tres años y de treinta a ciento veinte días-multa, cuando el agente revela la intimidad conocida de la manera antes prevista. Si utiliza ***algún medio de comunicación social****, la pena privativa de libertad será no menor de dos ni mayor de cuatro años y de sesenta a ciento ochenta días-multa".*

Consideramos factible la utilización y empleo del Hardware y el Software para la comisión de este delito, pues se encuentra como medio idóneo, al hacer mención expresa de ***"medios técnicos u otros medios"*** para la configuración de la conducta allí descrita. Por otra parte, si tal conducta hubiese sido realizada a través del empleo de Redes de Interconexión (como Internet), estaríamos frente a la figura agravada pues tal como hemos señalado, dichas Redes son perfectamente equiparables a ***"algún medio de comunicación social".***

De igual forma el **artículo 157º** dispone que**:** "El que, indebidamente, organiza, proporciona o emplea ***cualquier archivo que tenga datos*** referentes a las convicciones políticas o religiosas y otros aspectos de la vida íntima de una o más personas, será reprimido con pena privativa de libertad no menor de uno ni mayor de cuatro años".

Otra figura comprendida dentro de los llamados delitos contra la intimidad es ***la organización indebida de archivos de datos de la vida intima,*** contenida en este artículo, este supuesto, comportamiento consiste en organizar, proporcionar o emplear archivos que contengan datos referentes a las convicciones políticas, religiosas o de otros aspectos de la vida intima de la víctima, como es lógico, se comprenden aquí las bases de datos.

De igual forma, podemos afirmar que "... con el desarrollo de la sociedad, el legislador se ha visto obligado a proteger penalmente la intimidad de la personas, teniendo en cuenta sobre todo el avance tecnológico alcanzado. Con esta rúbrica se está protegiendo la intimidad de las personas y la intimidad familiar; se trata de la protección de hechos o actividades propias o destinadas a la persona o a un círculo reducido de personas, bien jurídico protegido reconocido también en el artículo 2, inciso 7 de la Constitución."[45] Finalmente Juan Francisco Arana Chalco, en su publicación a través del Internet "El Derecho a la Intimidad y el Avance de la Informática", precisa que: "…además de modificar el concepto de intimidad con el paso del tiempo

[45] BRAMONT - ARIAS TORRES, Luis Alberto y GARCIA CANTIZANO, María del Carmen Ob. cit.. pág. 196.

existe una colisión con el denominado derecho a la información, de establecer el limite entre ambos derechos y señalar que el derecho a la intimidad es absoluto sería utópico, sin embargo la intimidad, el bienestar físico, la parte emocional y la espiritual conforman un todo, siendo de necesidad su protección".[46] 47

3.8.4 Delito de Violación del Secretos de las Comunicaciones

Del los tipos penales previstos en el presente capítulo titulado, "Violación de del secreto de las comunicaciones, se encuentra tipificado en **artículo 161º** el cual trata sobre la **violación de correspondencia**, dispone que: *"El que abre, indebidamente, una carta, un pliego, telegrama, radiograma, despacho telefónico u* ***otro documento de naturaleza análoga****, que no le esté dirigido, o se apodera indebidamente de alguno de estos documentos, aunque no esté cerrado, será reprimido con pena privativa de libertad no mayor de dos años y con sesenta a noventa días-multa".*

En principio este artículo exige que la conducta recaiga sobre "**una carta, *un pliego, telegrama, radiograma, despacho telefónico u otro documento de naturaleza análoga***. Así las cosas, habrá que descifrar a que se refiere el legislador al mencionar a dichas formas de comunicación. Sin embargo, el propio artículo 161 del Código sustantivo prevé una salida al incluir los documentos de **"naturaleza análoga"**, en donde se puede comprender el correo electrónico, sin necesidad de recurrir a una interpretación peligrosamente extensivo del concepto de "carta", por esto podemos afirmar que la correspondencia digital, ya ha sido protegido por nuestro ordenamiento jurídico penal.[48] Finalmente, cuando se trata con relación al acceso del empleador al correo electrónico de sus subordinados Luis Reyna Alfaro refiere que tiene efectos más lesivos que otras formas de intrusión laboral y cita a Sundstrom quien subraya los siguiente: "porque el monitoreo de e-mail no requiere la presencia física del supervisor y puede ser realizado de manera completamente subrepticia en cualquier lugar y en cualquier momento en los trabajadores usen sus redes de computadoras"[49]

---

46 *"El Derecho a la Intimidad y el Avance de la Informática",* Juan Francisco ARANA CHALCO. Revista Electrónica de Derecho Informático "ALFA REDI".

48 REYNA ALFARO, Luis Miguel, (2002) pág. 175 – 176

49 REYNA ALFARO, Luis Miguel, (2002) pág. 180

3.8.5 Delito de Ofensas al Pudor Público

Del los tipos penales previstos en el presente capítulo titulado, "Ofensas contra el pudor, se encuentra tipificado en **artículo 183º** el cual trata sobre las **exhibiciones y publicaciones obscenas**, el cual dispone lo siguiente: ***"****Será reprimido con pena privativa de libertad no mayor de dos años:*

1. El que expone, vende o entrega a un menor de catorce años ***objetos, libros, escritos, imágenes visuales o auditivas que, por su carácter obsceno, pueden afectar gravemente el pudor del agraviado*** *o excitar prematuramente o pervertir su instinto sexual.*

3. El que incita a un menor de catorce años a la ebriedad o ***a la práctica de un acto obsceno*** *o le facilita la entrada a los prostíbulos u otros lugares de corrupción".*

Respecto a estas conductas, es posible considerar a las redes de interconexión o también conocido como Internet, vienen a ser el medio comisivo en los actos descritos en los incisos primero y tercero de dicho artículo. En tal sentido es importante mencionar lo señalado por Luis Reyna Alfaro cuando refiere que "… aunque no existen estudios al respecto, se estima que el 15% del material existente en Internet es de contenido erótico, pornográfico e intolerante y ello debido a que la pornografía, especialmente la infantil, es un negocio que produce alrededor de 8 a 10 billones de dólares siendo considerada la tercera más grande actividad de la criminalidad organizada, después del trafico ilícito de drogas y las apuestas. Las razones de esta afirmación son claras, si tenemos en cuenta que, como es común apreciar, las redes como Internet ofrecen a sus usuarios acceso a páginas de alto contenido sexual, las cuales pueden reproducir imágenes visuales y auditivas, inclusive es posible la reproducción de obras y escritos con tales características lo cual configura el injusto propio del artículo 183 -1 del Código Penal, si el agraviado fuese menor de 14 años de edad. En el caso del artículo 183-3 del Código Penal, de los comportamientos allí se distinguen, son la incitación a la ebriedad o a la práctica de un acto obsceno de los que puedan configurarse con la ayuda de medios informáticos que se destinara a lograr que el menor de 14 años se alcoholice o practique un acto obsceno. [50]

Cabe resaltar que "... según la moderna doctrina penal, el Derecho penal no puede proteger meros contenidos morales, si es que se requiere aceptar la idea de que solo han de perseguirse conductas que poseen una apacible nocividad social... se protege en forma específica, el desarrollo y formación

[50] REYNA ALFARO, Luis Miguel, (2002) pág. 180 - 182

sexual del menor, como presupuesto de libertad sexual." [51]

Por otro lado, podemos apreciar la adición al Código Penal vigente del ***artículo 183-A,*** el cual trata sobre la ***Pornografía Infantil*** y dispone lo siguiente: *"El que posee, promueve, fabrica, distribuye, exhibe, ofrece, comercializa o publica, importa o exporta objetos, libros, escritos, imágenes visuales o auditivas, o realiza espectáculos en vivo de carácter pornográfico, en los cuales se utilice a menores de catorce a dieciocho años de edad, será sancionado con pena privativa de libertad no menor de cuatro ni mayor de seis años y con ciento veinte a trescientos sesenta y cinco días multa. Cuando el menor tenga menos de catorce años de edad la pena será no menor de cuatro ni mayor de ocho años y con ciento cincuenta a trescientos sesenta y cinco días multa. Si la víctima se encuentra en alguna de las condiciones previstas en el último párrafo del artículo 173, la pena privativa de libertad será no menor de ocho ni mayor de doce años. De ser el caso, el agente será inhabilitado conforme al artículo 36, incisos 1), 2), 4) y 5)."*

El artículo antes mencionado es una novedad legislativa destinada a sancionar a quines utilicen a menores de edad para hacerlos protagonistas de exhibiciones obscenas. Se advierte, asimismo, plausible intención de salvaguardar la integridad moral de los menores, con especial énfasis en los de mas corta edad.[52]

Es importante tener en cuenta que en abril del año 2002 se expidió la Ley Nº. 27697, que otorgó al Fiscal la facultad de intervenir y controlar las comunicaciones y documentos privados de personas que son materia de investigación (preliminar o jurisdiccional) en un total de doce delitos tipificados en nuestra legislación penal. Ello con la finalidad de facilitar la represión de dichos delitos. Asimismo, mediante la reciente dación del Decreto Legislativo Nº 991, publicado el 22 de julio del presente año 2007, se modifica la norma anteriormente citada, incorporando dentro del alcance de la citada Ley al delito de Pornografía Infantil.

Como bien se conoce, la Pornografía Infantil es un delito tipificado en el artículo 183-A de nuestro Código Penal mediante el cual se vulnera la llamada "Indemnidad Sexual del niño o adolescente", es decir las condiciones físicas y psicológicas del menor respecto a su sexualidad.

51 BRAMONT - ARIAS TORRES, Luis Alberto y GARCIA CANTIZANO, María del Carmen, Ob. cit.. pág. 278.

52 CHIRINOS SOTO Francisco, Código Penal Comentado, Editorial RODHAS Segunda Edición 2005 Lima pág 391

Nuestra legislación penal considera como sujeto activo de este delito y, por tanto, castiga, a quien posee, promueve, fabrica, distribuye, exhibe, ofrece, comercializa o publica, importa o exporta por cualquier medio incluido Internet, objetos, libros, escritos, imágenes visuales o auditivas, o realiza espectáculos en vivo de carácter pornográfico, en los cuales se utilice a niños o adolescentes.

Por tanto, habría incurrido en este delito quien cuenta, por ejemplo, en su domicilio, con videos pornográficos donde participen menores de edad, ya que dichos videos estarían bajo su posesión. Por el contrario, no incurría en este delito quien -a través de una cabina pública de Internet- ingresa a una página Web de contenido pornográfico infantil pues faltaría el elemento de la "posesión". Tampoco sería responsable el titular de la cabina pues la página Web donde se encuentran estos materiales pornográficos no son de su propiedad y, lamentablemente, Internet permite en muchos casos el acceso gratuito a algunas páginas.

Por otro lado, sí incurriría en este delito, quien por ejemplo, desde una cabina pública elabora una página con contenido pornográfico infantil y la difunde pues estaría entre los supuestos de tipo que señala la ley: "fabrica", "distribuye", "ofrece" y "publica", elementos que pueden concurrir en forma simultánea.

La modificatoria introducida a través de la dación del Decreto Legislativo Nº 991 representa a nuestro modo de ver un acierto en estos tiempos en que el delito de Pornografía Infantil se ha desarrollado en forma alarmante ayudado en gran medida por el avance tecnológico, específicamente, con el uso de la herramienta del Internet. El costo de acceso a Internet a través de las cabinas públicas es sumamente bajo lo que ha determinado, en lo últimos tiempos una proliferación de estos servicios y un uso masivo de los mismos por personas que pueden utilizarlos con fines lícitos, pero también, con fines ilícitos, como es el caso que nos ocupa: La Pornografía Infantil.

Con la dación de esta norma, el Ministerio Público, ante el conocimiento de la existencia de indicios de la comisión del delito en determinada cabina pública de Internet, podrá legítimamente solicitar, por ejemplo, la relación de usuarios de dicha cabina, e inclusive accesar a través de personal técnico

especializado en comunicaciones, a las páginas en que dichos usuarios hayan ingresado facilitando de esta manera su línea de investigación.

Si bien es cierto podría válidamente sostenerse que esta facultad estaría generando una colisión de derechos reconocidos constitucionalmente: La Intimidad versus el Interés Superior del Niño y del Adolescente, debemos señalar que, tanto la Doctrina nacional como la extranjera, así como jurisprudencia del Tribunal Constitucional, han determinado que ante una confrontación de derechos de igual jerarquía debe efectuarse una ponderación de los mismos a efectos de determinar cuál prevalece. Así, el Tribunal Constitucional, ha señalado que el Estado puede legítimamente dictar medidas que afecten la libre iniciativa privada a fin de ejercer su función supervisora, correctiva y sancionadora.

La especial protección que brinda nuestra Constitución al Niño, la abundante legislación nacional que existe en aras de su protección, la legislación internacional a la cual el Perú se ha adherido, el fin legítimo de prevención de un delito que vulnera la indemnidad sexual del niño y por tanto su Interés Superior, hacen que prevalezca legítimamente su defensa, en desmedro al Derecho a la Intimidad. No obstante lo anteriormente expuesto el tiempo evidenciará –y esperamos que así sea-si el Ministerio Público ejerce dicha facultad bajo los principios de proporcionalidad y motivación suficientes a fin de evitar posibles excesos.[53]

3.8.6 Delito de Hurto

Del los tipos penales previstos en el presente Título denominado “Delitos contra el patrimonio”, se encuentra capítulo titulado como “Hurto”, en el cual se encuentra tipificado en **artículo 185º** el cual trata sobre las **el hurto simple**, dispone lo siguiente: *“El que, para ver provecho, se apodera ilegítimamente de un bien mueble, total o parcialmente ajeno, sustrayéndolo del lugar donde se encuentra, será reprimido con pena privativa de libertad no menor de uno ni mayor de tres años. Se equiparan a bien mueble la energía eléctrica, el gas, el agua **y cualquier otra energía o elemento que tenga valor económico, así como el espectro electromagnético.*** Uno de los supuestos en los que la información ha sido empleada como medio para cometer delitos es la figura del Hurto, que

[53] TORRES DE FERREYROS Silvia, PORNOGRAFIA INFANTIL: HACIA UNA LEGISLACION QUE FACILITE SU REPRESION (A propósito de la dación del Decreto Legislativo No. 991) www.tytl.com.pe 07 agosto 2007 Lima.

establece como modalidad agravada el uso de ***"sistemas de transferencia electrónica de fondos, de la telemática en general o violación del empleo de claves secretas"***.

De igual forma en el capítulo titulado como "Hurto", en el cual se encuentra tipificado en **artículo 186º** el cual trata sobre las **el hurto agravado**, dispone lo siguiente: "*El agente será reprimido con pena privativa de libertad no menor de tres ni mayor de seis años si el hurto es cometido...."*

La pena será no menor de cuatro ni mayor de ocho años si el hurto es cometido:

3. *Mediante la utilización de* ***sistemas de transferencia electrónica de fondos, de la telemática en general, o la violación del empleo de claves secretas.*** *La pena será no menor de ocho ni mayor de quince años cuando el agente actúa en calidad de jefe, cabecilla o dirigente de una organización destinada a perpretar estos delitos".*

Este delito se refiere al *Hurto Agravado*, la configuración de tal agravante responde al avance observado por estas formas modernas de criminalidad, como sin: *la utilización de sistemas de transferencia electrónica de fondos, de la telemática en general, o la violación del empleo de claves secretas.* El uso de las redes de interconexión se ha generalizado principalmente, por los requerimientos de eficacia y celeridad en las instituciones bancarias y financieras de nuestro país, situación que se viene observando desde hace unos pocos años, constituyendo por lo tanto un objeto atractivo de vulneración, aunque consideramos que en este caso el agente encontrarse sumamente calificado en esta tecnología o estrechamente ligado a la entidad bancaria que se pretende agraviar, para acceder a estas redes (redes de interconexión bancaria) de carácter sumamente reservado a fin de configurar el ilícito.

El objeto material del delito ha planteado muchas dudas en los supuestos relacionados a la transferencia electrónica de fondos, vinculadas la mayoría de ellas a la ausencia de tangibilidad del bien, sin embargo, si partimos de la idea que el bien mueble es "todo objeto del mundo exterior con valor económico, que sea susceptible de apoderamiento y desplazamiento", resulta evidente que a pesar de no existir una tangibilidad inmediata del dinero sustraído a través de sistemas de transferencia electrónica o telemática, existe un apoderamiento constatable ex post, es decir, cuando el sujeto activo pretenda retirar el dinero sustraído. [54]

[54] REYNA ALFARO, Luis Miguel, (2002) pág. 185 – 186.

3.8.7 Delito de Estafa

Del los tipos penales previstos en el presente capítulo titulado “Estafa y otras defraudaciones”, se encuentra tipificado en **artículo 185º** el cual trata sobre la **estafa**, dispone lo siguiente: *“El que procura para sí o para otro un provecho ilícito en perjuicio de tercero, induciendo o manteniendo en error al agraviado mediante engaño, astucia, ardid* ***u otra forma fraudulenta,*** *será reprimido con pena privativa de libertad no menor de uno ni mayor de seis años”.*

Con relación al delito de estafa, Luis Bramont – Arias refiere que el acto de disposición ha de realizarlo la persona engañada, quien se encuentra en una situación de error, de ahí, que siempre se entienda en la estafa el acto de disposición es un acto humano, es decir realizado por una persona, en el caso de las manipulaciones informáticas fraudulentas el acto de disposición lo realiza la computadora, con el cual el esquema planteado en el delito de estafa[55].

Otros autores afirman que este ilícito, da cabida a realizarse a través de medios informáticos, así como el Internet, al indicar en su tipo base la frase *“u otra forma fraudulenta”.* La doctrina penal se ha planteado la posibilidad de recurrir a esta figura con el fin de reprimir el fraude informático, en especial, en aquellos casos en los cuales se introducen datos falsos en sistemas de información a fin de obtener un provecho económico, por ejemplo “Carlos”, empleado de una empresa, introduce en los sistemas de información de ésta, datos en los que aparecen sueldos a personas ficticias, los cuales luego cobra, obteniendo beneficio patrimonial indebido.[56]

La doctrina define la estafa por computadora como «toda manipulación o alteración del proceso de elaboración electrónica de cualquier clase o en cualquier momento de éste (dentro del sistema o fuera del sistema), realizada con ánimo de lucro y causando un perjuicio económico a un tercero», incluyéndose también las manipulaciones operadas sobre ficheros o soportes informáticos, electrónicos o telemáticos, pudiendo realizar estas conductas también personas legitimadas para acceder y operar en el sistema informático. [57]

---

55 BRAMONT - ARIAS TORRES, Luis (1997) pág. 38

56 REYNA ALFARO, Luis Miguel, (2002) pág. 187

57 DICCIONARIO JURÍDICO ESPASA, Editorial Espasa Calpe S.A. Madrid 2001

Siendo así, se entiende que el "...fraude a través de Internet es una de las conductas que mayores perjuicios económicos genera en las economías modernas, de lo que desprende la especial atención que ha generado por parte de los estudiosos del Derecho Penal, esto debido a las grandes dificultades que surgen para comprender el amplio catálogo de conductas defrauatorias que tiene cabida en Internet en la figura tradicional de Estafa, dificultades que según creo tienen su principal génesis en la diversidad de características que concurren en éstas." [58]

Entre algunas de las modalidades más usuales de fraude a través de sistemas de información tenemos:

Los Datos Engañosos (data diddling), consiste en la introducción de datos falsos e los ordenadores o en la eliminación de informaciones veraces. Agrupa a todas las manipulaciones informáticas de ese tipo, como el uso de identidad falsa.

Los Caballos de Troya (troyan horses), el mecanismo de este fraude funciona en forma análoga al conocido episodio épico, se introducen al ordenador rutinas o instrucciones destinadas a realizar operaciones no autorizadas, como la transferencia de fondos de una cuenta bancaria a otra, con el beneficio del delincuente. Desde el punto de vista probatorio resultan difíciles de detectar toda vez que incluso dentro de sus ordenes puede aparecer las de autodestrucción luego de culminada la labor encomendada.

La Técnica del "Salami" (Salami Tecnique / Rounding Down), mecanismo que permite mediante el redondeo de pequeñas cantidades de activos financieros de una serie de cuentas bancarias, la obtención de beneficios considerables en el sujeto activo de la conducta, piénsese, por ejemplo, en el beneficio que puede obtener quien sustrae solo diez centavos de dólar de cada cuenta bancaria, luego de miles de estas.

Suplantación de Personalidad (Impersonation), consiste en la utilización de datos personales ajenos, suplantando a la persona afectada, se produce generalmente ante la sustracción de tarjetas o claves secretas, así el sujeto activo puede adquirir bienes empleando los datos de otra persona y lograr que estos sean asumidos por éste.

Fraude Bancario o electrónico o "carding", es el fraude a través de tarjetas de crédito, resulta ser una modalidad muy similar a la suplantación de personalidad.

[58] REYNA ALFARO, Luis Miguel, (2002) pág. 187

Fraude en loterías y apuestas electrónicas, modalidad muy usual en Internet y por la cual algunas "sites" plantean o elaboran apuestas cuyos premios nunca serán abonados.

Ventas fraudulentas a través de e-mail, consiste en ofertar productos a través de Internet, sin embargo, pese a efectuar los cobros respectivos, los bienes ofertados nunca son entregados a los compradores.

3.8.8 Delito de Daños

Del los tipos penales previstos en el presente capítulo titulado "Daños", se encuentra tipificado en **artículo 205º** el cual trata sobre el daño simple y dispone lo siguiente: *"El que daña, destruye o inutiliza un bien, mueble o inmueble, total o parcialmente ajeno será reprimido con pena privativa de libertad no mayor de dos años y con treinta a sesenta días multa."*

El objeto material de este delito resulta ser un bien mueble o inmueble, surge sin embargo la interrogante ¿Comete el delito de daños el que causa daños a los elementos lógicos del ordenador?, la respuesta debe de ir vinculada al propio concepto del objeto material de la conducta, esto es, del bien mueble o inmueble.[59]

El profesor Juan Morales Godo, en un artículo llamado "La Vida Privada y el Peligro ante el Desarrollo de la Informática", donde indica que "La lucha permanente del ser humano ha sido por la libertad; por librarse de todo aquello que impide el desarrollo personal. Han existido y existen múltiples y variadas formas de provocar daño a las personas limitando su libertad. El desarrollo de la ciencia y el de la tecnología han producido efectos contradictorios: así como ha traído progreso a la humanidad, siendo indudable que hoy en día el hombre vive más y mejor, también han provocado una serie de interrogantes de carácter ético, legal y político … por los daños que puedan ocasionar al propio ser humano".[60]

En tal sentido según Luis Reyna Alfaro afirma que la protección de datos y programas informáticos, a nuestro entender no encuadra dentro de los alcances del delito de daños, así como está actualmente redactado, pues surgen diferencias cualitativas entre el objeto material de una y otra

[59] REYNA ALFARO, Luis Miguel, (2002) pág. 191.

[60] IUS ET PRAXIS, Revista de la Facultad de Derecho y Ciencias Políticas, Fondo de Desarrollo Editorial de la Universidad de Lima, Nro. 26 Enero – Diciembre. Lima, 1996. pág. 24.

conducta, mientras en el delito de daños, el objeto material del injusto será un bien mueble o inmueble, total o parcialmente ajeno, en los daños a los elementos lógicos del sistema informático el objeto será una especie de flujo electromagnético, no subsumible en el concepto de cosa mueble. Distinto es de caso del Hardware que si cumple con el requisito de materialidad del bien, conforme propugna la doctrina dominante al respecto."[61]

Finalmente, concurrimos cuando Luis Bramont – Arias afirma que es indudable que estos comportamientos producen un daño en el patrimonio de las personas, por lo que no hay inconveniente en sancionar penalmente dichas conductas. Pero es necesario indicar que con el delito de daños se protege un determinado grupo de conductas que están comprendidos en el delito informático, quedando fuera otras, como por ejemplo, el acceso a una información reservada sin dañar la base de datos. De ahí que el delito de daños será de aplicación siempre que la conducta del autor del hecho limite la capacidad de funcionamiento de la base de datos.[62]

3.8.9 Delitos Contra los Derechos Intelectuales

Del los tipos penales previstos en el presente Título denominado "Delitos contra los derechos intelectuales", se encuentra el capítulo titulado "Delitos contra los derechos de autor y conexos", tenemos el **artículo 216º** el cual trata sobre la copia o reproducción no autorizada, dispone lo siguiente: *"Será reprimido con pena privativa de la libertad no menor de dos ni mayor de cuatro años y de diez a sesenta días-multa, a quien estando autorizado para publicar una obra, lo hiciere en una de las formas siguientes:*

a. Sin mencionar en los ejemplares el nombre del autor, traductor, adaptador, compilador o arreglador.

b. Estampe el nombre con adiciones o supresiones que afecte la reputación del autor como tal, o en su caso, del traductor, adaptador, compilador o arreglador.

c. Publique la obra con abreviaturas, adiciones, supresiones, o cualquier otra modificación, sin el consentimiento del titular del derecho.

d. Publique separadamente varias obras, cuando la autorización se haya conferido para publicarlas en conjunto; o las publique en conjunto, cuando solamente se le haya autorizado la publicación de ellas en forma separada."

En primer lugar debemos indicar que en el ámbito de los Derechos Intelectuales son muchas las cuestiones que han salido a la palestra del debate jurídico. La primera de ellas fue la dilucidación del carácter de

61 REYNA ALFARO, Luis Miguel, (2002) pág. 191.
62 BRAMONT - ARIAS TORRES, Luis (1997) pág. 42

creación intelectual de los programas de ordenador, luego surgieron problemas vinculados a los derechos propios de la creación intelectuales el entorno digital, finalmente, como un tema más reciente, están las repercusiones que programas como el MP3 generan en los derechos de autor. Con relación de la primera cuestión, se tiene que los programas de ordenador han obtenido resguardo jurídico a partir de las últimas décadas, cuando las dudas acerca de su naturaleza se despejan y dejan claro el panorama. En sus inicios, no existía en realidad necesidad de tutela, toda vez que la rusticidad de los componentes informáticos hacía poco frecuente su vulneración, esto debido a que tanto Hardware y Software eran un todo único e indispensable, cada unidad de ordenador que lo contenía su respectivo programa interiormente dispuesto, de tal manera que resultaba imposible o poco probable su reproducción, pues retirar el programa significaba dañarlo y hacer inservible el ordenador que lo contenía, los problemas en realidad surgieron a partir de la aparición de tecnologías avanzadas que permiten la reproducción de programas en pocos segundos[63].

A esta conducta los autores asimilan lo que se conoce como “piratería de software” frente a la copia ilícita. Estos hechos han alcanzado en la realidad una especial gravedad dada la frecuencia con la que abundan copias piratas de todo tipo de programas de computadoras. Inclusive en nuestro país ello ha obligado a la creación de una fiscalía especializada en la persecución de de todas la conductas relativas a la defraudación del derecho de autor. Estas conductas presentan un considerable perjuicio económico al autor, quien deja de percibir sus correspondientes derechos por la información o venta del software, que es elaborado con un considerable esfuerzo. Por tanto, el delito contra la propiedad intelectual solo comprendería un grupo de comportamientos incluidos en el delito informático, básicamente los refereidos a la defraudación de los derechos de autor por su creación científica en el campo del software.

A raíz de ello aparecen tres vertientes doctrinarias respecto a la rama que debía amparar al software. La primera de ellas considera que la tutela de los programas de ordenador se ubica dentro del Derecho Industrial, sin embargo, fue rápidamente desvirtuada pues confundía la protección de la creación en si con la tutela al soporte físico que la contiene. La segunda corriente propone

63 REYNA ALFARO, Luis Miguel, (2002) pág. 192-193

que la protección del software se realice a través de un derecho específico, sin embargo, tampoco resulta adecuado postularla pues genera el aumento de la disposición legislativa y porque en su tratamiento se aprecian consideraciones entre el contendido del derecho específico y autoral[64].

3.8.10 Terrorismo

Se entiende por ***terrorismo***, al "... uso de la violencia, o amenaza de recurrir a ella, con fines políticos, que se dirige contra víctimas individuales o grupos más amplios y cuyo alcance trasciende con frecuencia los límites nacionales. El término implica una acción llevada a cabo por grupos no gubernamentales o por unidades secretas o irregulares, que operan fuera de los parámetros habituales de las guerras y a veces tienen como objetivo fomentar la revolución. El terrorismo de Estado, ejercido por un Estado contra sus propios súbditos o comunidades conquistadas, se considera también una modalidad de terrorismo. Más que la realización de fines militares, el objetivo de los terroristas es la propagación del pánico en la comunidad sobre la que se dirige la violencia. En consecuencia, la comunidad se ve coaccionada a actuar de acuerdo con los deseos de los terroristas. El terrorismo extremo busca a menudo la desestabilización de un Estado causando el mayor caos posible, para posibilitar así una transformación radical del orden existente." [65]

De igual forma entendemos "... la noción de *"terrorismo por computadora",* la cual rebasa los elementos técnicos y económicos, convirtiendo en menester en estudio integral de carácter multidisciplinario, bajo una perspectiva social (finalmente es un problema específico que atañe de manera cada vez más directa a la sociedad) tomando en cuenta de igual forma los insoslayables factores políticos, étnicos, históricos, religiosos, etc., a través de una reglamentación jurídica confiable. Es una cuestión directamente vinculada a aquella relativa a la seguridad de la informática y a los riesgos informáticos, tratándose de una formulación fundamentalmente enunciativa y no tanto propositiva, con un punto de vista breve, pero realista de dichas implicancias, con el afán de recordarnos que, sin el control necesario es uso de las computadoras puede convertirse en un factor de autodestrucción en detrimento del desarrollo del hombre"[66].

---

64 REYNA ALFARO, Luis Miguel, (2002) pág. 193.

65 BIBLIOTECA DE CONSULTA ENCARTA 2003. Microsoft Corporation. © 1993-2002.

66 BLOSSIERS HUME, Juan José. Ob. cit. págs. 244 – 245.

Hasta hace poco las actividades de estos grupos eran vulnerables ante la posible intervención de los servicios de inteligencia, pero en lo que se ha convertido Internet para estos grupos es en un medio óptimo para actuar al margen de cualquier tipo de control. La encriptación de los mensajes, la extrema vulnerabilidad de los contenidos y, fundamentalmente, la falta de una legislación uniforme y global es lo que está permitiendo a este tipo de grupos actuar impunemente y al margen de la ley.

La red está siendo utilizada no sólo con fines propagandísticos sino para llevar a cabo actos terroristas sin la necesidad de arriesgar ningún tipo de infraestructura ni humana ni material. Tales son las posibilidades que las nuevas tecnologías ponen a disposición de estos grupos, que hoy en día es factible la posibilidad de intervenir, alterar o destruir los núcleos neurálgicos de cualquier sistema informático.

Por lo que en el Perú, "... el fenómeno de violencia y destrucción que ha afectado nuestra sociedad durante las dos últimas décadas a través del accionar grupos como "Sendero Luminoso" y el Movimiento Revolucionario "Tupac Amaru", ha contado con una serie de organismos y grupos de apoyo en el exterior, que han colaborado logística y económicamente con la subversión por lo que es posible observar páginas Web que favorecen y apoyan este tipo de acciones, transformando la realidad a su conveniencia, logrando generar una imagen lejana a la realidad, basta con "navegar" en la red para encontrar páginas apoyando a agrupaciones terrorista de todo el orbe (ETA, IRA, HAMAS, SOL ROJO entre las más conocidas); ello configura el delito de apología al terrorismo previsto en la norma especial que reprime el terrorismo (Decreto Ley Nº 25475), pues la idoneidad de las redes de interconexión es perfectamente admisible[67].

Según lo indicado en los párrafos precedentes el desarrollo de la ciencia y tecnología acarrea tanto a nivel nacional como internacional que se realicen nuevas formas de criminalidad como son los llamados delitos informáticos, a través de red, pueden hacer propagandas referente a los diversos grupos terroristas; asimismo, de igual forma es factible la posibilidad de intervenir, alterar o destruir los núcleos neurálgicos de cualquier sistema informático.

67 REYNA ALFARO, Luis Miguel, (2002) pág. 197.

3.8.11 Delitos Electorales

Del los tipos penales previstos en el presente capítulo titulado "De los Delitos contra el Derecho de sufragio", se encuentra tipificado en **artículo 359º** el cual trata sobre los **atentados contra el derecho de sufragio** y dispone lo siguiente: *"Será reprimido con pena privativa de libertad no menor de dos ni mayor de ocho años el que, con propósito de impedir o alterar el resultado de un proceso electoral, realiza cualquiera de las acciones siguientes:*

> *"...5. Altera, **de cualquier manera**, el resultado de una elección o torna imposible la realización del escrutinio".*

Aunque son muchos los supuestos comprendidos en el presente artículo, el inciso quinto el de mayor interés para el presente estudio, que sanciona a la persona que: ***"altera, de cualquier manera"*** el resultado de una elección. El manejo indebido de la información ha cobrado un especial interés en nuestro país donde actualmente se están procesando una multiplicidad de sujetos que laboraban en la Oficina Nacional de Procesos Electorales (OMPE) por haber alterado el resultado de la elección de congresistas de las últimas elecciones generales, ingresando datos falsos en sus sistemas de procesamientos de datos.[68]

3.8.12 Delitos de Falsedad Documental

Del los tipos penales previstos en el presente capítulo titulado "Falsificación de documentos en general", se encuentra tipificado en **artículo 427º** el cual trata sobre la **falsificación de documentos** y dispone lo siguiente: **"***El que hace, en **todo o en parte, un documento falso o adultera** uno verdadero que pueda dar origen a derecho u obligación o servir para probar un hecho, con el propósito de utilizar el documento, será reprimido, si de su uso puede resultar algún perjuicio, con pena privativa de libertad no menor de dos ni mayor de diez años y con treinta a noventa días-multa si se trata de un documento público, registro público, título auténtico o cualquier otro trasmisible por endoso o al portador y con pena privativa de libertad no menor de dos ni mayor de cuatro años, y con ciento ochenta a trescientos sesenta y cinco días-multa, si se trata de un documento privado. El que hace **uso de un documento falso o falsificado**, como si fuese legítimo, siempre que de su uso pueda resultar algún perjuicio, será reprimido, en su caso, con las mismas penas.*

Este ilícito, exagera para su consumación que el autor haga, en ***"todo o en parte, un documento falso o adultere uno verdadero***" que pueda dar origen a derecho u obligación que pueda servir para probar un hecho, con el

[68] REYNA ALFARO, Luis Miguel, (2002). pág. 198.

propósito de utilizar el documento, si de su uso puede resultar algún perjuicio.

En el tema que nos ocupa, la principal cuestión a debatir se encuentra relacionado a la posibilidad de comprender dentro del concepto de documentos aquellos de orden digital, en este punto coincido con Bramont – Arias Torres en admitir los documentos digitales, toda vez que existe un soporte corporal estable, reconocible visualmente e individualizable en su autoría. Esta postura se abona con la redacción del artículo 234* del Código Procesal Civil y la Ley de Firmas y Certificaciones digitales que regula el empleo de la firma electrónica, otorgándole la misma validez y eficacia jurídica que la firma manuscrita u otra análoga. La firma digital, como indica Galindo: "es el mecanismo que permite garantizar la identidad del autor de un documento así como la no alteración de su contenido," por lo que sus efectos, como resulta obvio, van más allá de la mera encriptación.[69]

Finalmente, compartimos las afirmaciones de Luis Bramont – Arias, cuando se refiere a que esta modalidad delictiva puede aplicarse al delincuente informático siempre y cuando se supere la concepción tradicional de documento, anclada básicamente en un papel escrito, y se acepten nuevas formas de de expresión documental, sobre la base de los diskettes, CD, discos duros, en cuanto a sistemas actuales de expresión de información. De ahí que en algunas legislaciones como la alemana, para cubrir esta laguna se crea un nuevo tipo penal, en el mismo capítulo de falsedad documental (capítulo 23) relativo a la falsedad de datos computarizados –parágrafo 267 del StGB, *Falschung beweiserheblicher Dater*-, con el fin de adaptar características particulares de la información de una computadora a nuevas modalidades de falsificación[70].

---

69 REYNA ALFARO, Luis Miguel, (2002). pág. 199

* Artículo 234º "Clases de documentos".- Son documentos los escritos públicos o privados, los impresos, fotocopias, facsímil o fax, planos, cuadros, dibujos, fotografías, radiografías, cintas cinematográficas, microformas tanto en la modalidad de microfilm como en la modalidad de soportes informáticos, y otras reproducciones de audio o video, la telemática en general y demás objetos que recojan, contengan o representen algún hecho, o una actividad humana o su resultado.

70 BRAMONT - ARIAS TORRES, Luis (1997) pág. 46

CAPÍTULO IV:

LEGISLACIÓN COMPARADA

En el presente Capítulo desarrollaremos sobre la legislación comparada de países tanto europeos y americanos relacionado con los delitos informáticos, motivo por el cual cabe precisar que los países considerados en el presente trabajo de investigación han incluido dentro de su legislación nacional a esta nueva forma de criminalidad; los mismos que han sido incluido en sus respectivos códigos penales o leyes especiales contra estos delitos de nueva data; asimismo, este capítulo, nos va a permitir tener mayor conocimiento de como se esta haciendo frente en la actualidad esta nueva forma de criminalidad, por ello la importancia del presente capítulo en el presente trabajo de investigación.

En tal sentido tanto los países y las organizaciones internacionales se han visto en la necesidad de legislar sobre los denominados delitos informáticos, debido a los daños y perjuicios que le han causado a la humanidad. Sin embargo, si bien es cierto existe un esfuerzo por parte de los países para tratar de evitarlos, no existe un criterio unificado de cómo deben ser atacados, por lo cual se hace imprescindible que se siga trabajando para llegar a la unificación de los criterios y así poder tener una legislación internacional coherente y comprometer a los países para que legislen sobre la materia basándose en los criterios adoptados internacionalmente y "aunque es uniforme el interés por la problemática de los delitos informáticos, solo algunos países han legislado en sede penal al respecto, no obstante lo afirmado, actualmente se vienen planteando en el derecho comparado una serie de propuestas, siendo las más cercanas y de mayor interés en nuestro país la de México, Brasil y la Unión Europea".[1]

Es importante resaltar que los diferentes países tanto americanos como europeos han incorporado en su legislación nacional así como en sus respectivos códigos penales y a través de leyes especiales relacionado con los delitos informáticos, estableciendo así garantías y mecanismos para hacer frente a estos ilícitos de nueva data. Asimismo, de lo investigado hasta el momento, se ha podido apreciar que en América Latina la regulación de los "Delitos Informáticos", se encuentran una fase de incorporación dentro ordenamiento jurídico penal.

[1] REYNA ALFARO, Luis Miguel. *"Los Delitos Informáticos – Aspectos Criminológicos, Dogmáticos y de Política Criminal.* JURISTA Editores. Lima, 2002, pág. 275.

4.1 En la Unión Europea

A continuación vamos a tratar como vienen haciendo frente a estos delitos de nueva data por parte de los países europeos, pudiendo apreciar que en general, en la legislación comparada como es el caso de la legislación europea viene siendo insuficiente con relación al incremento de los ilícitos denominados delitos informáticos.

Asimismo, podemos apreciar que se está trabajando ampliamente, tanto en el ámbito estadual, como a nivel bloque comunitario. Para formarnos una breve idea de lo avanzado que está el tema, entraremos en detalles respecto de ciertos países que por su trascendencia o similitud al nuestro, estimamos nos brindarán una comparación generosa en consideraciones.

4.1.1 Alemania

El modelo alemán seguido por la legislación penal alemana respecto a la lucha contra la criminalidad informática, se construye sobre la base de identificar dos supuestos de acciones atentatorias para determinados bienes jurídicos. Se tipifica al fraude informático y al delito de sabotaje informático.

El bien jurídico protegido primordialmente es el patrimonio. En cuanto a conductas atentatorias a la vida personal y la privacidad, el código penal alemán sanciona el espionaje de datos pero excluye la información que se encuentre almacenada o que pueda ser transmitida electrónica o magnéticamente o transmitida de forma inmediatamente accesible. Con ello, prácticamente no se regula ningún tipo penal que pudiera estar referido a un espionaje de datos informatizados. No se quiso punir la mera intrusión informática, sino sólo en aquellos casos de conductas que signifiquen la manipulación de las computadoras y persigan un ánimo de lucro.

En Alemania[2] para hacer frente a delincuencia relacionada con la informática y con sus efectos a partir del 1 de agosto de 1986, se adoptó la ***Segunda Ley contra la Criminalidad Económica*** del 15 de mayo de 1986 en la que se contemplan los siguientes delitos:

Espionaje de datos (202 a)

Estafa informática (263 a)

[2] INSTITUTO NACIONAL DE ESTADISTICA E INFORMATICA (INEI), Colección de Seguridad de la Información: *"Delitos Informáticos"*, Lima, 2001, pág. 56

Falsificación de datos probatorios (269) junto a modificaciones complementarias del resto de falsedades documentales como el engaño en el tráfico jurídico mediante la elaboración de datos, falsedad ideológica, uso de documentos falsos (270, 271, 273)

Alteración de datos (303 a) es ilícito cancelar, inutilizar o alterar datos inclusive la tentativa es punible.

Sabotaje informático (303 b). Destrucción de elaboración de datos de especial significado por medio de destrucción, deterioro, inutilización, eliminación o alteración de un sistema de datos. También es punible la tentativa.

Utilización abusiva de cheques o tarjetas de crédito (266b)

En lo que se refiere a la estafa informática, la formulación de un nuevo tipo penal, tuvo como dificultad principal el hallar un equivalente análogo al triple requisito de acción engañosa, causación del error y disposición patrimonial en el engaño del computador, así como en garantizar las posibilidades de control de la nueva expresión legal, quedando en la redacción que el perjuicio patrimonial que se comete consiste en influir en el resultado de una elaboración de datos por medio de una realización incorrecta del programa, a través de la utilización de datos incorrectos o incompletos, mediante la utilización no autorizada de datos, o a través de una intervención ilícita. Sobre el particular, cabe mencionar que esta solución en forma parcialmente abreviada, fue también adoptada en los Países Escandinavos y en Austria. En opinión de estudiosos de la materia, el legislador alemán ha introducido un número relativamente alto de nuevos preceptos penales, pero no ha llegado tan lejos como los Estados Unidos.

De esta forma, dicen que no sólo ha renunciado a tipificar la mera penetración no autorizada en sistemas ajenos de computadoras, sino que tampoco ha castigado el uso no autorizado de equipos de procesos de datos, aunque tenga lugar de forma cualificada. En el caso de Alemania, se ha señalado que a la hora de introducir nuevos preceptos penales para la represión de la llamada criminalidad informática el gobierno, tuvo que reflexionar acerca de dónde radicaban las verdaderas dificultades para la aplicación del Derecho penal tradicional a comportamientos dañosos en los que desempeña un papel esencial la introducción del proceso electrónico de

datos, así como acerca de qué bienes jurídicos merecedores de protección penal resultaban así lesionados. Fue entonces cuando se comprobó que, por una parte, en la medida en que las instalaciones de tratamiento electrónico de datos son utilizadas para la comisión de hechos delictivos, en especial en el ámbito económico, pueden conferir a éstos una nueva dimensión, pero que en realidad tan sólo constituyen un nuevo modus operandi, que no ofrece problemas para la aplicación de determinados tipos. Por otra parte, sin embargo, la protección fragmentaria de determinados bienes jurídicos ha puesto de relieve que éstos no pueden ser protegidos suficientemente por el Derecho vigente contra nuevas formas de agresión que pasan por la utilización abusiva de instalaciones informáticas.

En otro orden de ideas, las diversas formas de aparición de la criminalidad informática propician además, la aparición de nuevas lesiones de bienes jurídicos merecedoras de pena, especialmente en la medida en que el objeto de la acción sean datos almacenados o transmitidos o se trate del daño a sistemas informáticos. Podemos concluir que la violación al derecho a la intimidad u otras acciones que no tengan consecuencias patrimoniales, como por ejemplo accesos ilegítimos realizados por hackers en los que el móvil es el desafío de acceder ilegítimamente a un sistema y curiosear la información contenida en él, la interceptación de un correo electrónico, etc. no se encuentran previstas en la Legislación alemana.

4.1.2 Austria

Según la Ley de reforma del Código Penal del 22 de diciembre de 1987, se contemplan los siguientes delitos:

Destrucción de datos (art. 126) no solo datos personales sino también los no personales y los programas.

Estafa informática (art. 148) se sanciona a aquellos que con dolo causen un perjuicio patrimonial a un tercero influyendo en el resultado de una elaboración de datos automáticos a través de la confección del programa, por la introducción, cancelación o alteración de datos o por actuar sobre el procesamiento de datos. Además contempla sanciones para quienes cometen este hecho utilizando su profesión[3].

[3] INSTITUTO NACIONAL DE ESTADISTICA E INFORMATICA (2001), pág. 58

4.1.3 Francia

La ley Nº 88-19 del 5 de enero de 1988 sobre el ***"Fraude Informático"***, la cual prevé penas de dos meses a dos años de prisión y multas de diez mil a cien mil francos por la intromisión fraudulenta que suprima o modifique datos; asimismo, contemplando los siguientes delitos informáticos:

Acceso fraudulento a un sistema de elaboración de datos(462-2).- En este artículo se sanciona tanto el acceso al sistema como al que se mantenga en él y aumenta la sanción correspondiente si de ese acceso resulta la supresión o modificación de los datos contenidos en el sistema o resulta la alteración del funcionamiento del sistema.

Sabotaje informático (462-3).- En este artículo se sanciona a quien impida o falsee el funcionamiento de un sistema de tratamiento automático de datos.

Destrucción de datos (462-4).- En este artículo se sanciona a quien, intencionadamente y con menosprecio de los derechos de los demás, introduzca datos en un sistema de tratamiento automático de datos o suprima o modifique los datos que este contiene o los modos de tratamiento o de transmisión.

Falsificación de documentos informatizados (462-5). En este artículo se sanciona a quien, de cualquier modo, falsifique documentos informatizados con intención de causar un perjuicio a otro.

Uso de documentos informatizados falsos (462-6) En este artículo se sanciona a quien conscientemente haga uso de documentos falsos haciendo referencia al artículo 462-5[4].

4.1.4 Inglaterra

La Computer Misuse Act (Ley de Abusos Informáticos) comenzó a regir debido varios casos de hacking, motivo que surgieron nuevas leyes sobre delitos informáticos.

En agosto de 1990 comenzó a regir la Computer Misuse Act, mediante esta ley el intento, exitoso o no, de ***alterar datos informáticos*** es penado con hasta cinco años de prisión o multas. Contiene además la ley un apartado que específica la modificación de datos sin autorización. Los virus están incluidos en esa categoría. Asimismo dispone que liberar un virus tiene penas desde un mes a cinco años, dependiendo del daño que causen.

[4] INSTITUTO NACIONAL DE ESTADISTICA E INFORMATICA (2001), pág. 59

El acceso ilegal a una computadora contempla hasta seis meses de prisión o multa de hasta dos mil libras esterlinas. El acta se puede considerar dividida en tres partes: hackear (ingresar sin permiso en una computadora), hacer algo con la computadora hackeada y realizar alguna modificación no autorizada.

El último apartado se refiere tanto al hacking (por ejemplo, la modificación de un programa para instalar un backdoor), la infección con virus o, yendo al extremo, a la destrucción de datos como la inhabilitación del funcionamiento de la computadora. Bajo esta ley liberar un virus es delito y en enero de 1993 hubo un raid contra el grupo de creadores de virus. Se produjeron varios arrestos en la que fue considerada la primera prueba de la nueva ley en un entorno real[5].

4.1.5 Holanda

El 1º de marzo de 1993 entró en vigencia la Ley de Delitos Informáticos, Holanda, en el cual se penalizaba hacking, phreacking (utilización de servicios de telecomunicaciones evitando el pago total o parcial de dicho servicio), la ingeniería social (arte de convencer a la gente a entregar información que en circunstancias normales no la entregaría), la distribución de virus .

La distribución de virus esta penada de distinta forma si se escaparon por error o si fueron liberados para causar daño. Si se demuestra que el virus se escapó por error la pena no supera el mes de prisión; pero, si se comprueba que fueron liberados con la intención de causar daño, la pena puede llegar hasta los cuatro años de prisión.[6]

Ley de Delitos Informáticos, en la cual se penaliza los siguientes delitos:

El hacking

El preacking (utilización de servicios de telecomunicaciones evitando el pago total o parcial de dicho servicio)

La ingeniería social (arte de convencer a la gente de entregar información que en circunstancias normales no entregaría)

[5] http://www.segu-info.com.ar/delitos/inglaterra.htm

[6] INSTITUTO NACIONAL DE ESTADISTICA E INFORMATICA (2001), pág. 66

La distribución de virus: La distribución de virus está penada de distinta forma si se escaparon por error o si fueron liberados para causar daño. Si se demuestra que el virus se escapó por error, la pena no superará el mes de prisión; pero, si se comprueba que fueron liberados con la intención de causar daño, la pena puede llegar hasta los cuatro años de prisión.

El mero hecho de entrar en una computadora en la cual no se tiene acceso legal ya es delito y puede ser castigado hasta con seis meses de cárcel. Si se usó esa computadora hackeada para acceder a otra, la pena sube a cuatro años aunque el crimen, a simple vista, no parece ser peor que el anterior. Copiar archivos de la máquina hackeada o procesar datos en ella también conlleva un castigo de cuatro años en la cárcel.

Publicar la información obtenida es ilegal si son datos que debían permanecer en secreto, pero si son de interés público es legal. El daño a la información o a un sistema de comunicaciones puede ser castigado con cárcel de seis meses a quince años, aunque el máximo está reservado para quienes causaron la muerte de alguien con su accionar. Cambiar, agregar o borrar datos puede ser penalizado hasta con dos años de prisión pero, si se hizo vía remota aumenta a cuatro. Los virus están considerados de manera especial en la ley. Si se distribuyen con la intención de causar problemas, el castigo puede llegar hasta los cuatro años de cárcel; si simplemente se “escapó”, la pena no superará el mes.

El usar el servicio telefónico mediante un truco técnico (Phreacking) o pasando señales falsas con el objetivo de no pagarlo puede recibir hasta tres años de prisión. La venta de elementos que permitan el Phreaking se castiga con un año de prisión como tope y si ese comercio es el modo de ganarse la vida del infractor, el máximo aumenta a tres. La ingeniería social también es castigada con hasta tres años de cárcel.

Recibir datos del aire es legal (transmisiones satelitales), siempre y cuando no haga falta un esfuerzo especial para conseguirlos; la declaración protege datos encriptados, como los de ciertos canales de televisión satelital. Falsificar tarjetas de crédito de banca electrónica y usarlas para obtener beneficios o como si fueran las originales está penado con hasta seis años. Aunque hacerlas y no usarlas parece ser legal.

4.1.6 España

Este país quizás sea el que mayor experiencia ha obtenido en casos de delitos informáticos, en Europa. Su actual Ley Orgánica de Protección de Datos de Carácter Personal (LOPDCP) aprobada el 15 de diciembre de 1999, la cual reemplaza una veintena de leyes anteriores de la misma índole, contempla la mayor cantidad de acciones lesivas sobre la información.

Se sanciona en forma detallada la obtención o violación de secretos, el espionaje, la divulgación de datos privados, las estafas electrónicas, el hacking maligno o militar, el phreacking, la introducción de virus, etc.; aplicando pena de prisión y multa, agravándolas cuando existe una intención dolosa o cuando el hecho es cometido por parte de funcionarios públicos.
Asimismo, su nuevo Código Penal establece castigos de prisión y multas "a quien por cualquier medio destruya, altere, inutilice o de cualquier otro modo dañe los datos, programas o documentos electrónicos ajenos contenidos en redes, soportes o sistemas informáticos".

Si bien es cierto que el ***Código Penal de España***, es el más actualizado de la Unión Europea, las distintas figuras convencionales no alcanzan para perseguir la amplia gama de delitos informáticos que se pueden presentar, como por ejemplo distintas conductas de hacking, accesos ilegítimos a sistemas informáticos y distribución de virus, bombas lógicas, etc.

El 26 de octubre de 1995 se aprobó la nueva Ley Orgánica 1071995 del nuevo Código Penal Español[7], el cual entró en vigor el 24 de mayo de 1996. Este nuevo código intenta solucionar el problema de conductas delictivas que surgen a raíz del incremento de las nuevas tecnologías. Introduce tipos penales nuevos y modifica algunos de los existentes con el fin de adaptar la norma positiva al uso delictivo de los ordenadores, sistemas lógicos y tecnologías de la información aunque no alcanzan para perseguir la amplia gama de delitos informáticos que se pueden presentar, como por ejemplo distintas conductas de hacking, accesos ilegítimos a sistemas informáticos y distribución de virus, bombas lógicas, etc. La reforma aborda temas, desde la delincuencia clásica con medios tecnológicos a los delitos cometidos a través

[7] http://delitosinformaticos.com/legislacion/espana.shtml

de redes informáticas, como Internet. Podemos extraer los siguientes principios, receptados en el texto legal mencionado:

1. Se equiparan los mensajes de correo electrónico a las cartas y papeles privados se sanciona con una pena de prisión de uno a cuatro años. Asimismo, se castiga a quien, sin estar autorizado, se apodere, utilice o modifique, en perjuicio de terceros, datos personales de otro que se hallen registrados, entre otros, ***en soportes informáticos*** se sanciona con una pena de prisión de uno a seis años (artículo 197).
2. Se castiga al que produjere, vendiere, distribuye, exhibiere o facilite la producción, venta, difusión o exhibición ***por cualquier medio de material*** pornográfico en cuya elaboración haya sido utilizado menores de edad o incapaces (artículo 189.1.b) se sanciona con una pena de prisión de uno a tres años.
3. Se reprime el ***delito de amenazas*** hechas "por cualquier medio de comunicación" (artículo 169) se sanciona con una pena de prisión de uno a cinco años.
4. Se castigan las ***calumnias e injurias*** difundidas por cualquier medio (artículo 211) se sanciona con una pena de prisión de seis meses a seis años.
5. A los efectos de tipificar el ***delito de robo*** con fuerza en las cosas, se incluye el ***uso de llaves falsas***, entendiendo que son llaves las tarjetas, magnéticas o perforadas, y los mandos o instrumentos de apertura a distancia. (art 238- 239) se sanciona con una pena de prisión de dos a cinco años. Se modifica el artículo 248 que tipifica el delito de estafa incluyendo a los que con ánimo de lucro y valiéndose de alguna ***manipulación informática o artificio semejante***, consigan la transferencia no consentida de cualquier activo patrimonial en perjuicio de tercero.
6. Respecto a la modalidad de ***estafa por medios informáticos*** del párrafo 2 del artículo 248, que constituye novedad, su singularidad reside en que no hay ni engaño ni error pues es imposible engañar o inducir a error a un ordenador, modificándose, en esta singular estafa, el medio comisivo que no se dirige a una persona sino a una máquina, empleando alguna ***manipulación informática o artificio semejante,*** se sanciona con uno a seis años de prisión.

7. Penaliza la conducta de quien hiciera ***uso de cualquier equipo terminal de telecomunicación sin consentimiento de su titular***, ocasionando a este un perjuicio de más de cincuenta mil pesetas. 7. Se ***protege el software***, al castigarse a quien ***dañe*** los datos, programas o documentos electrónicos ajenos contenidos en redes, 8 soportes o sistemas informáticos (artículo 264) se sanciona con una pena de prisión de uno a seis años, así como la fabricación, puesta en circulación y tenencia de cualquier medio destinado a facilitar la supresión no autorizada de cualquier dispositivo utilizado para proteger programas de ordenador (artículo 270) se sanciona con una pena de prisión de seis meses a dos años.
8. Se sanciona la ***fabricación o tenencia de programas*** de ordenador, entre otros, específicamente destinados a la ***falsificación*** de todo tipo de documento (artículo 400) se sanciona con una pena de prisión de tres a seis años.

Es importante precisar que en la legislación penal española, las penas que se imponen a las personas que cometen delitos a través de medios informáticos varían de tres meses hasta seis años según la afectación o consumación del delito, como podemos apreciar en los artículos antes mencionados el legislador ha venido incorporando estas conductas a través de medios informáticos mediante constantes modificaciones e inclusiones en su código penal, lo cual es importante debido a que es uno de los países europeos que más ha legislado en materia de delitos informáticos.

4.1.7 Portugal

La Criminalidad Informática en el país luso ha sido abordado a través de la Ley Nº 109/91, esta norma contiene 19 artículos que se aplican subsidiariamente al Código Penal. El legislador portugués no solo ha tipificado los delitos de falsedad informática (art. 4), daños informáticos (art. 5), sabotaje informático (art.6), intrusismo informático (art. 7), interceptación ilegal (art.8), reproducción ilegítima de programas de ordenador (art. 9), sin que establece un glosario de términos (art. 2), una cláusula sobre la responsabilidad penal de las personas jurídicas (art. 3 y 10) y un conjunto de de consecuencias jurídicas y medidas accesorias (art. 11 al 19)[8].

[8] REYNA ALFARO, Luis Miguel. *"Los Delitos Informáticos – Aspectos Criminológicos, Dogmáticos y de Política Criminal*. JURISTA Editores. Lima, 2002, pág. 272.

4.2 En América

A continuación trataremos como vienen haciendo frente a estos delitos de nueva data los países americanos, donde se puede apreciar que en general, en la legislación comparada en este continente al igual que en Europa viene siendo insuficiente con relación al incremento de los ilícitos denominados delitos informáticos.

Asimismo, podemos apreciar que los países como Venezuela y Argentina son los que han legislado de manera más acertada y actualizada, por lo que en el presente capítulo entraremos en detalles respecto a países de América que por su trascendencia o similitud al nuestro, estimamos nos brindarán una comparación generosa en consideraciones.

4.2.1 Estados Unidos de Norte América

El primer abuso de una computadora se registró en 1958 mientras que recién en 1966 se llevó adelante el primer proceso por la alteración de datos de un banco de Mineapolis. En la primera mitad de la década del 70, mientras los especialistas y criminólogos discutían si el delito informático era el resultado de una nueva tecnología o un tema específico, los ataques computacionales se hicieron más frecuentes. Para acelerar las comunicaciones, enlazar compañías, centros de investigación y transferir datos, las redes debían (y deben) ser accesibles, por eso el Pentágono, la OTAN, las universidades, la NASA, los laboratorios industriales y militares se convirtieron en el blanco de los intrusos.

Pero en 1976 dos hechos marcaron un punto de inflexión en el tratamiento policial de los casos: el FBI dictó un curso de entrenamiento para sus agentes acerca de delitos informáticos y el Comité de Asuntos del Gobierno de la Cámara presentó dos informes que dieron lugar a la Ley Federal de Protección de Sistemas de 1985.

Esta ley fue la base para que Florida, Michigan, Colorado, Rhode Island y Arizona se constituyeran en los primeros estados con legislación específica, anticipándose un año al dictado de la Computer Fraud y Abuse Act de 1986. Este se refiere en su mayor parte a delitos de abuso o fraude contra casas financieras, registros médicos, computadoras de instituciones financieras

o involucradas en delitos interestatales. También especifica penas para el tráfico de claves con intención de cometer fraude y declara ilegal el uso de passwords ajenas o propias en forma inadecuada. Pero sólo es aplicable en y casos en los que se verifiquen daños cuyo valor supere el mínimo de mil dólares.

Consideramos importante mencionar la adopción en los Estados Unidos en 1994 del Acta Federal de Abuso Computacional (18 U.S.C. Sec. 1030), que modificando al Acta de Fraude y Abuso Computacional de 1986. Con la finalidad de eliminar los argumentos hipertecnicos acerca de qué es y que no es un virus, un gusano, un caballo de trolla, etcétera y en que difieren de los virus, la nueva acta proscribe la transmisión de un programa, información, códigos o comandos que causan daños a la computadora, a sistemas informáticos, a las redes, información, datos o programas (18 U.S.C. Sec 1030 (a) (5) (A). La nueva ley es un adelanto porque está directamente contra los actos de transmisión de virus[9]; en esta Ley se contempla la regulación de los virus (computer contaminant) conceptualizándolos aunque no los limita a los comúnmente llamados virus o gusanos sino que contempla a otras instrucciones designadas a contaminar otros grupos de programas o bases de datos.

Modificar, destruir, copiar, transmitir datos o alterar la operación normal de las computadoras, los sistemas o las redes informáticas es considerado delito. Así, esta ley es un acercamiento real al problema, alejado de argumentos técnicos para dar cabida a una nueva era de ataques tecnológicos.

El aumento en la cantidad de casos de hacking y la sensación de inseguridad permanente que generaron (fomentada por la difusión de los hechos en programas especiales de televisión y artículos de revistas especializadas), cambiaron la percepción de las autoridades con respecto a los hackers y sus ataques. Los casos que demostraron ese cambio fueron los del “Cóndor” Kevin Mitnicky y los de “ShadowHawk” Herbert Zinn hijo.

El FCIC (Federal Computers Investigation Commitee), es la organización más importante e influyente en lo referente a delitos computacionales: los investigadores estatales y locales, los agentes federales, abogados, auditores

[9] INSTITUTO NACIONAL DE ESTADISTICA E INFORMATICA (2001), pág. 64-65

financieros, programadores de seguridad y policías de la calle trabajan allí comunitariamente. El FCIC es la entrenadora del resto de las fuerzas policiales en cuanto a delitos informáticos, y el primer organismo establecido en el nivel nacional.

Además existe la Asociación Internacional de Especialistas en Investigación Computacional (IACIS), quien investiga nuevas técnicas para dividir un sistema en sus partes sin destruir las evidencias. Sus integrantes son "forenses de las computadoras" y trabajan, además de los Estados Unidos, Canadá, Taiwán e Irlanda.

La nueva ley constituye un acercamiento más responsable al creciente problema de los virus informáticos, específicamente no definiendo a los virus sino describiendo el acto para dar cabida en un futuro a la nueva era de ataques tecnológicos a los sistemas informáticos en cualquier forma en que se realicen. Diferenciando los niveles de delitos, la nueva ley da lugar a que se contemple qué se debe entender como acto delictivo. Asimismo, en materia de estafas electrónicas, defraudaciones y otros actos dolosos relacionados con los dispositivos de acceso a sistemas informáticos, la legislación estadounidense sanciona con pena de prisión y multa, a la persona que defraude a otro mediante la utilización de una computadora o red informática.

En el mes de julio del año 2000, el Senado y la Cámara de Representantes de este país tras un año largo de deliberaciones establece el "Acta de Firmas Electrónicas en el Comercio Global y Nacional". La ley sobre la firma digital responde a la necesidad de dar validez a documentos informáticos, mensajes electrónicos y contratos establecidos mediante Internet – entre empresas (para el B2B) y entre empresas y consumidores (para el B2C).

En los Estados Unidos, existen leyes federales que protegen contra el ataque a ordenadores, uso ilegítimo de passwords, invasiones electrónicas en la privacidad, y otras transgresiones. Las dos leyes Federales de EEUU mas importantes utilizadas por los jueces Federales de USA para perseguir a los delincuentes informáticos son: 18 USC, CAPÍTULO 47, SECCIÓN 1029, Y SECCIÓN 1030, de 1994 que modificó al Acta de Fraude y el Acta Federal de Abuso Computacional de 1986. El Pronunciamiento sobre Abuso y Fraude

Informático de 1986, es la principal pieza legislativa aplicable a la mayoría de los delitos informáticos, aunque muchas otras leyes pueden ser usadas para perseguir diferentes tipos de delitos informáticos. Éste pronunciamiento fue modificado con el Título 18 USA Código 1030. También complementó a la Ley de Privacidad de las Comunicaciones Electrónicas de 1986, que dejó fuera de la ley el interceptar comunicaciones digitales. Las Modificaciones de la Ley de Abusos Informáticos de 1994 amplió la Ley de 1986 al acto de transmitir virus y otra clase de código dañino.

El Acta de 1994 diferencia el tratamiento de aquellos que de manera temeraria lanzan ataques de virus, de aquellos que lo realizan con la intención de hacer estragos. El acta define dos niveles para el tratamiento de quienes crean virus, estableciendo para aquellos que intencionalmente causan un daño por la transmisión de un virus un castigo de hasta 10 años en prisión federal más una multa y para aquellos que lo transmiten sólo de manera negligente la sanción fluctúa entre una multa y un año en prisión. En virtud del Acta de 1994, el creador de un virus no podría escudarse en el hecho que no conocía que con su actuar iba a causar daño a alguien o que él solo quería enviar un mensaje.

En opinión de los legisladores estadounidenses, la nueva ley constituye un acercamiento más responsable al creciente problema de los virus informáticos. No se define a los virus, sino que se los describe, para dar cabida en un futuro a la nueva era de ataques tecnológicos a los sistemas informáticos en cualquier forma en que se realicen.

En general, un delito informático quebranta las leyes federales cuando entra en alguna de las siguientes categorías:

- Implica el compromiso o el robo de información de defensa nacional, asuntos exteriores, energía atómica u otra información restringida.
- Involucra a un ordenador perteneciente a departamentos o agencias del gobierno de los Estados Unidos.
- Involucra a un banco o cualquier otra clase de institución financiera.
- Involucra comunicaciones interestatales o con el extranjero.
- Afecta a gente u ordenadores en otros países o estados.

Asimismo, se debe destacar que existe una abundante legislación dentro de cada uno de los más de cincuenta estados. Estos suelen avanzar, tanto en lo que hace a la tipificación de los delitos u ofensas (spam, etc), como respecto de materias procesales. Algunos ejemplos son: i. Arizona Computer Crimes Laws, Section 13-2316 ii. Iowa Computer Crime Law, Chapter 716A.9 iii. Kansas Computer Crimes Law, Kansas, Section 1-3755 iv. Louisiana evised Status 14:73.4 (Computer Fraud) v. Michigan Compiled Laws Section 752.794 (Acces to computers for devising or excecuting scheme to defraud or obtain money, property, or services).

4.2.2 Chile

Éste fue el primer país latinoamericano en tipifica figuras penales relativas a la informática, mediante Ley Nº 19.223, denominada "***Ley contra los delitos informáticos"***, la cual entró en vigencia el 7 de junio de 1993, consta de cuatro artículos y son los siguientes artículos:

"Artículo 1° - El que maliciosamente **destruya o inutilice** un sistema de tratamiento de información o sus partes o sus componentes, o impida, obstaculice o modifique su funcionamiento, sufrirá la pena de presidio menor en su grado medio a máximo. Si como consecuencia de estas conductas se afectaren los datos contenidos en el sistema, se aplicará la pena señalada en el inciso anterior, en su grado máximo.

Artículo 2°.- El que con el ánimo de **apoderarse, usar o conocer** indebidamente de la información contenida en un sistema de tratamiento de la misma, lo intercepte, interfiera o acceda a él, será castigado con presidio menor en su grado medio.

Artículo 3°.- El que maliciosamente **altere, dañe o destruya los datos** contenidos en un sistema de tratamiento de información, será castigado con presidio menor en su grado medio.

Artículo 4°.- El que maliciosamente **revele o difunda los datos** contenidos en un sistema de información, sufrirá la pena de presidio menor en su grado medio. Si quien incurre en estas conductas es el responsable del sistema de información, la pena se aumentará en un grado"[10].

Según esta ley, la destrucción o inutilización de los de los datos contenidos dentro de una computadora es castigada con penas desde un año y medio a cinco años de prisión. Como no se estipula la condición de acceder a ese sistema, puede encuadrarse a los autores de virus. Si esa acción afectara los

[10] INSTITUTO NACIONAL DE ESTADISTICA E INFORMATICA (2001), pág. 58

datos contenidos en el sistema, la prisión se establecería entre los tres y los cinco años.

El hacking, definido como el ingreso en un sistema o su interferencia con el ánimo de apoderarse, usar o conocer de manera indebida la información contenida en éste, también es pasible de condenas de hasta cinco años de cárcel; pero ingresar en ese mismo sistema sin permiso y sin intenciones de ver su contenido no constituye delito.

Dar a conocer la información almacenada en un sistema puede ser castigado con prisión de hasta tres años, pero si el que lo hace es el responsable de dicho sistema puede aumentar a cinco años. Esta ley es muy similar a la inglesa aunque agrega la protección a la información privada.

4.2.3 Argentina

Mediante Ley Nº 26388[11] fue sancionada el 04 junio 2008, promulgada el 24 junio del 2008 y publicada el 25 junio 2008 mediante la cual efectúan diversas modificaciones e inserciones al Código Penal relacionadas con los delitos informáticos.

El Senado y Cámara de Diputados de la Nación Argentina reunidos en Congreso, etc. sancionan con fuerza de Ley:

Artículo 1.- Incorpórense como últimos párrafos del artículo 77 del Código Penal, los siguientes: El término "documento" comprende toda representación de actos o hechos, con independencia del soporte utilizado para su fijación, almacenamiento, archivo o transmisión. Los términos "firma" y "suscripción" comprenden la firma digital, la creación de una firma digital o firmar digitalmente. Los términos "instrumento privado" y "certificado" comprenden el documento digital firmado digitalmente.

Artículo 2.- Sustitúyese el artículo 128 del Código Penal, por el siguiente:

Artículo 128: Será reprimido con prisión de seis (6) meses a cuatro (4) años el que produjere, financiare, ofreciere, comerciare, publicare, facilitare, divulgare o distribuyere, por cualquier medio, toda representación de un menor de dieciocho (18) años dedicado a actividades sexuales explícitas o toda representación de sus partes genitales con fines predominantemente sexuales, al igual que el que organizare espectáculos en vivo de representaciones sexuales explícitas en que participaren dichos menores.

[11] http://abogadopoblete.blogspot.com/2008/06/ley-26388-delitos-informaticos-reforma.html

Será reprimido con prisión de cuatro (4) meses a dos (2) años el que tuviere en su poder representaciones de las descriptas en el párrafo anterior con fines inequívocos de distribución o comercialización. Será reprimido con prisión de un (1) mes a tres (3) años el que facilitare el acceso a espectáculos pornográficos o suministrare material pornográfico a menores de catorce (14) años.

Artículo 3.- Sustitúyese el epígrafe del Capítulo III, del Título V, del Libro II del Código Penal, por el siguiente: "Violación de Secretos y de la Privacidad"

Artículo 4.- Sustitúyese el artículo 153 del Código Penal, por el siguiente:

Artículo 153: Será reprimido con prisión de quince (15) días a seis (6) meses el que abriere o accediere indebidamente a una comunicación electrónica, una carta, un pliego cerrado, un despacho telegráfico, telefónico o de otra naturaleza, que no le esté dirigido; o se apoderare indebidamente de una comunicación electrónica, una carta, un pliego, un despacho u otro papel privado, aunque no esté cerrado; o indebidamente suprimiere o desviare de su destino una correspondencia o una comunicación electrónica que no le esté dirigida. En la misma pena incurrirá el que indebidamente interceptare o captare comunicaciones electrónicas o telecomunicaciones provenientes de cualquier sistema de carácter privado o de acceso restringido. La pena será de prisión de un (1) mes a un (1) año, si el autor además comunicare a otro o publicare el contenido de la carta, escrito, despacho o comunicación electrónica. Si el hecho lo cometiere un funcionario público que abusare de sus funciones, sufrirá además, inhabilitación especial por el doble del tiempo de la condena.

Artículo 5.- Incorpórase como artículo 153 bis del Código Penal, el siguiente: Artículo 153 bis: Será reprimido con prisión de quince (15) días a seis (6) meses, si no resultare un delito más severamente penado, el que a sabiendas accediere por cualquier medio, sin la debida autorización o excediendo la que posea, a un sistema o dato informático de acceso restringido. La pena será de un (1) mes a un (1) año de prisión cuando el acceso fuese en perjuicio de un sistema o dato informático de un organismo público estatal o de un proveedor de servicios públicos o de servicios financieros.

Artículo 6.- Sustitúyese el artículo 155 del Código Penal, por el siguiente: Artículo 155: Será reprimido con multa de pesos un mil quinientos ($ 1.500) a pesos cien mil ($ 100.000), el que hallándose en posesión de una

correspondencia, una comunicación electrónica, un pliego cerrado, un despacho telegráfico, telefónico o de otra naturaleza, no destinados a la publicidad, los hiciere publicar indebidamente, si el hecho causare o pudiere causar perjuicios a terceros. Está exento de responsabilidad penal el que hubiere obrado con el propósito inequívoco de proteger un interés público.

Artículo 7.- Sustitúyese el artículo 157 del Código Penal, por el siguiente: Artículo 157: Será reprimido con prisión de un (1) mes a dos (2) años e inhabilitación especial de un (1) a cuatro (4) años, el funcionario público que revelare hechos, actuaciones, documentos o datos, que por ley deben ser secretos.

Artículo 8.- Sustitúyese el artículo 157 bis del Código Penal, por el siguiente: Artículo 157 bis: Será reprimido con la pena de prisión de un (1) mes a dos (2) años el que: 1. A sabiendas e ilegítimamente, o violando sistemas de confidencialidad y seguridad de datos, accediere, de cualquier forma, a un banco de datos personales; 2. Ilegítimamente proporcionare o revelare a otro información registrada en un archivo o en un banco de datos personales cuyo secreto estuviere obligado a preservar por disposición de la ley. 3. Ilegítimamente insertare o hiciere insertar datos en un archivo de datos personales. Cuando el autor sea funcionario público sufrirá, además, pena de inhabilitación especial de un (1) a cuatro (4) años.

Artículo 9.- Incorpórase como inciso 16 del artículo 173 del Código Penal, el siguiente: Inciso 16. El que defraudare a otro mediante cualquier técnica de manipulación informática que altere el normal funcionamiento de un sistema informático o la transmisión de datos.

Artículo 10.- Incorpórase como segundo párrafo del artículo 183 del Código Penal, el siguiente: En la misma pena incurrirá el que alterare, destruyere o inutilizare datos, documentos, programas o sistemas informáticos; o vendiere, distribuyere, hiciere circular o introdujere en un sistema informático, cualquier programa destinado a causar daños.

Artículo 11.- Sustitúyese el artículo 184 del Código Penal, por el siguiente: Artículo 184: La pena será de tres (3) meses a cuatro (4) años de prisión, si mediare cualquiera de las circunstancias siguientes: 1. Ejecutar el hecho con el fin de impedir el libre ejercicio de la autoridad o en venganza de sus determinaciones; 2. Producir infección o contagio en aves u otros animales domésticos; 3. Emplear substancias venenosas o corrosivas; 4. Cometer el delito en despoblado y en banda; 5. Ejecutarlo en archivos, registros, bibliotecas, museos o en puentes, caminos, paseos u otros bienes de uso

público; o en tumbas, signos conmemorativos, monumentos, estatuas, cuadros u otros objetos de arte colocados en edificios o lugares públicos; o en datos, documentos, programas o sistemas informáticos públicos; 6. Ejecutarlo en sistemas informáticos destinados a la prestación de servicios de salud, de comunicaciones, de provisión o transporte de energía, de medios de transporte u otro servicio público.

Artículo 12.- Sustitúyese el artículo 197 del Código Penal, por el siguiente: Artículo 197: Será reprimido con prisión de seis (6) meses a dos (2) años, el que interrumpiere o entorpeciere la comunicación telegráfica, telefónica o de otra naturaleza o resistiere violentamente el restablecimiento de la comunicación interrumpida.

Artículo 13.- Sustitúyese el artículo 255 del Código Penal, por el siguiente: Artículo 255: Será reprimido con prisión de un (1) mes a cuatro (4) años, el que sustrajere, alterare, ocultare, destruyere o inutilizare en todo o en parte objetos destinados a servir de prueba ante la autoridad competente, registros o documentos confiados a la custodia de un funcionario público o de otra persona en el interés del servicio público. Si el autor fuere el mismo depositario, sufrirá además inhabilitación especial por doble tiempo. Si el hecho se cometiere por imprudencia o negligencia del depositario, éste será reprimido con multa de pesos setecientos cincuenta ($ 750) a pesos doce mil quinientos ($ 12.500).

Artículo 14.- Deróganse el artículo 78 bis y el inciso 1- del artículo 117 bis del Código Penal.

Artículo 15.- Comuníquese al Poder Ejecutivo. Dada en la sala de sesiones del congreso Argentino, en Buenos Aires, a los cuatro días del mes de Junio del año dos mil ocho. (Registrado bajo el N- 26.388 - Eduardo A. Fellner. - Julio C. C. Cobos. - Enrique Hidalgo. - Juan H. Estrada).

4.2.4 México

La ley penal mexicana, en la que mediante reformas legislativas de fecha 17 de mayo del 2000 publicadas en el Diario Oficial de la Federación, se crearon en la especie, los artículos 211 bis 1 al 211 bis 7 al Código Penal Federal[12], que en lo medular, tipifican comportamientos -de los llamados hackers o crackers- que atentan contra los sistemas de cómputo que pueden o no, ser parte del sector financiero mexicano. Este cuerpo normativo federal se sancionan el que un sujeto tenga acceso ilegal a dichos sistemas y los altere,

[12] INSTITUTO NACIONAL DE ESTADISTICA E INFORMATICA (2001), pág. 66-67

dañe, modifique o provoque pérdida de información contenida en tales sistemas, siendo los siguientes artículos:

Artículo 211 bis 1.- Al que sin autorización modifique, destruya o provoque ***pérdida de información contenida en sistemas o equipos de informática*** protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a dos años de prisión y de cien a trescientos días multa.

Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, se le impondrán de tres meses a un año de prisión y de cincuenta a ciento cincuenta días multa.

Artículo 211 bis 2.- Al que sin autorización modifique, destruya o provoque ***pérdida de información contenida en sistemas o equipos de informática del Estado***, protegidos por algún mecanismo de seguridad, se le impondrán de uno a cuatro años de prisión y de doscientos a seiscientos días multa. Al que sin autorización ***conozca o copie información*** contenida en sistemas o equipos de informática del Estado, protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a dos años de prisión y de cien a trescientos días multa.

Artículo 211 bis 3.- Al que estando ***autorizado para acceder a sistemas y equipos de informática del Estado,*** indebidamente modifique, destruya o provoque pérdida de información que contengan, se le impondrán de dos a ocho años de prisión y de trescientos a novecientos días multa. Al que estando autorizado para acceder a sistemas y equipos de informática del Estado, indebidamente copie información que contengan, se le impondrán de uno a cuatro años de prisión y de ciento cincuenta a cuatrocientos cincuenta días multa.

Artículo 211 bis 4.- Al que sin autorización ***modifique, destruya o provoque pérdida de información c***ontenida en sistemas o equipos de informática de las instituciones que integran el ***sistema financiero***, protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a cuatro años de prisión y de cien a seiscientos días multa. Al que sin autorización ***conozca o copie información*** contenida en sistemas o equipos de informática de las instituciones que integran el sistema financiero, protegidos por algún mecanismo de seguridad, se le impondrán de tres meses a dos años de prisión y de cincuenta a trescientos días multa.

Artículo 211 bis 5.- Al que ***estando autorizado para acceder a sistemas*** y equipos de informática de las instituciones que integran el **sistema**

financiero, indebidamente modifique, destruya o provoque pérdida de información que contengan, se le impondrán de seis meses a cuatro años de prisión y de cien a seiscientos días multa.

Al que estando autorizado para acceder a sistemas y equipos de informática de las instituciones que integran el sistema financiero, indebidamente copie información que contengan, se le impondrán de tres meses a dos años de prisión y de cincuenta a trescientos días multa. Las penas previstas en este artículo se incrementarán en una mitad cuando las conductas sean cometidas por funcionarios o empleados de las instituciones que integran el sistema financiero.

Artículo 211 bis 6.- Para los efectos de los artículos 211 bis 4 y 211 bis 5 anteriores, se entiende por instituciones que integran el sistema financiero, las señaladas en el artículo 400 bis de este Código.

Artículo 211 bis 7.- Las penas previstas en este capítulo se aumentarán hasta en una mitad cuando la información obtenida se utilice en provecho propio o ajeno.

En estos artículos se sanciona al que, sin autorización:

a) Modifique, destruya o provoque pérdida de información contenida en sistemas de informática protegidos por algún mecanismo de seguridad;

b) Conozca o copie dicha información. Se agravan las conductas anteriores si se tratare de sistemas de informática del Estado o de instituciones que integran el sistema financiero y más aún si el agente estuviere autorizado para acceder a los mismos o cuando la información obtenida se utilice en provecho propio o ajeno.

El software es considerado obra intelectual y, consecuentemente, recibe protección legal. Sin perjuicio de advertirse preocupación por el impacto de la alta tecnología en la comisión de delitos, ninguna de las legislaciones analizadas contempla íntegramente la problemática que la materia ofrece. No se prevé expresamente el fraude informático, aunque todas condenan el acceso ilegítimo a datos ajenos informatizados (hacking). La corta vigencia de las normas peruanas (2000) y mexicanas (1999) impiden hacer una evaluación precisa de la efectividad de las mismas. En este punto corresponde destacar las recomendaciones dadas en dos congresos internacionales. Estos son los de Río de Janeiro del año 1994, y del de Montevideo de 1998.

En el primero se distinguen distintos delitos que deben ser tipificados, como el fraude en la introducción alteración, o supresión de datos; las falsificaciones informáticas; los daños causados a datos o programas; el sabotaje informático; los accesos ilegítimos; la interceptación, reproducción no autorizada de un programa informático; etc. En el segundo, se analizó profundamente la cuestión de la responsabilidad penal emergente de estos delitos, el respeto por el principio de legalidad y la protección de la propiedad intelectual.

4.2.5 Colombia

El Código Penal colombiano expedido con la Ley Nº 599 del 2000, no hace referencia expresa a los delitos informáticos como tales; no obstante, en varias de sus normas recoge conductas que podrían entenderse incorporadas al concepto que la doctrina ha elaborado a este respecto.

Es recién con la Ley Nº 679 - 2001, publicado en el Diario Oficial 44509 de fecha 04 de agosto del 2001[13], el Estatuto para Prevenir y Contrarrestar La Explotación, la Pornografía y el Turismo Sexual con menores de edad. En Su Capitulo Segundo se refiere a las Redes Globales, donde tiene el objetivo de dictar medidas de protección contra la explotación, la pornografía, el turismo sexual y demás formas de abuso sexual con menores de edad, mediante el establecimiento de normas de carácter preventivo y sancionatorio, y la expedición de otras disposiciones en desarrollo del artículo 44 de la Constitución.

Asimismo, en el **Capitulo VII**, de la citada ley, se incluyen las medidas penales, en la cual realizan adiciones al Código Penal, siendo las siguientes:

"Artículo 33. Adiciónese el artículo 303 del Código Penal con el siguiente inciso. "Si el agente realizare cualquiera de las conductas descritas en este artículo con personas menores de catorce años por ***medios virtuales***, utilizando ***redes globales de información***, incurrirá en las penas correspondientes disminuidas en una tercera parte."

Parágrafo transitorio. Tan pronto como entre en vigencia la Ley 599 de 2000 el presente artículo tendrá el número 209.

Artículo 34. Adiciónese un nuevo artículo al Código Penal, con el número 312A, del siguiente tenor:

[13] http://www.ert.com.co/site/ley679-3agosto2001.pdf

Artículo 312A. Utilización o facilitación de medios de comunicación para *ofrecer servicios sexuales de menores*. El que utilice o facilite el correo tradicional, las redes globales de información, o cualquier otro medio de comunicación para obtener contacto sexual con menores de dieciocho (18) años, o para ofrecer servicios sexuales con éstos, incurrirá en pena de prisión de cinco (5) a diez (10) años, y multa de cincuenta (50) a cien (100) salarios mínimos legales mensuales vigentes.

Las penas señaladas en el inciso anterior se ***aumentarán hasta en la mitad*** (1/2) cuando las conductas se realizaren ***con menores de doce (12)*** años.

Parágrafo transitorio. Tan pronto como entre en vigencia la Ley 599 de 2000, el presente artículo tendrá el número 219A.

Artículo 35. Adiciónese un nuevo artículo al Código Penal, con el número 312B, del siguiente tenor:

Artículo 312B. *Omisión de denuncia*. El que, por razón de su oficio, cargo, o actividad, tuviere conocimiento de la utilización de menores para la realización de cualquiera de las conductas previstas en el presente capítulo y omitiere informar a las autoridades administrativas o judiciales competentes sobre tales hechos, teniendo el deber legal de hacerlo, incurrirá en multa de diez (10) a cincuenta (50) salarios mínimos legales mensuales vigentes.

Si la conducta se realizare por servidor público, se impondrá, además, la pérdida del empleo.

4.2.6 Costa Rica

El Código Penal costarricense de 1970, adiciona los artículos 196 bis, 217 bis y 229 bis, mediante Ley Nº 8131 de Administración Financiera de Costa Rica - Normas Relacionadas con la Delincuencia Informática de fecha 18 de septiembre del 2001[14], incorpora los siguientes artículos:

Artículo 110 - Hechos generadores de responsabilidad administrativa.

Además de los previstos en otras leyes y reglamentaciones propias de la relación de servicio, serán hechos generadores de responsabilidad administrativa, independientemente de la responsabilidad civil o penal a que puedan dar lugar, los mencionados a continuación:

[14] http://200.2.12.198/nede/files/archivos/LEY%208131%20DE%20ADMINISTRACION%20FINANCIERA%20DE%20COSTA%20RICA.doc.

m) El ingreso, por cualquier medio, a los sistemas informáticos de la Administración Financiera y de Proveeduría, sin la autorización correspondiente.

n) Obstaculizar el buen desempeño de los sistemas informáticos de la Administración Financiera y de Proveeduría, omitiendo el ingreso de datos o ingresando información errónea o extemporánea.

ñ) Causar daño a los componentes materiales o físicos de los aparatos, las máquinas o los accesorios que apoyan el funcionamiento de los sistemas informáticos de la Administración Financiera y de Proveeduría.

Artículo 111 - Delito informático.

Cometerán delito informático, sancionado con prisión de uno a tres años, los funcionarios públicos o particulares que realicen, contra los sistemas informáticos de la Administración Financiera y de Proveeduría, alguna de las siguientes acciones:

a) Apoderarse, copiar, destruir, alterar, transferir o mantener en su poder, sin el debido permiso de la autoridad competente, información, programas o bases de datos de uso restringido.

b) Causar daño, dolosamente, a los componentes lógicos o físicos de los aparatos, las máquinas o los accesorios que apoyan el funcionamiento de los sistemas informáticos.

c) Facilitar a terceras personas el uso del código personal y la clave de acceso asignados para acceder a los sistemas.

d) Utilizar las facilidades del sistema para beneficio propio o de terceros.

Artículo 114 - Responsabilidad civil.

Todo servidor público será responsable civil por los daños y perjuicios que ocasione, por dolo o culpa grave, a los órganos y entes públicos, independientemente de si existe con ellos relación de servicio. Tal responsabilidad se regirá por la Ley General de la Administración Pública y podrá surgir, sin que esa enumeración sea taxativa, por la comisión de alguno de los hechos contemplados en los Artículos 110 y 111 de la presente Ley.

Artículo 117 - Responsabilidad civil de particulares.

Además de lo preceptuado por la Ley Orgánica de la Contraloría General de la República, incurrirán en responsabilidad civil los particulares, sean personas físicas o jurídicas, que se beneficien con recursos públicos cuando estén involucrados en alguno de los supuestos de los Artículos 110 y 111.

Ley Número 8148, de fecha 24 de Octubre del 2001, para reprimir y sancionar los Delitos Informáticos[15]

Artículo 196 bis.-**Violación de comunicaciones electrónicas**. Será reprimida con pena de prisión de seis meses a dos años, la persona que, para descubrir los secretos o vulnerar la intimidad de otro, sin su consentimiento, se apodere, accese, modifique, altere, suprima, intercepte, interfiera, utilice, difunda o desvíe de su destino, mensajes, datos e imágenes contenidas en soportes: electrónicos, informáticos, magnéticos y telemáticos. La pena será de uno a tres años de prisión, si las acciones descritas en el párrafo anterior, son realizadas por personas encargadas de los soportes: electrónicos, informáticos, magnéticos y telemáticos."

Artículo 217 bis.-**Fraude informático**. Se impondrá pena de prisión de uno a diez años a la persona que, con la intención de procurar u obtener un beneficio patrimonial para sí o para un tercero, influya en el procesamiento o el resultado de los datos de un sistema de cómputo, mediante programación, empleo de datos falsos o incompletos, uso indebido de datos o cualquier otra acción que incida en el proceso de los datos del sistema."

Artículo 229 bis.-**Alteración de datos y sabotaje informático**. Se impondrá pena de prisión de uno a cuatro años a la persona que por cualquier medio accese, borre, suprima, modifique o inutilice sin autorización los datos registrados en una computadora. Si como resultado de las conductas indicadas se entorpece o inutiliza el funcionamiento de un programa de cómputo, una base de datos o un sistema informático, la pena será de tres a seis años de prisión. Si el programa de cómputo, la base de datos o el sistema informático contienen datos de carácter público, se impondrá pena de prisión hasta de ocho años.

4.2.7 Venezuela

El 30 de Octubre del 2001, es publicada en la Gaceta Oficial de la República Bolivariana de Venezuela Número 37.313, la Ley Número 48, ***Ley Especial contra Delitos Informáticos***,[16] la misma que significa un gran avance en materia penal para dicho país, lo que permitirá la protección de la tecnología de la información, persiguiendo todas aquellas conductas antijurídicas que se realicen en este campo. Como puede apreciarse en Venezuela se ha dado un paso importante en la legislación penal que regula los delitos informáticos pero que debe continuar con su evolución para enfrentar las exigencias de un

[15] http://delitosinformaticos.com/legislacion/costarica.shtml

[16] http://www.delitosinformaticos.com/legislacion/venezuela.shtml

mundo en proceso de globalización. Es por eso, que a continuación señalare los aspectos más importantes de la ley:

Objeto de la Ley: El objeto de la Ley se encuentra consagrado en el artículo 1 el cual establece: “La presente ley tiene por objeto la protección de los sistemas que utilicen tecnologías de información, así como la prevención y sanción de los delitos cometidos contra tales sistemas o cualquiera de sus componentes o los cometidos mediante el uso de dichas tecnologías, en los términos previstos en esta ley.” Asimismo, se puede inferir que la ley tiene como objetivos principales, 1) la protección de los sistemas de tecnologías de información; 2) prevención y sanción de los delitos cometidos contra tales sistemas; y 3) los delitos cometidos mediante el uso de dichas tecnologías.

Extraterritorialidad: La previsión de la Extraterritorialidad se encuentra señalado en su artículo 3, y el cual es de gran importancia en razón de la dimensión transnacional del problema pues se trata de hechos que pueden cometerse de un país a otro.

Sanciones: Para las sanciones se adopto simultáneamente el sistema binario, esto es, pena privativa de libertad y pena pecuniaria. Con relación a esta última se fijan montos representativos calculados sobre la base de unidades tributarias por considerarse que la mayoría de estos delitos, no obstante la discriminación de bienes jurídicos que se hace en el proyecto, afecta la viabilidad del sistema económico, el cual se sustenta, fundamentalmente, en la confiabilidad de las operaciones. Cabe destacar que el legislador tomó en cuenta las deficiencias de otras leyes donde no se preveían las penas accesorias. Así, en la ley encontramos que las penas para los hechos punibles que se encuentran tipificados son principales y accesorias.

Se establece como penas accesorias las siguientes:

- El decomiso de equipos, dispositivos, instrumentos, materiales, útiles, herramientas y cualquier otro objeto que haya sido utilizado para la comisión de los delitos.
- El trabajo comunitario.
- La inhabilitación para el ejercicio de funciones o empleos públicos, para el ejercicio de la profesión industria, o para laborar en instituciones o

empresas del ramo.

- La suspensión del permiso, registro o autorización para operar el ejercicio de cargos directivos y de representación de personas jurídicas vinculadas con el uso de tecnologías de información.
- Divulgación de la sentencia condenatoria.
- Indemnización civil a la víctima por los daños causados.

Responsabilidad de las Personas Jurídicas:

Por cuanto algunos de los hechos punibles previstos en la ley pueden ser perpetrados por intermedio de una persona jurídica o con el fin que ésta reciba sus efectos o beneficios, se establece los supuestos que harían procedente su responsabilidad, es así que los gerentes, administradores, directores o dependientes, actuando en su nombre o representación, responderán de acuerdo con su participación en el hecho punible.

Clasificación de los Delitos Informáticos:

Delitos contra los sistemas que utilizan tecnologías de Información

a. *Acceso indebido.* (Pena: Prisión de 4 a 8 años y multa de 400 a 800 Unidades Tributarias).
b. *Sabotaje o daño a sistemas*. (Pena: Prisión de 4 a 8 años y multa de 400 a 800 Unidades Tributarias).
c. *Sabotaje o daño culposo*. (Pena: se revisa el caso en concreto y se aplica una reducción entre la mitad y dos tercios).
d. *Acceso indebido o sabotaje a sistemas protegidos*. (Pena: las penas previstas anteriormente se aumentarán entre una tercera parte y la mitad cuando los hechos recaigan sobre un componente que utilice tecnología de información protegido con alguna medida de seguridad).
e. *Posesión de equipos o prestación de servicios de sabotaje*. (Pena: prisión de 3 a 6 años y multa de 300 a 600 Unidades Tributarias).
f. *Espionaje informático*. (Pena: prisión de 4 a 8 años y multa de 400 a 800 Unidades Tributarias).
g. *Falsificación de documentos*. (Pena: prisión de 3 a 6 años y multa de 300 a 600 Unidades Tributarias).

Delitos contra la propiedad

a. *Hurto*. (Pena: prisión de 2 a 6 años y multa 200 a 600 Unid. Tribu.).
b. *Fraude*. (Pena: prisión de 3 a 7 años y multa de 300 a 700 Unid. Tribu.).
c. *Obtención indebida de bienes y servicios*. (Pena: prisión de 2 a 6 años y multa de 200 a 600 Unidades Tributarias).
d. *Manejo fraudulento de tarjetas inteligentes o instrumentos análogos*. (Pena: prisión 5 a 10 años y multa de 500 a 1000 Unidades Tributarias).
e. *Apropiación de tarjetas inteligentes o instrumentos análogos*. (Pena: prisión de 1 a 5 años y multa de 10 a 50 Unidades Tributarias).
f. *Provisión indebida de bienes o servicios*. (Pena: prisión de 2 a 6 años y multa de 200 a 600 Unidades Tributarias).
g. *Posesión de equipo para falsificaciones*. (Pena: prisión de 3 a 6 años y multa de 300 a 600 Unidades Tributarias).

Delitos contra la privacidad de las personas y de las comunicaciones

a. *Violación de la privacidad de la data o información de carácter personal*. (Pena: prisión de 2 a 6 años y multa de 200 a 600 Unidades Tributarias).
b. *Violación de la privacidad de las comunicaciones*. (Pena: prisión de 2 a 6 años y multa de 200 a 600 Unidades Tributarias).
c. *Revelación indebida de data o información de carácter personal*. (Pena: prisión de 2 a 6 años y multa de 200 a 600 Unidades Tributarias).

Delitos contra niños, niñas o adolescentes

a. *Difusión o exhibición de material pornográfico*. (Pena: prisión de 2 a 6 años y multa de 200 a 600 Unidades Tributarias).
b. *Exhibición pornográfica de niños o adolescentes*. (Pena: prisión de 4 a 8 años y multa de 400 a 800 Unidades Tributarias).

Delitos contra el orden económico

a. *Apropiación de propiedad intelectual*. (Pena: prisión de 1 a 5 años y multa de 100 a 500 Unidades Tributarias).
b. *Oferta Engañosa*. (Pena: prisión de 1 a 5 años y multa de 100 a 500 Unidades Tributarias).

4.3 Análisis de las legislaciones penales y leyes especiales sobre delitos informáticos en los países de Europa y América

A continuación analizaremos las legislaciones penales y leyes especiales relacionadas con los delitos informáticos tanto en Europa como en América, los cuales han sido tratados anteriormente; asimismo, nos va a permitir tener mayor conocimiento de como viene haciendo frente en la actualidad esta nueva forma de criminalidad, motivo por el cual con la finalidad de realizar el análisis del caso hemos dividido esta nueva forma de criminalidad en cinco campos para un mejor análisis, los cuales se indican a continuación:

1. **Delitos contra los sistemas informáticos:**
   a. Acceso indebido
   b. Sabotaje informático
   c. Espionaje informático.
   d. Falsificación de documentos
   e. Distribución de virus

2. **Delitos contra la propiedad:**
   a. Hurto, fraude
   b. Obtención indebida de bienes y servicios
   c. Manejo fraudulento de tarjetas inteligentes o instrumentos análogos
   d. Apropiación de tarjetas inteligentes o instrumentos análogos
   e. Provisión indebida de bienes o servicios

3. **Delitos contra la privacidad de las personas y de las comunicaciones:**
   a. Violación de la privacidad de la data o información de carácter personal
   b. Violación de la privacidad de las comunicaciones
   c. Revelación indebida de data o información de carácter personal
   d. Calumnia, injuria, intimidad

4. **Delitos contra menores (niños, niñas y adolescentes)**
   a. Difusión o exhibición de material pornográfico
   b. Exhibición pornográfica de niños o adolescentes

5. **Delito contra el orden económico y patrimonio**
   a. Apropiación de propiedad intelectual
   b. Oferta Engañosa

4.3.1 Países europeos que han legislado sobre delitos informáticos

PAÍSES	1. Delitos contra los sistemas	2. Delitos contra la propiedad	3. Delitos contra la privacidad	4. Delito contra menores	5. Delito contra el orden financiero
Alemania	X	X	----	----	---
Austria	X	X	----	----	---
Francia	X	X	----	----	---
Inglaterra	X	X	----	----	---
Holanda	X	X	X	----	---
España	X	X	X	X	X
Portugal	X	X	X	----	---

Interpretación de la legislación sobre delitos informáticos en países europeos

PRIMERO: Es importante precisar con relación a la forma que han optado los países europeos con la finalidad de hacer frente a esta nueva forma de criminalidad como son los denominados delitos informáticos, países como Alemania, Austria, Francia, España y Portugal han optado por adicionar e incluir dentro de sus respectivos códigos penales artículos relacionados éstos delitos; asimismo, Alemania, Austria y Francia dentro de sus respectivos códigos penales han incluido solo a los delitos que afectan a los sistemas informáticos y la propiedad. España y Portugal han incluido aparte de los delitos antes mencionados delitos contra la privacidad.

SEGUNDO: Por otro lado, Inglaterra a optado por crear una ley especial para hacer frente a esta nueva forma de criminalidad, en la cual ha legislado sobre delitos que afectan a los sistemas informáticos y la propiedad; asimismo, de igual forma Holanda a optado por crear una ley especial para hacer frente a esta nueva forma de criminalidad, en la cual trata sobre delitos que afectan a los sistemas informáticos, la propiedad y la privacidad.

TERCERO: Es importante mencionar que todos los países europeos materia de estudio en el presente trabajo de investigación han legislado en materia de delitos informáticos sobre delitos contra los sistemas informáticos y contra el patrimonio; asimismo, de igual forma es importante indicar que países como Alemania, Austria, Francia e Inglaterra son los que menos han legislados para hacer frente a esta nueva forma de criminalidad.

CUARTO: Finalmente los países europeos materia de análisis en el presente trabajo de investigación, España, es el que más ha legislado sobre delito informático e incluido dentro de su respectivo código penal delitos que afectan a los sistemas informáticos, la propiedad, la privacidad, contra menores y contra el orden financiero entre otros; asimismo, España es el país europeo que sanciona más severamente esta nueva forma de criminalidad.

4.3.2 Países americanos que han legislado sobre delitos informáticos

PAÍSES	1. Delitos contra los sistemas	2. Delitos contra la propiedad	3. Delitos contra la privacidad	4. Delito contra menores	5. Delito contra el orden financiero
EE.UU.	X	X	----	----	---
Chile	X	X	X	----	---
Argentina	X	X	----	----	---
México	X	X	----	----	X
Colombia	X	X	X	X	---
Costa Rica	X	X	X	----	X
Venezuela	X	X	X	X	X

PRIMERO: Al respecto podemos apreciar con relación a la forma de que han optado los países de América con la finalidad de hacer frente a esta nueva forma de criminalidad países como Argentina, México, Colombia y Costa Rica, han optado por adicionar e incluir dentro de sus respectivos códigos penales artículos relacionados éstos delitos; asimismo, países como Estados Unidos, Chile y Venezuela han legislado a través de leyes especiales.

.

SEGUNDO: Por otro lado, es importante indicar que la República de Venezuela es el país que ha optado por crear una ley especial contra los delitos informáticos incluyendo en la citada ley delitos que afectan a los sistemas informáticos, la propiedad, la privacidad, contra menores y contra el orden financiero; asimismo, tanto las penas y sanciones económicas son altas en relación a los demás países de América; asimismo, de igual forma los Estados Unidos a través del Acta Federal de Abuso Computacional, solo trata sobre delitos contra los sistemas de información y delitos contra la propiedad, imponiendo sanciones severas.

TERCERO: Es importante mencionar que todos los países americanos de estudio en el presente trabajo de investigación ha legislado en materia de delitos informáticos con relación a los delitos contra los sistemas informáticos y contra el patrimonio; asimismo, de igual forma es importante indicar que países como EE.UU, Argentina y México son los que menos han legislados para hacer frente a esta nueva forma de criminalidad.

CUARTO: De las legislaciones de países americanos materia de análisis en el presente trabajo de investigación, la República de Venezuela es el país que más ha legislado sobre delitos a través de una ley especial para hacer frente a esta nueva forma de criminalidad; asimismo, los países que sancionan más drásticamente esta nueva forma de criminalidad en América son los Estados Unidos y Venezuela.

4.4 Organismos Internacionales que han legislado sobre Delitos Informáticos

A continuación trataremos a algunos instituciones internacionales como la Organización de Cooperación y Desarrollo Económico, la Organización de las Naciones Unidas y la Comunidad Europea, instituciones que han legislado con la finalidad de hace frente al constante incremento de esta nueva forma de criminalidad, como es la criminalidad informática, los cuales nos van a servir como un referente a fin de que nuestros legisladores, en caso de opten por realizar una legislación especial contra los delitos informáticos como lo realizó en América del Sur la República de Venezuela.

En tal sentido es importante precisar que tanto los organismos e instituciones internacionales, vienen legislando a través de los años sobre delitos informáticos con la finalidad de hace frente a esta nueva forma de criminalidad, por ello indicamos la importancia de tratar estas normas internacionales.

4.4.1 Organización de Cooperación y Desarrollo Económico (OCDE)

En 1983, inició un estudio de la posibilidad de aplicar y armonizar en el plano internacional las leyes penales a fin de luchar contra el problema del uso indebido de los programas computarizados, siendo publicado en 1986 el informe titulado “Delitos Informáticos análisis de la normativa jurídica”.

Asimismo, es importante indicar que los principales delitos tratados por la legislación existente a nivel europeo así como a nivel nacional son los siguientes:[17]

- **Delitos contra la intimidad:** recogida, almacenamiento, modificación, revelación o difusión ilegales de datos personales.
- **Delitos relativos al contenido:** difusión, especialmente por Internet, de pornografía, y en especial de pornografía infantil, declaraciones racistas e información que incita a la violencia.
- **Delitos económicos,** acceso no autorizado y sabotaje: muchos países han aprobado leyes que abordan los delitos económicos perpetrados por ordenador y tipifican nuevos delitos relacionados con el acceso no autorizado a sistemas informáticos (por ejemplo, la piratería, el sabotaje informático y la distribución de virus, el espionaje informático, y la falsificación y el fraude informáticos).

[17] http://europa.eu/legislation_summaries/justice_freedom_security/fight_against_organised_crime/l33193b_es.htm

- **Delitos contra la propiedad intelectual:** delitos contra la protección jurídica de programas de ordenador y la protección jurídica de las bases de datos, los derechos de autor y derechos afines.

4.4.2 Organización de las Naciones Unidas (ONU)

En el marco del Octavo congreso sobre Prevención del Delito y Justicia Penal, celebrado en 1990 en la Habana, Cuba se dijo que la delincuencia relacionada con la informática era consecuencia del mayor empleo del proceso de datos en las economías y burocracias de los distintos países y que por ello se había difundido la comisión de actos delictivos.

Con fecha 28 noviembre 2002 la Organización de las Naciones[18] publica los tipos de delitos informáticos reconocidos por Naciones Unidas, entre las cuales tenemos a las siguientes:

a. Fraudes cometidos mediante manipulación de computadoras:

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

Manipulación de programas: Es muy difícil de descubrir y a menudo pasa inadvertida debido a que el delincuente debe tener conocimientos técnicos concretos de informática. Este delito consiste en modificar los programas existentes en el sistema de computadoras o en insertar nuevos programas o nuevas rutinas. Un método común utilizado por las personas que tienen conocimientos especializados en programación informática es el denominado Caballo de Troya, que consiste en insertar instrucciones de computadora de forma encubierta en un programa informático para que pueda realizar una función no autorizada al mismo tiempo que su función normal.

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

[18] http://lac.derechos.apc.org/cdocs.shtml?x=8325

para codificar información electrónica falsificada en las bandas magnéticas de las tarjetas bancarias y de las tarjetas de crédito.

Manipulación informática aprovechando repeticiones automáticas de los procesos de cómputo: Es una técnica especializada que se denomina "técnica del salchichón" en la que "rodajas muy finas" apenas perceptibles, de transacciones financieras, se van sacando repetidamente de una cuenta y se transfieren a otra.

b. Falsificaciones informáticas

Como Objeto: Cuando se alteran datos de los documentos almacenados en forma computarizada.

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

c. Daños o modificaciones de programas o datos computarizados

Sabotaje Informático: Es el acto de borrar, suprimir o modificar sin autorización funciones o datos de computadora con intención de obstaculizar el funcionamiento normal del sistema. Las técnicas que permiten cometer sabotajes informáticos son:

Virus: Es una serie de claves programáticas que pueden adherirse a los programas legítimos y propagarse a otros programas informáticos. Un virus puede ingresar en un sistema por conducto de una pieza legítima de soporte lógico que ha quedado infectada, así como utilizando el método del Caballo de Troya.

Gusanos: Se fabrica de forma análoga al virus con miras a infiltrarlo en programas legítimos de procesamiento de datos o para modificar o destruir los datos, pero es diferente del virus porque no puede regenerarse. En términos médicos podría decirse que un gusano es un tumor benigno, mientras que el virus es un tumor maligno. Ahora bien, las consecuencias del ataque de un gusano pueden ser tan graves como las del ataque de un virus: por ejemplo, un programa gusano que subsiguientemente se destruirá puede dar instrucciones a un sistema informático de un banco para que transfiera continuamente dinero a una cuenta ilícita.

Bomba lógica o cronológica: Exige conocimientos especializados ya que requiere la programación de la destrucción o modificación de datos en un momento dado del

futuro. Ahora bien, al revés de los virus o los gusanos, las bombas lógicas son difíciles de detectar antes de que exploten; por eso, de todos los dispositivos informáticos criminales, las bombas lógicas son las que poseen el máximo potencial de daño. Su detonación puede programarse para que cause el máximo de daño y para que tenga lugar mucho tiempo después de que se haya marchado el delincuente. La bomba lógica puede utilizarse también como instrumento de extorsión y se puede pedir un rescate a cambio de dar a conocer el lugar en donde se halla la bomba.

Acceso no autorizado a servicios y sistemas informáticos: Por motivos diversos: desde la simple curiosidad, como en el caso de muchos piratas informáticos (hackers) hasta el sabotaje o espionaje informático.

Piratas informáticos o hackers: El acceso se efectúa a menudo desde un lugar exterior, situado en la red de telecomunicaciones, recurriendo a uno de los diversos medios que se mencionan a continuación. El delincuente puede aprovechar la falta de rigor de las medidas de seguridad para obtener acceso o puede descubrir deficiencias en las medidas vigentes de seguridad o en los procedimientos del sistema. A menudo, los piratas informáticos se hacen pasar por usuarios legítimos del sistema; esto suele suceder con frecuencia en los sistemas en los que los usuarios pueden emplear contraseñas comunes o contraseñas de mantenimiento que están en el propio sistema.

Reproducción no autorizada de programas informáticos de protección legal: Esta puede entrañar una pérdida económica sustancial para los propietarios legítimos. Algunas jurisdicciones han tipificado como delito esta clase de actividad y la han sometido a sanciones penales. El problema ha alcanzado dimensiones transnacionales con el tráfico de esas reproducciones no autorizadas a través de las redes de telecomunicaciones modernas. Al respecto, consideramos, que la reproducción no autorizada de programas informáticos no es un delito informático debido a que el bien jurídico a tutelar es la propiedad intelectual.

La Conferencia de la ONU sobre Comercio y Desarrollo (UNCTAD)[19] con fecha 12 de junio, 2009 propuso a los países latinoamericanos que los problemas legales que surjan del uso de las nuevas tecnologías de la información y la comunicación se aborden en conjunto. En un nuevo informe, el organismo revisó y comparó las leyes y decretos de 11 de los Estados miembros de la Asociación Latinoamericana de Integración (ALADI). Señaló que ante el creciente uso de esas tecnologías se requieren nuevas normas y regulaciones y una reforma de algunas existentes.

[19] http://www.un.org/spanish/News/fullstorynews.asp?newsID=15793&criteria1=Latina&criteria2=internet

Esto es sumamente importante para los empresarios de los países en desarrollo que cada vez más hacen negocios por Internet, y para los gobiernos que brindan servicios electrónicos a sus ciudadanos, afirmó la UNCTAD. El estudio compara legislación en materia, entre otras, de protección de la privacidad y datos personales, delitos informáticos y spam, firma digital y contratos electrónicos. Subrayó que los países de ALADI han reformado o están en el proceso de adaptar sus leyes y regulaciones civiles, comerciales, penales, fiscales y administrativas. Finalmente es importante precisar que en algunos casos, observó que se deberán incrementar los esfuerzos, por ejemplo: la situación en México, donde 32 estados han adoptado regulaciones diferentes.

4.4.3 Unión Europea

Con la finalidad de mejorar la seguridad de las infraestructuras de la información, la Comisión de la Unión Europea, ha estudiado los distintos caminos que podría emprender con el fin de prevenir los delitos informáticos y luchar contra ellos. Asimismo, cabe precisar que el desarrollo de las nuevas tecnologías de la información y la comunicación dan lugar a profundos cambios en la economía y en la sociedad. El éxito de la sociedad de la información es decisivo para el crecimiento, la competitividad y la creación de empleos en Europa. Esta es la razón por la que la Comisión lanzó la Iniciativa en Europa en diciembre de 1999, cuyo objetivo era permitir a la Unión Europea utilizar todas las posibilidades. El plan de acción global sobre esta Iniciativa, aprobado por el Consejo Europeo de Feira en junio de 2000, destaca la importancia de la seguridad de las redes y de la lucha contra los delitos informáticos. Al mismo tiempo, esta importancia creciente de las infraestructuras de información y comunicación abre nuevos caminos a conductas delictivas. Esta es la razón por la que la Unión Europea ya lanzó una serie de medidas para luchar contra el contenido ilícito y perjudicial en Internet con el fin de proteger los derechos de la propiedad intelectual y los datos de carácter personal, promover el comercio electrónico y reforzar la seguridad en las transacciones.

Motivo por el cual con fecha 25 de mayo de 2001 en la ciudad de Estrasburgo, se publica el Convenio Preliminar Sobre Delitos Informáticos y Memorando Explicativo Correspondiente, la misma que fue preparado por el Comité Especial de Expertos sobre Delitos relacionados con el empleo de Computadoras (PC-CY) Presentado ante: Comité Europeo para los Problemas de la Delincuencia (CDPC) en su 50ª sesión plenaria (18-22 de junio de 2001).

De igual forma con fecha 27 de agosto del 2002 la Unión Europea publica en su Diario Oficial N° 203 la Propuesta de Decisión Marco del Consejo relativa a los ataques de los que son objeto los sistemas de información[20] COM/2002/0173 final - CNS 2002/008621, cabe precisar que la presente Decisión Marco tiene por objeto reforzar la cooperación entre las autoridades judiciales y las otras autoridades competentes, incluida la policía y los otros servicios especializados encargados de la aplicación de la ley en los Estados miembros, mediante la aproximación de su legislación penal en materia de ataques contra los sistemas de información.

Los artículos de la Decisión Marco del Consejo relativa a los ataques que son objeto los sistemas informáticos, en síntesis se trata con relación al Acceso ilegal a los sistemas de información; intromisión ilegal en los sistemas de información; Inducción, complicidad y tentativa; Sanciones; Circunstancias agravantes; Circunstancias particulares, Responsabilidad de las personas jurídicas; Sanciones penales de las personas jurídicas; Competencia e Intercambio de información.

Adicionalmente con fecha 16 de marzo del 2005, la Unión Europea publica en su Diario Oficial N° 069 Decisión Marco 2005/222/JAI del Consejo, de 24 de febrero de 2005, relativa a los ataques contra los sistemas de información[22], se ha tomando en cuenta entre los considerandos el objeto de la presente Decisión marco es reforzar la cooperación entre las autoridades judiciales y otras autoridades competentes, incluida la policía y los demás servicios represivos especializados de los Estados miembros, mediante la aproximación de su legislación penal en materia de ataques contra los sistemas de información. Es así que se ha comprobado la existencia de ataques contra los sistemas de información, en particular como consecuencia de la amenaza de la delincuencia organizada, y crece la inquietud ante la posibilidad de ataques terroristas contra sistemas de información que forman parte de las infraestructuras vitales de los Estados miembros. Esto pone en peligro la realización de una sociedad de la información segura y de un espacio de libertad, seguridad y justicia, y por tanto exige una respuesta por parte de la Unión Europea.

Los artículos de la Decisión Marco del Consejo relativa a los ataques que son objeto los sistemas informáticos, se ha legislado con relación al igual Acceso ilegal a los sistemas de información, Intromisión ilegal en los sistemas de información, Intromisión ilegal en los datos, Inducción, complicidad y tentativa, Sanciones,

[20] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52002PC0173:ES:HTML

[22] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32005F0222:ES:HTML

Circunstancias agravantes, Responsabilidad de las personas jurídicas, Sanciones aplicables a las personas jurídicas, Competencia, Intercambio de información y Aplicación.

Con fecha 14 de julio 2008, la Comisión de las Comunidades Europeas, presenta su Informe de la Comisión al Consejo basado en el artículo 12 de la Decisión Marco del Consejo, de 24 de febrero de 2005, relativa a los ataques contra los sistemas de información /* COM/2008/0448 final[23]. Cabe precisar que el presente Informe ha llegado a las presentes conclusiones:

Grado de aplicación: El presente informe ofrece una primera visión general de la aplicación de la Decisión Marco por los Estados miembros. Se confirma la amplia diversidad de modalidades de incorporación de las normas penales a los ordenamientos de los Estados miembros y la dificultad subsiguiente de evaluar globalmente la legislación nacional si no se puede analizar la forma en que ésta se aplica en la práctica. La Comisión constata que la Decisión Marco está aún en fase de transposición en algunos Estados miembros. Se han registrado notables progresos en prácticamente los 20 Estados miembros evaluados en el presente informe, y se estima que el grado de aplicación es relativamente satisfactorio. Obviamente, la preocupación principal de la Comisión se centra en los siete Estados miembros que todavía no han comunicado ninguna medida de transposición. La Comisión ruega a los Estados miembros que todavía no han incorporado la Decisión Marco a sus ordenamientos nacionales que pongan remedio a esta situación a la mayor brevedad. La Comisión también ruega a los Estados miembros que procedan a revisar sus legislaciones en un esfuerzo mayor por combatir los ataques contra los sistemas de información.

Evolución futura: Desde la adopción de la Decisión Marco, los recientes ataques sufridos en toda Europa han puesto de manifiesto las diversas amenazas que están apareciendo y, en particular, los ataques simultáneos y masivos contra los sistemas de información y la creciente utilización delictiva de los denominados botnets. Estos ataques no centraban la atención en el momento de aprobación de la Decisión Marco. En respuesta a esta situación, la Comisión considerará la adopción de medidas que respondan mejor a la amenaza que representan los botnets. Estas medidas podrán sancionar como infracción penal determinadas actividades que facilitan el uso delictivo de botnets y prever sanciones mínimas más severas para los delitos consistentes en ataques masivos y especialmente peligrosos contra los sistemas de información. La Comisión también está considerando adoptar medidas

[23] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2008:0448:FIN:ES:HTML

para fomentar el uso eficaz y oportuno de los puntos de contacto operativos las 24 horas del día todos los días de la semana, a los que se refiere el artículo 11.

Los graves incidentes ocurridos en 2007 han puesto de manifiesto la necesidad de adoptar medidas comunes rápidas —que a menudo implican a los operadores privados— a nivel internacional para hacer frente a los ataques masivos contra los sistemas de información. Para lograr una mejor coordinación y coherencia del mecanismo de respuesta, los Estados miembros deberán considerar la conveniencia de seguir utilizando los mismos puntos de contacto que utilizan las redes del Consejo de Europa y del G8. La Comisión considerará la posibilidad de establecer directrices comunitarias sobre la utilización de las diversas redes internacionales para combatir la delincuencia de alta tecnología.

4.5 Conclusiones generales del Capítulo

Primero: Luego de realizar el estudio de la legislación comparada, hemos podido apreciar que se vienen tipificación esta nueva forma de criminalidad, con la finalidad de hacer frente a estos delitos de nueva data denominados delitos informáticos, en tal sentido países europeos como Alemania, España, Francia, Portugal y Austria han adicionado en sus respectivos códigos penales a estos delitos de nueva data y países como Inglaterra y Holanda han promulgado leyes especiales contra los delitos informáticos; asimismo, los países americanos como Argentina, Colombia, Costa Rica, Chile y México han adicionado en sus respectivos códigos penales a los delitos informáticos y países como Estados Unidos y Venezuela han optado por crear leyes especiales para hacer frente a los delitos informáticos.

Segundo: De igual forma, al estudiar como vienen haciendo frente a esta nueva forma de criminalidad, por parte de los organismos internacionales como la Organización de Cooperación y Desarrollo Económico, la Organización de las Naciones Unidas y la Comunidad Europea, hemos podido apreciar que las citadas organismos vienen haciendo denodados esfuerzos con la finalidad de hacer frente a los delitos informáticos, legislando y dando unas pautas con la finalidad de contrarrestas la incidencia de éstos delitos, como es el caso del Consejo Europeo, que ha logrado que los países miembros incluyan

dentro de su respectiva legislación nacional normas que les permitan hacer frente a los delitos informáticos.

Tercero: Es importante precisar el aporte de la Organización de Cooperación y Desarrollo Económico, quienes han realizado estudios para hacer frente a esta nueva forma de criminalidad, lo cual ha permitido identificar los delitos informáticos con la finalidad de hacerles frente; asimismo, los delitos informáticos afectan a los bienes jurídicos como la intimidad, relativos al contenido, económicos y contra la propiedad intelectual.

Cuarto: De igual forma es importante el aporte de la Organización de las Naciones Unidas, al realizar diversos congresos con la finalidad de hacer frente a los delitos informáticos, lo cual le ha permitido publicar los diversos tipos de delitos informáticos entre los cuales tenemos a los fraudes cometidos mediante manipulación de computadoras, falsificaciones informáticas y daños o modificaciones de programas o datos computarizados.

Quinto: Finalmente, hemos podido apreciar de los países europeos y americanos que sancionan drásticamente a los delitos informáticos; han utilizado simultáneamente el sistema binario, esto es, pena privativa de la libertad y pena pecuniaria, como son Estados Unidos, España y la República de Venezuela, a comparación con nuestro país, como se puede apreciar en el cuadro que se indica a continuación:

PAÍSES	**1. Delitos contra los sistemas**	**2. Delitos contra la propiedad**	**3. Delitos contra la privacidad**	**4. Delito contra menores**	**5. Delito contra el orden financiero**
EE.UU.	Pena: Hasta 10 años Multa: según caso	Pena: Hasta 10 años Multa: según caso	----	----	---
Venezuela	Pena: 3 a 8 años Multa: 300 a 800 UT	Pena: 2 a 10 años Multa: 200 a 1000 UT	Pena: 2 a 6 años Multa: 200 a 600 UT :	Pena: 2 a 8 años Multa: 200 a 800 UT	Pena: 1 a 5 años Multa: 100 a 500 UT
España	Pena:1 a 6 años Multa: según caso	Pena:2 a 5 años Multa: según caso	Pena:6 m. a 6 años Multa: según caso	Pena: 1 a 3 años Multa: según caso	Pena:1 a 6 años Multa: según caso
Perú	Pena:3 a 5 años Multa: 60 a 90 días Servicios com. hasta 104 jornadas	----	----	Pena: 4 a 6 años Multa: 265 días	----

CAPÍTULO V:

VERIFICACIÓN DE LA HIPÓTESIS

5.1 Contrastación de las hipótesis

A continuación efectuaremos la contrastación de las hipótesis del presente trabajo de investigación hemos podido confirmar lo siguiente:

PRIMERO: De lo investigado se ha podido confirmar, que desde la aparición del Internet, el desarrollo tecnológico, la informática y la telemática se viene incrementando en forma alarmante la comisión de los denominados delitos informáticos y en la actualidad nuestra legislación penal vigente resulta deficiente, motivo por el cual urge realizar una reforma por parte de los legisladores debido a que se ha incluido en forma poco acertada dentro del Código Penal a los delitos informáticos, dentro de los delitos contra el patrimonio, como si estos delitos informáticos solo afectan el patrimonio; por lo antes expuesto se puede apreciar que, en la actualidad los legisladores se encuentran en la disyuntiva de seguir incluyendo a estos delitos de nueva data dentro de los tipos penales ya existente o crear una ley especial contra los delitos informáticos, como lo han realizado otros países y organizaciones internacionales.

Asimismo, el incremento se debe en muchos casos al difícil control y falta de peritos informáticos y especialistas en esta nueva forma de criminalidad parte de los efectivos policiales, jueces y fiscales; de igual forma el poco conocimiento de estas nuevas formas de criminalidad han originado un caos social, debido a que estos delitos afectan diversos bienes jurídicos protegidos como son el patrimonio, el honor, la intimidad, la libertad informática, la vida el cuerpo y salud, los derechos de autor, el orden económico entre otros.

SEGUNDO: De igual forma se ha podido confirmar que el incremento de la piratería informática se debe al avance de la tecnología, informática, telemática e Internet, lo cual origina que nuestra legislación penal sea deficiente, originando desprotección a los derechos de autor y patrimonio; asimismo, existe desconocimiento de esta nueva forma de criminalidad informática por parte las autoridades competentes, aunado a la existencia de un mercado negro donde se efectúa el tráfico de diversos programas informáticos, lo cual origina grandes pérdidas económicas.

TERCERO: Hemos podido apreciar que el incremento de los delitos realizados por medios informáticos, telemática e Internet, se han incrementado afectando en algunos casos contra la vida el cuerpo y la salud, especialmente en menores de edad, debido a lo vulnerables que son frente a los peligros del Internet, el uso de la red sirve en muchos casos para difundir pornografía, asesinatos, violencia, agresión y suicidio, exponen a nuestra población de niños, que están en la etapa más vulnerable de su vida, a una serie de estímulos que aún son incapaces de manejar y discriminar como nocivos para su salud mental, originado la muerte de algunos menores inducidos directamente por Internet.

CUARTO: Finalmente, en el presente trabajo de investigación se ha podido confirmar que el incremento de la pornografía infantil por Internet se debe al avance tecnológico, falta de control por parte de los padres en caso de menores de edad y aunado a la inoperancia de las autoridades competentes y la deficiente legislación penal vigente, originando el incremento de delitos que atentan contra el pudor, honor y la Intimidad de menores de edad quienes son los más vulnerables; asimismo, influyen directamente en el incremento de la pornografía infantil, la falta de prevención, la extrema pobreza, la escasa denuncia por parte de los agraviados, debido a que en muchos casos los menores de edad son amedrentados por sus agresores con la finalidad que no le cuenten lo que sucede a sus respectivos padres.

5.2 Estudio de casos relacionado con los delitos informáticos

Para mejor ilustración del presente trabajo de investigación analizaremos cuatro casos actuales, relacionados con esta nueva forma de criminalidad, los cuales se han sido realizados en sede nacional, los cuales serán analizados en forma cabal y rigurosa, los cuales se indican a continuación:

Caso Nº 01: Tres detenidos en Perú por extorsionar con el sello falso de ETA (03/09/2008)[1]

Tres personas han sido detenidas en Perú por extorsionar a empresas en España con el sello falso de ETA, informó la Policía Nacional española. La "Operación Clínica", que han llevado a cabo las policías española y peruana, comenzó después de que más de 50 empresarios españoles denunciaran haber recibido amenazas, presuntamente de la banda armada, si no abonaban 3.000 euros.

Tras estas denuncias, agentes del grupo de secuestros y extorsiones de la Policía Nacional se desplazaron a Lima, donde comenzaron las pesquisas en colaboración con la División de Investigación de Secuestros y la División de Investigación de Alta Tecnología peruanas. El seguimiento policial comenzó en julio pasado tras recibirse en una clínica de estética española un mensaje en el que se solicitaba un depósito de 3.000 euros bajo amenazas al propietario y a su familia en nombre de ETA.

A ésta siguieron otras misivas similares, acompañadas de fotografías de cadáveres, a empresas de transporte y turismo. En las cartas se instaba a remitir el dinero a través de una empresa de envío de dinero al extranjero. Una vez descartada la autoría de ETA (..) los agentes averiguaron desde un primer momento que el lugar de procedencia de dichos mensajes era la ciudad de Lima', dijo una nota de prensa de la Policía Nacional.

En Lima, los agentes localizaron la ubicación exacta de los terminales informáticos desde los que se remitían los mensajes amenazantes, todos ellos de diversos locutorios de Internet en el distrito 'Los Olivos' del norte de la capital peruana. Para intentar cobrar el dinero, los extorsionadores llegaron a captar en Internet a personas que viajaran a España para realizar unos cobros simulando ser proveedores de productos de belleza. Dos de los cobradores fueron interceptados en Madrid y ambos declararon que fueron contratados a través de un programa de mensajería instantánea a través de Internet por parte de una empresa de belleza que les instaba a cobrar pedidos en varias ciudades españolas. Finalmente, las detenciones en Perú

[1] http://www.20minutos.es/noticia/408975/0/ESPANA/PERU/DETENIDOS/

pudieron realizarse gracias al seguimiento de las direcciones IP de los ordenadores desde donde se remitían los mensajes.

A manera de análisis relacionado con el presente caso, podemos apreciar que estos delitos de nueva data, son delitos transfonterizos, debido a que estos actos delictivos se pueden realizar entre dos o más países; los delincuentes informáticos enviaron mensajes a través de cabinas de Internet desde los Olivos - Lima a empresarios españoles, donde los amedrentaban y extorsionaban indicando que eran el grupo terrorista ETA, donde se les solicitaba que se depositen en cuentas de los delincuentes la suma de 3,000 euros. Asimismo, al ser estos ilícitos de nueva data es importante la colaboración internacional por parte de la Policía Nacional española, quienes tienen experiencia para combatir estas nuevas formas de criminalidad, quienes con un apoyo de la División de Delitos de Alta Tecnologías, luego de un seguimiento por más de tres meses se pudo hacer un exhaustivo seguimiento de las direcciones IP de los ordenadores desde donde se remitían los mensajes.

Caso Nº 02: Capturan a 'Elegante' por extorsionar a mujeres con videos pornográficos en Internet (07/02/2010)[2]

Carlos Ricardo Jave Luyo (31), “el elegante”, fue apresado por la Policía, acusado de haber captado 27 jovencitas a través de Internet, a quienes prostituyó, filmó y colgó sus videos pornográficos en el ciberespacio para luego extorsionarlas con la finalidad de quitar las imágenes de la red.

Según informó el diario 'Trome', este sujeto fue detenido en la cuadra 16 de la avenida Arenales, en Lince, cuando cobraba 400 dólares a una joven para retirar sus imágenes del ciberespacio; además, le estaba solicitando favores sexuales.

Una mujer de 20 años contó a los policías que fue captada a través de la página Hi5.com por una supuesta empresaria llamada 'Eva', quien le ofreció trabajo como 'dama de compañía' por lo cual le iban a pagar 200 soles para tener relaciones sexuales con hombres de clase A-1. "Me dijeron que yo tenía que pagar un buen hotel porque los 'clientes' no se iban a exponer y luego del encuentro sexual me pagarían, pero nunca me pagaron. A las tres semanas me llamó un sujeto y me dijo que abriera una página de Internet e iba a ver una sorpresa. Luego vi que las imágenes del encuentro sexual estaban colgadas en www.gratisblog.com/agencia-eva-vip/", contó la agraviada cuya identidad se guarda en reserva.

[2] http://www.peru.com/noticias/portada20100207/79893/Capturan-a-Elegante-por-extorsionar-a-mujeres-con-videos-pornograficos-en-Internet

Los policías comprobaron que Carlos Jave se contactaba con la agraviada y le ofrecía hablar con 'Eva' para borrar definitivamente las imágenes, pero a cambio debía pagar 500 dólares. Primero borró el video, pero como la muchacha no le pagó volvió a colgarlo y le exigió 400 dólares. Además de sus favores sexuales. Los policías hallaron un USB con el cual descubrieron que Carlos y 'Eva' eran la misma persona.

En el presente caso podemos apreciar como los delincuentes informáticos son jóvenes y tienen un amplio conocimiento en informática y tecnologías de la información, mediante el cual se dedican a captar a jovencitas a través de Internet, con la finalidad de sacarles provecho, en algunos casos las obligan a prostituir, las filman y posteriormente cuelga los videos pornográficos en el ciberespacio para luego extorsionarlas con la finalidad de quitar las imágenes de la red. Estos tipos de casos en la actualidad son poco denunciados debido a que existe falta de conocimiento y por parte de las agraviadas; asimismo, es importante mencionar que estos actos delictivos son pluriofensivos debido a que afectan el patrimonio, extorsión, honor e intimidad de las personas agraviadas.

Caso Nº 03: Capturan peruano estafador por Internet (02/02/2010)[3]

En Roldanillo, Valle (Colombia) el peruano Wilfredo Beltrán, enamoraba por internet a decenas de mujeres mayores de 40 años para estafarlas. Este peruano de 58 años conocido como "Willy" por sus víctimas. se presentaba como un piloto de guerra combatiente en Africa, y con una gran fortuna, de esta manera contactaba a mujeres preferiblemente viudas o jubiladas que estuviesen a punto de recibir dinero, y después de estafarlas las maltrataba.

Las autoridades colombianas tienen información que en los últimos cuatro años llegó a estafar a mujeres de las ciudades colombianas de Cali, Barranquilla, Cartagena, Santa Marta y Bogotá, así como de localidades de Perú, Ecuador, Panamá, Brasil y Venezuela. Todo el dinero que consiguió por las estafas realizadas a mujeres incautas, le ayudó instalar un local de venta de ceviche (diversos platos de cocina a base de pescado o mariscos frescos) en Roldanillo donde fue capturado.

Wilfredo Beltran, será procesado judicialmente en Colombia por los delitos de extorsión, violencia intrafamiliar, hurto calificado y estafa. Nuevamente una alerta

[3] http://artigoo.com/capturado-peruano-estafador-por-internet

para abrir bien los ojos, y no estar divulgando información por Internet; así como tampoco estar confiando en todo lo que por aquí se dice, ya que "No todo lo que brilla es oro", pero infortunadamente cuando se hacen estas advertencias muchas personas no la toman en cuenta, para después sufrir las consecuencias.

En el presente caso podemos apreciar la diversidad de beneficios que traen consigo el avance de las tecnología y el Internet; asimismo, como pueden ser utilizados por delincuentes informáticos con la finalidad de realizar diversos delitos como son: la extorsión, violencia intrafamiliar, hurto calificado y estafa, entre otros, debiendo tener mucho cuidado todas las personas al momento de utilizar el Internet, saber exactamente con quien uno tiene contacto en el ciberespacio; por tanto es un rol importante de los padres quienes tienen el deber y la obligación de controlar y tener mucho cuidado cuando sus menores hijos se encuentren navegando por Internet, instruyéndolos constantemente con medidas y precauciones al memento de estar en el Internet.

Caso Nº 04 Pornografía infantil por Internet - Fingía ser mujer para captar a menores (02/06/2010)[4]

Desde hace un año, Alan Anthony Honorio Delgado (26), estudiante de Ingeniería Agroindustrial, se hacía llamar Ericka y utilizaba el e-mail ericka_swayne@hotmail, quién a través del software ‘fake web cam’, engañaba a menores edad mostrando la imagen de una mujer desnuda que, aparentemente, conversaba con ellos. Así lograba convencerlos de que realizaran actos sexuales para grabarlos en su computadora.

Después de un tiempo, Ericka volvía a contactarse con ellos, pero esta vez les exigía, bajo amenazas, que volvieran a hacer los mismos actos. Si no lo hacían, les advertía, las imágenes de sus primeros encuentros serían enviadas a sus padres y compañeros de estudios.

La captura de Alan Honorio se dio tras la denuncia de dos alumnos de 12 años de un prestigioso colegio de Miraflores. Otros tres estudiantes de la misma edad figuran entre sus víctimas. La Policía incautó su PC y, según la pericia psicológica que se le hizo, tuvo como resultado que el denunciado padece de un trastorno en su conducta sexual.

Alan Honorio será acusado por los delitos contra la libertad, en la modalidad de

[4] http://peru21.pe/noticia/488848/fingia-mujer-captar-menores

ofensas al pudor y pornografía infantil a través de Internet, así como contra el patrimonio, en la modalidad de chantaje y extorsión. De momento se desconoce si comercializaba las imágenes.

En el presente caso podemos apreciar que el sujeto activo del delito de pornografía infantil, ha realizado la comisión del delito contra la libertad, en la modalidad de ofensas al pudor y pornografía infantil a través de Internet, para lo cual ha utilizado el Internet, el MSN y otro software llamado 'fake web cam' mediante el cual el delincuente informático engaña a los menores edad, mostraba la imagen de una mujer desnuda que aparentemente, conversaba con ellos. Así lograba convencerlos de que realizaran actos sexuales para grabarlos en su computadora.

Asimismo, es importante precisar que esta nueva forma de criminalidad afectan diversos bienes jurídicos protegidos por tanto son delitos son pluriofensivos, como es en el presente caso materia de análisis el delito contra la libertad, en la modalidad de ofensas al pudor y pornografía infantil a través de Internet, así como contra el patrimonio, en la modalidad de chantaje y extorsión.

Finalmente a manera de conclusión general relacionados con los casos de delitos informáticos antes mencionados, debemos precisar que actualmente urge la intervención por parte del Estado con la finalidad que se capacite a los efectivos de la policía nacional, jueces y fiscales quienes deben contar con especialistas en delitos informáticos, informática forense y peritajes informático, con la finalidad que al momento de investigar tanto la policía, los jueces y fiscales cuenten con los elementos de prueba necesarios a fin de que la investigación se realice de forma eficaz y eficiente, debido a que se encuentra en juego la libertada de una persona que se presume inocente hasta que no se le pruebe lo contrario, motivo por el cual con la finalidad de que no se realicen excesos por falta de conocimiento de los operadores de justicia, y origine que se prive de la libertad injustamente.

5.3 Interpretación de los resultados y estadísticas

Con la finalidad de recolectar datos que nos muestren la opinión y la cercanía de los especialistas en sistemas informáticos con los Delitos Informáticos, se aplicó una encuesta a empleados tanto de empresas privadas como nacionales cuya labor diaria involucre el uso de sistemas informáticos.

Al desarrollar el presente trabajo de investigación se ha considerado un universo cuantitativo de 44 personas: 10 policías, 05 fiscales, 05 jueces, 24 abogados especialistas en Derecho Penal, a quienes se les aplicó como instrumento de opinión un cuestionario, el cual fue respondido en su totalidad.

Cabe precisar que luego de acopiar, clasificar y analizar los datos obtenidos con la aplicación del cuestionario se constató que el conocimiento que poseen los encuestados, acerca de los delitos informáticos denominados de nueva data, es relativo e insuficiente, debido a la poca producción bibliográfica por parte de los autores nacionales e internacionales. Cabe precisar que los encuestados han demostrado tener cierto conocimiento del tema, dando importantes aportes para el desarrollo del presente trabajo de investigación.

A continuación se detalla cada pregunta de la encuesta que se aplicó, así como su respectivo tratamiento estadístico:

1. **A la pregunta:** ¿Considera usted que a través de las computadoras, el Internet y la informática se pueden realizar algunos delitos?

Análisis de Frecuencias

Sí	44	100%
No	0	0%
Total respuestas	**44**	**100%**

Interpretación

Se pudo contrastar al 100% de los encuestados respondieron que a través de la computadora, el Internet y la informática se pueden realizar delitos, llamados Delitos Informáticos, demostrando tener los encuestados un cierto conocimiento relacionada con esta nueva forma de criminalidad.

2. **A la pregunta:** ¿Considera usted que la aparición del Internet y el desarrollo de la tecnología e informática han ocasionado el incremento de los delitos informáticos?

Análisis de Frecuencias

Si	44	100%
No	0	0%
Total respuestas	**44**	**100%**

Interpretación

En la presente pregunta se puede apreciar que el 100% de los encuestados afirman que la aparición del Internet y desarrollo de las tecnologías han permitido que se incrementen los delitos informáticos.

3. **A la pregunta:** ¿Qué tipos de delitos informáticos, conoce usted?

Análisis de Frecuencias

Delitos Informáticos	Total de respuestas	Total de respuestas (%)	Total de casos
Piratería	27	42	61,4
Pornografía	14	22	31,8
Robo	10	16	22,7
Virus	13	20	29,5
Total	**64**	**100**	**145,4**

Interpretación

La mayoría de los encuestados con relación a los tipos de delitos informáticos que conocen, se pudo apreciar que el 61,4% considera que uno de los delitos más incidentes es la piratería, luego la pornografía con el 31,8%, el virus con el 29,5% y por último el robo con el 22,7%, estos porcentajes nos dan una idea clara del acerca del porcentaje de delitos que origina esta nueva forma de criminalidad.

4. **A la pregunta:** ¿Cuáles de estos delitos considera que son los menos denunciados?

Análisis de Frecuencias

Delitos Informáticos	Total de respuestas	Total de respuestas (%)	Total de casos
Piratería	27	38	61,4
Pornografía	14	19	31,8
Robo	14	19	31,8
Virus	10	14	22,7
Ninguno	7	10	15,9
Total	**72**	**100**	**163,6**

Interpretación

Los encuestados, en su gran mayoría (61,4%) afirman que uno de los delitos informáticos menos denunciados es la piratería, seguida de la pornografía y el robo con el 31,8% cada uno, el virus con el 22,7% y sólo el 15,9% considera que ningún delito informático es menos denunciado.

5. **A la pregunta:** ¿Según usted qué y/o a quiénes afectan más los delitos informáticos?

Análisis de Frecuencias

Afectados	Total de respuestas	Total de respuestas (%)	Total de casos
A la persona	41	27	93,2
A la intimidad	27	18	61,4
Al patrimonio	34	23	77,3
A la información	34	23	77,3
Otros	14	9	31,8
Total	**150**	**100**	**341,0**

Interpretación

Con relación a que o quienes afectan esta nueva forma de criminalidad los encuestados en su gran mayoría, esto es el 93,2% han manifestado que consideran que los más afectados por los delitos informáticos es la persona, mientras que un 61,4% considera que es la intimidad, el 77,3% considera que es el patrimonio y la información y finalmente, el 31,8% del total de encuestados considera que los más afectados son otros.

6. **A la pregunta:** ¿Quiénes considera que son los más afectados por los delitos informáticos?

Análisis de Frecuencias

Afectados	Total de respuestas	Total de respuestas (%)
Persona	7	15,9%
Empresa	14	31,8%
Empresa y persona	20	45,5%
Otros	3	6,8%
Total respuestas	**44**	**100,0%**

Interpretación

Con relación a quienes son los más afectados por los delitos informáticos, se puede apreciar, el 45,5% de los encuestados consideran que los más afectados por los delitos informáticos son las empresas y las personas, mientras que el 31,8 considera que los son las sólo empresas, el 15,9% considera que es sólo la persona y el 6,8% considera que son otros.

7. **A la pregunta:** ¿Según usted, qué delitos pueden ser cometidos a través de medios informáticos (computadora, Internet, sistemas informáticos)?

Análisis de Frecuencias

Delitos	**Total de respuestas**	**Total de respuestas (%)**	**Total de casos**
Vida	10	6	22,7
Intimidad	44	27	100,0
Patrimonio	34	21	77,3
Secuestro	10	6	22,7
Contra la fe pública	24	15	54,5
Terrorismo	30	19	68,2
Otros	10	6	22,7
Total respuestas	**162**	**100**	**368,1**

Interpretación

En la presente pregunta se puede apreciar que el 100% de los encuestados coincide en que delitos contra la intimidad pueden ser cometidos a través de medios informáticos y la minoría, esto es, el 22,7% considera que a través de medios informáticos se pueden cometer delitos contra la vida, el cuerpo y la salud así como secuestros.

8. **A la pregunta:** ¿Durante su experiencia en esta actividad de la computación e informática, cómo se han presentado estos delitos?

A través de esta pregunta antes mencionada se obtuvieron respuestas muy diversas, todas ellas de suma de suma importancia para el desarrollo del presente trabajo, es por esta razón que se ha optado por citar las mencionadas respuestas:

- Copiando información sin consentimiento del autor
- Generalmente en algunas links de las webs
- Se presente por cracker que ingresa al sistema
- Cuando el hacker encuentra un enlace en la red abierta e insegura.
- Copia y venta de software
- Obtención de claves de cuentas bancarias mediante engaño
- Mediante el robo de tiempo
- A través de los correos
- Cuando te invitan a visualizar información ingresan los virus a tu sistema operativo.

Como se puede apreciar a través de las respuestas de los encuestados, se evidencia haber enfrentado en algún momento a esta nueva forma de criminalidad.

09. **A la pregunta:** ¿Por qué cree usted que algunos delitos informáticos tienden a quedarse impunes?

A la pregunta antes mencionada los encuestados respondieron:

- Por falta de pruebas
- Por falta de tipificación
- Por falta de autoridades especializadas
- Por falta de tecnología y apoyo del gobierno
- Por los culpables utilizan técnicas para no ser ubicados, no registrándose
- Realizan copias para su uso personal
- No existe una legislación sobre seguridad informática
- Por desconocimiento de las personas
- No son denunciados

Es importante precisar que los encuestados, pese a que no son especialistas en esta nueva forma de criminalidad, a través de sus respuestas se puede apreciar que conocen muy de cerca el problema de la impunidad de los delitos informáticos.

10. **A la pregunta:** ¿Considera usted, que dentro de nuestro Código Penal, los delitos informáticos más frecuentes se dan en el orden económico o patrimonial?

Análisis de Frecuencias

No	17	39%
Sí	24	54%
Depende	3	7%
Total	**44**	**100%**

Interpretación

Al respecto, los encuestados con relación a que en nuestro Código Penal, los delitos informáticos más frecuentes se dan en el orden económico o patrimonial, desde su óptica señalan lo siguiente: El 39% señala que no es económico o patrimonial, el 54% señala que si es económico o patrimonial, y por último sólo el 7% señala que depende de otros factores, con lo que se puede apreciar la pluralidad de bienes jurídicos afectados por esta nueva forma de criminalidad.

11. **Ante la pregunta:** ¿De qué manera se presenta el delito informático en el trabajo que usted realiza?

Los encuestados respondieron de la siguiente manera:

- Transferencias bancarias
- Piratería de música, video y software
- Por medio de Craker
- En centros de labores manejan información privada, donde atentan contra la intimidad de los trabajadores
- Virus y material pornográfico

Los encuestados al responder la pregunta antes mencionada, nos ha permitido demostrar que el personal encuestado, tiene cierto conocimiento y experiencia respecto a la forma de como se realizan estos ilícitos.

12. Ante la pregunta: ¿Qué aportes puede usted brindar que ayuden a contrarrestar los delitos informáticos?

Los encuestados respondieron:

- Mayor restricción a usuarios y mejor seguridad
- Tener en cuenta que los correos y webs no son seguros
- Aplicar penas severas
- Denunciar estos tipos de delitos
- Control más estricto por parte de las autoridades
- Tener una buena formación sobre seguridad informática
- Legislar de acuerdo a los avances tecnológicos y formar policías especializados
- Deben de realizarse estudios respecto al tema
- Controlar a su menor hijo cuando ingresen al Internet

Los encuestados al momento de indicar sus aportes, han demostrado su preocupación debido a que estos delitos de nueva data se vienen incrementando y en muchos casos afectan a los menores de edad quienes son los más vulnerables.

5.4 Análisis general del cuestionario de preguntas

A continuación procederemos a realizar un análisis general del cuestionario de preguntas efectuado a los diversos encuestados como son: jueces, fiscales, efectivos policiales y abogados, de donde en términos generales, hemos podido rescatar diversos aportes que servirán como aporte al presente trabajo de investigación, lo cual nos va a permitir apreciar cual es la situación actual y conocimiento relacionada con estos delitos de nueva data como son los delitos informáticos y a continuación mencionaremos los puntos mas resaltantes los mismos que se indican a continuación:

Primero: Se ha podido establecer según las respuestas de los encuestados, cuentan con cierto conocimiento del tema materia de investigación, indicando que a través de la computadora, el Internet y la informática se pueden realizar los delitos informáticos; asimismo, precisaron que la aparición del Internet y desarrollo de las tecnologías han permitido que se incrementen éstos delitos.

Segundo: Los encuestados entre sus respuestas relacionadas con la forma como se presentan los delitos informáticos en sus centros de trabajo indicaron que los citados delitos se presentan a través de las transferencias bancarias, la piratería de música, video y software, por medio del Craker, información privada, donde atentan contra la intimidad de los trabajadores, y finalmente los virus y material pornográfico, demostrando los encuestados tener un cierto conocimiento relacionado con la criminalidad informática.

Tercero: Por otro lado, es de suma importancia mencionar los aportes brindados por los encuestados, siendo los mas importantes a tomar en cuenta para el presente trabajo de investigación: tener mayor restricción a usuarios y mejor seguridad, tener en cuenta que los correos y webs no son seguros, aplicar penas severas, denunciar estos tipos de delitos, tener un control estricto por parte de las autoridades, tener una buena formación sobre seguridad informática, legislar de acuerdo a los avances tecnológicos, formar policías especializados y finalmente controlar a sus menores hijos cuando ingresen al Internet.

Cuarto: De igual forma es importante mencionar que según la apreciación de los encuestados, se pudo establecer que la mayoría de los delitos informáticos inciden en el orden económico o patrimonial; asimismo, se pudo apreciar que los más afectados por esta nueva forma de criminalidad son las personas y las empresas; finalmente los encuestados indicaron que los delitos contra la intimidad son los que más incidencia tienen por esta nueva forma de criminalidad y que pueden ser realizados por Internet y medios informáticos.

Es importante precisar que los aportes antes mencionados deben ser tomados en cuenta por parte de los congresistas debido a que son ellos quienes tienen como función legislar con relación a estos delitos de nueva data, con la finalidad de que nuestra legislación penal este acorde con los avances de la ciencia y tecnología; asimismo, los padres de familia deben de tener mayor control sobre sus menores hijos quienes son los más vulnerables ante esta nueva forma de criminalidad.

Quinto: Finalmente, es importante tener en cuenta que según la apreciación de los encuestados, con relación a los delitos menos denunciados indicaron que son los siguientes: la piratería, la pornografía y el robo informático, cabe precisar que con relación a la piratería informática, a todas luces es éste el delito menos denunciado en nuestro país por parte de los agraviados; de igual forma la pornografía por Internet son poco denunciados debido a la falta de conocimiento y el temor de los agraviados a que tomen represalias en contra de su persona; asimismo, con relación a los robos informáticos, parte de la falta de denuncias se debe al desconocimiento en caso de personas naturales y en caso de las personas jurídicas, como son las entidades bancarias, no formulan denuncias debido a que afectaría a la reputación de su entidad y acarrearía la perdida de clientes.

CONCLUSIONES Y RECOMENDACIONES

CONCLUSIONES

Después de haber analizado y estudiado ampliamente a los Delitos Informáticos en el Código Penal, hemos arribado a las siguientes conclusiones:

PRIMERA: El avance científico y tecnológico han acarreado aspectos positivos e importantes en nuestra sociedad en los últimos tiempos, motivo por el cual la interpretación tradicional de los delitos en nuestro código penal han quedado desfasados ante la aparición de estos delitos de nueva data como es la criminalidad informática.

SEGUNDO: Actualmente no existe una definición unánime de los *"Delitos Informáticos"*, por parte de los juristas nacionales y extranjeros, motivo por el cual a nuestro parecer la denominación más apropiada a estos delitos de nueva data es la de "C*riminalidad Informática"*, debido a que estos ilícitos son una nueva forma de criminalidad.

TERCERA: Que, estos delitos de nueva data son delitos *pluriofensivos***,** debido a que afectan a más de un bien jurídico protegido, con son el patrimonio, el honor, la intimidad, el pudor, el orden económico, la libertad informática, la vida el cuerpo entre otros, los cuales afectan gravemente el normal desenvolvimiento y desarrollo de nuestra sociedad.

CUARTA: Nos parece poco acertada la inclusión de los "Delitos Informáticos" como un Capítulo dentro del Título de los Delitos Contra el Patrimonio en nuestro Código Penal, lo cual permite colegir que solo existen *Delitos Informáticos Contra el Patrimonio*, no ajustándose a la realidad, debido a que la gama esta nueva forma de criminalidad afecta a diversos bienes jurídicos protegidos como el patrimonio, el honor, la intimidad, el pudor, la libertad Informática, la vida el cuerpo y la salud, etc.

QUINTA: Para poder regular jurídicamente en sede penal, estos nuevos ilícitos, los legisladores han tomado en cuenta la *Teoría del Bien Jurídico Protegido*, debido a que estos delitos afectan tanto a un bien jurídico individual, como un bien jurídico colectivo, como son los derechos personales, patrimoniales y económicos.

SEXTA: La naturaleza virtual e intangible de esta nueva forma de criminalidad, origina confusión al momento efectuarse su tipificación, al realizar las investigaciones por parte de la Policía Nacional; asimismo en la actualidad los jueces y fiscales, cuentan cono poco conocimiento y experiencia en el manejo de esta área del Derecho Informático con la finalidad de enfrentar a esta nueva forma de criminalidad.

SETIMA: La ocurrencia de esta nueva forma de criminalidad tanto en el ámbito nacional e internacional, es *un reto para los profesionales del Derecho y la Informática*; asimismo, el nuestro Código Penal al hacer frente a esta nueva forma de criminalidad, es *escasa y benigna,* debido a que no se sancionan esta nueva forma de criminalidad de manera ejemplar, en comparación a las legislaciones penales de otros países, como son los Estados Unidos, España y Venezuela.

OCTAVO: Finalmente hemos podido apreciar que en la actualidad son escasos los procesos penales relacionados con los delitos informáticos, los mismos que se encuentran tipificados en nuestro Código Penal vigente en los artículos 207º "A", 207º "B" y 207º "C" los cuales fueron incorporados en nuestro Código Penal vigente mediante Ley Nº 27309 "Ley que incorpora los Delitos Informáticos en el Código Penal" de fecha 17 de julio del 2000, motivo por el cual cabría la derogatoria de los artículos antes mencionados y que se efectúe un estudio minucioso de los tipos penales que pueden ser realizados por medios informáticos del Código Penal vigente, los cuales deben ser agravados debido al impacto que ocasiona en nuestra sociedad.

RECOMENDACIONES

En esta oportunidad nos permitimos recomendar las siguientes situaciones, extraídos de la experiencia en la elaboración del presente objeto de estudio.

PRIMERA: Es preciso resaltar que el desarrollo de los avances tecnológicos, y en particular la informática, posibilitan el acopio de gran cantidad de información, de distinta índole, aparición de bases de datos públicas y privadas, almacenadas en soporte magnético, discos de lectura y otros, susceptible de tratamiento, intermediación, marketing, intercambio, por tanto constituyéndose en una industria portentosa, por lo que urge establecer los pilares para la regulación y protección de los datos personales con la finalidad de salvaguardar el derecho a la información e intimidad de las personas.

SEGUNDA: Incentivar a los alumnos de la **FACULTAD DE DERECHO** y en especial la **ESCUELA DE POST GRADO – MAESTRÍA EN DERECHO PENAL** de ésta casa de estudios a que realicen diplomados, conferencias, foros, seminarios, relacionados con el Derecho Informático y en especial con relación a esta nueva forma de criminalidad, con el fin de poder contar con una doctrina y jurisprudencia; y así poder efectuar una adecuada tipificación en nuestra legislación penal sin tener que remitirnos a copiar normas extranjeras, que no van de acuerdo con nuestra realidad y el desarrollo tecnológico de nuestro país.

TERCERO: Crear en la Facultad de Derecho de esta casa de estudios un **DEPARTAMENTO DE DERECHO INFORMÁTICO**, donde estén comprometidos alumnos, ex alumnos y catedráticos, con el finalidad de desarrollar y llevar a cabo investigaciones respecto a esta nueva disciplina del Derecho como es el Derecho Informático, lo cual beneficiará a todos los profesionales del Derecho; así como a los peritos informáticos, debido a que el citado Departamento servirá como un centro de perfeccionamiento para hacer frente al desarrollo de las nuevas tecnologías y el incremento de esta nueva forma de criminalidad; asimismo, se debe de gestionar el apoyo de entidades e instituciones tanto nacionales como internacionales con la finalidad de hacer realidad la implementación del Departamento de Derecho Informático.

CUARTA: Se recomiendo encarecidamente crear conciencia a los usuarios; así como los padres de familia, personas mayores y menores de edad que el Internet, así como las redes de información, los correos y paginas web, no son lo suficientemente seguros para guardar información íntima y confidencial, debido a que son demasiados vulnerables a causa del avances de las tecnologías de la información, informática y telemática.

QUINTO: Se recomienda que tanto a través de las autoridades del gobierno central, regional y local, utilicen los medios y mecanismos necesarios con la finalidad de prevenir y restringir el acceso a menores de edad a las diversas cabinas públicas de Internet; asimismo, todas las computadores de las cabinas de Internet deben de contar con bloqueadores que no permitan el ingresar a páginas webs pornográficas, con la finalidad que no efectúe la visualización de las paginas Web pornográficas por parte de menores de edad.

SEXTO: Finalmente recomendamos que los legisladores deroguen los artículos 207º "A", 207º "B" y 207º "C" incorporados mediante la Ley Nº 27309 "Ley que incorpora los Delitos Informáticos en el Código Penal" de fecha 17 de julio del 2000, debido a que en la actualidad son escasos los procesos penales en sede judicial; asimismo, se recomienda que se efectúe una revisión minuciosa al Código Penal vigente, con la finalidad de que se tipifique adecuadamente esta nueva forma de criminalidad.

PROPUESTA

PROPUESTA

A continuación luego de haber realiza el presente trabajo de investigación y expuesto las conclusiones y recomendaciones correspondientes, es importante precisar debido a la inaplicación de la Ley que incorpora los Delitos Informáticos en el Código Penal, motivo por el cual amerita que se efectúe una propuesta legislativa con la finalidad de derogar la Ley Nº 27309 "Ley que incorpora los Delitos Informáticos en el Código Penal" de fecha 17 de julio del 2000.

EXPOSICIÓN DE MOTIVOS

Mediante Ley Nº 27309 "Ley que incorpora los Delitos Informáticos en el Código Penal" de fecha 17 de julio del 2000, se adiciona al Título V del Código Penal vigente, el Título X denominado Delitos Informáticas, entre ellos el Espionaje Informático en el artículos 207º "A", el Sabotaje Informático en el artículo 207º "B" y las agravantes en el artículo 207º "C".

En la actualidad son escasos los procesos penales relacionados con los delitos informáticos que se encuentran tipificados en nuestro Código Penal vigente, específicamente en el artículo 207º "A", 207º "B" y 207º "C", hecho que originaría que la Ley Nº 27309 sea una ley penal en blanco, debido a que no estaría cumpliendo su función; asimismo, es importante precisar que la ley penal se estructura sobre la base del precepto y de la sanción. Si se dan los requisitos establecidos en el precepto, entonces procede la aplicación de la sanción, hecho que no ocurre en los artículos que materia de derogación.

Por tanto, en resguardo del normal desenvolvimiento de la sociedad, la vida constitucional y democrática del país y a efecto de mejorar la normatividad relacionada con esta nueva forma de criminalidad, el Poder Legislativo considera pertinente derogar la Ley Nº 27309 "Ley que incorpora los Delitos Informáticos en el Código Penal".

ANÁLISIS COSTO BENEFICIO

La presente iniciativa legislativa no generará costo alguno al Tesoro Público. Por el contrario, resulta beneficiosa para el país por cuanto permitirá que se realice un adecuado análisis de la materia que regula la norma cuya derogatoria se propone.

IMPACTO DE LA NORMA EN LA LEGISLACIÓN NACIONAL

El presente proyecto de ley propone la derogatoria de la Ley Nº 27309 "Ley que incorpora los Delitos Informáticos en el Código Penal".

Proyecto de Ley

LEY QUE DEROGA LA LEY Nº 27309

Artículo 1.- Objeto
Deróguese la Ley Nº 27309 "Ley que incorpora los Delitos Informáticos en el Código Penal" de fecha 17 de julio del 2000.

Artículo 2.- Vigencia
La presente Ley entrará en vigencia al día siguiente de su publicación en el diario oficial El Peruano.

Comuníquese al señor Presidente de la República para su promulgación.

En Lima, a los ……. días del mes de setiembre del dos mil diez.

CESAR ZUMAETA FLORES
Presidente del Congreso de la República

WILSON MICHAEL URTECHO
Segundo Vicepresidente del Congreso de la República

AL SEÑOR PRESIDENTE CONSTITUCIONAL DE LA REPÚBLICA

POR TANTO:

Mando se publique y cumpla.

Dado en la Casa de Gobierno, en Lima a los ……. días del mes de setiembre del dos mil diez.

ALAN GARCIA PEREZ
Presidente Constitucional de la República

JAVIER VELASQUEZ QUESQUEN
Presidente del Consejo de Ministros

VICTOR GARCIA TOMA
Ministro de Justicia

BIBLIOGRAFÍA

1. BIBLIOGRAFÍA BÁSICA

1. BIBLIOTECA DE CONSULTA ENCARTA 2003. Microsoft Corporation. © 1993-2002
2. BUNGE, Mario. *"La Ciencia, su método y su filosofía"*, El Gráfico Editores. Buenos Aires 1985.
3. BLOSSIERS HUME, Juan José, *"Criminalidad Informática".* Editorial Librería Portocarrero. Lima, 2003.
4. BLOSSIERS HUME, Juan José, *"Derecho Informático".* Editorial Librería Portocarrero. Lima, 2003.
5. BLOSSIERS HUME, Juan José, *"Informática Jurídica".* Editorial Librería Portocarrero. Lima, 2003.
6. BLOSSIERS MANZZINI, Juan José y CALDERON GARCIA Silvia B., *"Delitos Informáticos en la Banca".* Editora ROA SRL. Lima, 2000.
7. BRAMONT - ARIAS TORRES, Luis Alberto, *"El Delito Informático en el Código Penal Peruano"*, Fondo Editorial de la Pontificia Universidad Católica del Perú. Lima, 1997.
8. BRAMONT - ARIAS TORRES, Luis Alberto y GARCIA CANTIZANO, María del Carmen, *"Manual de Derecho Penal Parte Especial",* Editorial San Marcos – Cuarta Edición. Lima, 1998.
9. BRAMONT - ARIAS TORRES, Luis Miguel, *"Lecciones de la Parte General y el Código Penal",* Editorial San Marcos – Segunda Edición. Lima, 1998.
10. CABANELLAS GUILLERMO, *"Diccionario Enciclopédico de Derecho Usual",* Editorial Eliasta, Buenos Aires, 1989.
11. CARRETERO, Jesús y otros: "Descubre Internet", editorial PEARSON EDUCACION S.A., Madrid, 2004.
12. CORREA, Carlos y otros: *"Derecho Informático",* Ediciones de Depalma, Buenos Aires, 1987.
13. CHIRINOS SOTO Francisco, *"Código Penal Comentado"*, Editorial RODHAS Segunda Edición Lima, 2005.
14. DAVARA, Miguel Ángel: *"Derecho Informático"* Editorial Aranzandi. Madrid, 1993
15. DICCIONARIO JURÍDICO ESPASA, Editorial Espasa S.A. Madrid. 2001.
16. Enciclopedia Universal Salvat, Editorial Salvat, Madrid 2009
17. FAJARDO CABANA Patricia: "*Nuevos retos del Derecho Penal en la era de la Globalización"*, Editorial Tirant lo Blanch, Valencia, 2004.
18. FERNANDEZ ESTEBAN Luisa: *"Nuevas Tecnologías, Internet y Derechos Fundamentales"*, Editorial Mac Graw Hill. Madrid, 1998.

19. FLORES POLO, Pedro. "*Diccionario de Términos Jurídicos",* Editores Importadores, Lima, 1984.

20. GIL ALBARRAN Guillermo, "Derecho Informático", Editorial Megabyte, Lima – 2007

21. IASONI Marie: *"Comercio Electrónico, Aspectos Legales"*, Editorial Librería Portocarrero. Lima, 2002.

22. INSTITUTO DE INVESTIGACION Y DE ESTUDIOS PARA EL TRATAMLIENTO DE LA INFORMACIÓN JURÍDICA: *"Diálogos para la Información Jurídica",* Universidad Nacional Autónoma de México, 1989.

23. INSTITUTO NACIONAL DE ESTADISTICA E INFORMATICA (INEI), Colección de Seguridad de la Información: *"Delitos Informáticos".* Lima, 2001.

24. NUÑEZ PONCE, Julio. *"Derecho Informático",* MARSOL Perú Editores S.A., Lima, 1996.

25. PEÑA CABRERA, Raúl: *"Tratado de Derecho Penal – Estudio Programático de la Parte Especial"*, Editora Jurídica Grijley. 3ra. Edición. Lima, 1999.

26. RAMOS SUYO, Juan. *"Derecho de Ejecución Penal"*, Editorial Ediciones Atenea, Lima, 2003

27. RAMOS NUÑEZ, Carlos. *"Cómo hacer una Tesis de Derecho y no envejecer en el intento"*, Editorial Gaceta Jurídica - Segunda Edición. Lima, 2002.

28. REYNA ALFARO, Luis Miguel. *"Los Delitos Informáticos – Aspectos Criminológicos, Dogmáticos y de Política Criminal.* JURISTA Editores. Lima, 2002.

29. RIOS ESTAVILO, José Luis, *"Derecho e Informática en México – Informática Jurídica y Derecho de la Informática",* Universidad Nacional Autónoma de México - 1997.

30. SAN MARTÍN CASTRO, César: *"Derecho Procesal Penal – Volumen I"* Editora Jurídica Grijley. 3ra. Edición. Lima, 1999.

31. SAN MARTÍN CASTRO, César: *"Derecho Procesal Penal – Volumen II"* Editora Jurídica Grijley. 2da. Reimpresión. Lima, 2000.

32. TELLEZ VALDEZ, Julio, *"Derecho Informático"*, Universidad Nacional Autónoma de México, 1991.

33. TELLEZ VALDEZ, Julio: *"Contratos Informáticos – Contratos, riesgos y seguros informáticos",* Universidad Nacional Autónoma de México, 1988.

34. TIEDEMAN, Klaus: "Derecho Penal y Nuevas Formas de Criminalidad", Editorial IDEMSA. Lima, 2000.

35. TORRES Y TORRES LARA, Carlos: *"La Informática y el Derecho Empresarial"*. Revista Peruana de Derecho de la Empresa Nro. 32, 1989.

36. ZUÑIGA Rodríguez Laura: "Derecho Penal, Sociedad y Nuevas Tecnologías", editorial Colex, Madrid 2001.

2. HEMEROGRAFÍA

1. IUS ET PRAXIS, Revista de la Facultad de Derecho y Ciencias Políticas, Fondo de Desarrollo Editorial de la Universidad de Lima, Nº 32 Enero–Diciembre, Lima, 2001.
2. Revista Jurídica del Perú Nº 203, Trujillo 2001.
3. IUS ET PRAXIS, Revista de la Facultad de Derecho y Ciencias Políticas, Fondo de Desarrollo Editorial de la Universidad de Lima, Nro. 26 Enero – Diciembre, 1996.
4. Boletín Mexicano de Derecho Comparado Nº 86, 1996.
5. Revista Cuadernos de la Facultad de Derecho y Ciencias Sociales Nº 19, Montevideo - 1990.
6. Revista de Derecho y Tecnologías Informáticas Nº 04, Bogota, 1990.
7. Revista Cubana de Derecho Nº 01, 1991.
8. Revista de Derecho Nº 39, Bilbao, 1991.
9. Revista Peruana de Derecho de Empresa Nº 32, Lima, 1989.
10. Revista Jurídica de Catalunya Nº 03, Barcelona, 1988.
11. Revista de Derecho y Ciencias Políticas de la Universidad Nacional Mayor de San Marcos. Nº 47. Lima, 1987.
12. Revista de la Facultad de Derecho y Ciencias Políticas Medellin, 1985.

3. ARTÍCULOS PUBLICADOS EN LA WEB

Revista Electrónica de Derecho Informático "www.derechoinformatico.com"

1. "Breve ensayo sobre delitos de violación de la intimidad en la legislación Peruana, C.J. VILLON MEDINA y M.P. VALDIVIA LUQUE, Abril 2003
2. "El derecho a controlar la información personal". : Dr. Esteban RUÍZ MARTÍNEZ. Nº 49 Agosto 2002
3. "El derecho a la intimidad en una sociedad informatizada", María Barberá Fraguas. Nº 42 Enero de 2002.
4. "El Derecho Peruano Frente a los Desafíos del Nuevo Milenio: Conciliación, Tecnología e Innovación", César Antonio MAITA AZPIRI, Abril 2001.
5. "El Bien Jurídico en el Delito Informático", Luis Miguel REYNA ALFARO, Abril 2001.
6. "De la Informática Jurídica y el Derecho Informático, al Derecho Informático, Telemático y del Ciberespacio", Marcelo BAUZA R., Febrero 2001.

7. “Del Derecho de la Información al Derecho Informático: Propuesta de Sistematización”, Carlos E. DELPIAZZO, Enero 2001.

8. “El Corpus Juris del Derecho de Internet”, Francisco José BARRIENTOS, Enero 2003.

9. “El Bien Jurídico Tutelado: Delitos Informáticos o Delitos Cometidos por Medios Informáticos”, José SÁEZ CAPEL, Abril 2002.

10. “El Derecho a la Intimidad en una sociedad informatizada”, María BARBERÁ FRAGUAS, Licenciada en Derecho, Doctora en Derecho Civil en la Universidad de Sevilla y Oficial de la Administración de Justicia, Enero 2002.

11. “La Privacidad Laboral”, Renato Javier JIJENA LEIVA – Profesor de Derecho Informático de la Universidad Católica de Valparaíso. (Chile) Agosto 2002.

12. “El Tratamiento de los datos personales en internet”, Javier DOMINGO RIPALDA, Octubre 2002.

13. “El proyecto de Convención del Consejo de Europa para reprimir el ciberdelito y los peligros que entrañará...” José SÁEZ CAPEL. - Profesor ordinario de Derecho Penal en las carreras de grado y de postgrado de la Facultad de Derecho y Ciencias Sociales de la Universidad de Buenos Aires. Diciembre de 2001.

14. “Delitos informáticos o delitos cometidos por medios informáticos. El bien jurídico tutelado”, José SÁEZ CAPEL - Profesor regular de Derecho Penal en las carreras de grado y postgrado de la Facultad de Derecho y Ciencias Sociales de la Universidad de Buenos Aires, Abril de 2002.

15. “Internet y Delito informático: Nuevas formas de criminalidad”, Erinda EVA BERRIER. - Abogada. Doctorada en Ciencias Penales en la Universidad John F.Kennedy. Corte Suprema de Justicia de la Nación. Cuerpo de Peritos Contadores Oficiales, Octubre de 2001.

Revista Electrónica de Derecho Informático Alfa–Redi “www.alfa-redi.com”

16. “Pornografía e Internet: Aspectos Penales”, REYNA ALFARO, Luis Miguel. Oct. 2003

17. “Delitos informáticos y su prueba algunas consideraciones sobre la ley Penal Mexicana, con base en la Legislación Penal Internacional, SÁNCHEZ FRANCO, Alfredo. Enero 2004.

18. “La Intimidad y el Avance de la Informática”, Juan Francisco Arana Chalco

Revista Electrónica Delitos Informáticos www.delitosinformaticos.com

19. “Rasgos afines de los llamados delitos informáticos”, Siura L. ARREGOITIA LÓPEZ

20. “El derecho a la intimidad y el avance de la informática”, ARANA CHALCO, Juan Francisco.

21. CLAUDIO HERNÁNDEZ : Hackers Los piratas del Chip y de Internet© 1999-2000-2001 http://perso.wanadoo.es/snickers/ snickers@wanadoo.es

Otras direcciones electróncas

22. http://delitosinformaticos.com/legislacion/espana.shtml

23. http://abogadopoblete.blogspot.com/2008/06/ley-26388-delitos-informaticos-reforma.html

24. http://www.ert.com.co/site/ley679-3agosto2001.pdf

25. http://200.2.12.198/nede/files/archivos/LEY%208131%20DE%20ADMINISTRACION%20FINANCIERA%20DE%20COSTA%20RICA.doc.

26. http://delitosinformaticos.com/legislacion/costarica.shtml

27. http://www.delitosinformaticos.com/legislacion/venezuela.shtml

28. http://europa.eu/legislation_summaries/justice_freedom_security/fight_against_organised_crime/l33193b_es.htm

29. http://lac.derechos.apc.org/cdocs.shtml?x=8325

30. http://www.un.org/spanish/News/fullstorynews.asp?newsID=15793&criteria1=Latina&criteria2=internet

31. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52002PC0173:ES:HTML

32. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32005F0222:ES:HTML

33. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2008:0448:FIN:ES:HTML

4. TESIS CONSULTADAS

ARATA SALINAS, Ángel Alfonso; Tesis para optar el Grado de Abogado: “Las Nuevas tecnologías de la información y la problemática jurídica del comercio electrónico”, Universidad Nacional Mayor de San Marcos. Facultad de Derecho y Ciencia Política, Lima, 2002.

ARMAS MORALES, Carlos Eduardo: Tesis para optar el Grado Académico de Magíster: “Sistema de contratación por medios electrónicos: Manifestación de la voluntad y perfeccionamiento contractual”, Universidad Nacional Mayor de San Marcos. Facultad de Derecho y Ciencia Política, Lima, 2002.

FERNÁNDEZ DE SOTO, María Clara; Tesis para optar el Grado de Abogado: “Atipicidad relativa en los Delitos de falsedad, hurto, estafa y daño informáticos”, Universidad Sergio Arboleda, Escuela de Derecho Rodrigo de Bastidas, Santa Marta D.T.C.H 2001

BORGHELLO Cristian Fabián; Tesis para obtener Licenciatura en Sistemas: “Seguridad Informática: Sus implicancias e Implementación”, Universidad Tecnológica Nacional, Septiembre 2001.

REYES KRAFFT, Alfredo Alejandro; Tesis para obtener el Diploma de Doctor en Derecho: “La firma electrónica y las entidades de certificación”, Universidad Panamericana, Facultad de Derecho, México D.F. 2002.

ANEXOS

ANEXO (01)

PROYECTO DE TESIS

UNIVERSIDAD CATÓLICA DE SANTA MARIA

ESCUELA DE POSTGRADO

MAESTRÍA EN DERECHO PENAL

“LOS DELITOS INFORMÁTICOS EN EL CÓDIGO PENAL”

PROYECTO DE TESIS PRESENTADO POR EL BACHILER:
JORGE ALBERTO VEGA AGUILAR
Para optar el Grado Académico de:
Magíster en Derecho Penal

AREQUIPA – PERÚ

2010

.

INDICE

I. PREÁMBULO

El presente proyecto de investigación, versa sobre los delitos informáticos en el Código Penal, lo cual resulta ser un tema novedoso; asimismo, ha sido poco analizado a nuestra realidad, pues poco se ha estudiado y se tiene escaso conocimiento del tema, lo cual ha originado que no todas los delitos de nueva data, así como los realizados por medios informáticos sean denunciados, especialmente por parte de las empresas, con la finalidad de no perder credibilidad y reputación ante sus clientes, aunado a la poca experiencia por parte de los efectivos de la Policía Nacional, Fiscales y Jueces; quienes debido al avance de la ciencia y tecnología, aún no cuentan con especialistas para afrontar esta nueva forma de criminalidad.

Por ello es importante tener en cuenta que "el desarrollo de los sistemas de comunicación, la informática y las modernas técnicas de captación y grabación del sonido y la imagen hacen que cada día sea más difícil conservar intacto y el ámbito de la propia vida privada. Los peligros que representan las nuevas tecnologías han sido mencionados por el Tribunal Constitucional[5]"; en tal sentido en estos tiempos a nadie escapa la enorme influencia que ha alcanzado la informática en la vida diaria de las personas y organizaciones, siendo de gran importancia para el desarrollo y progreso de los países; motivo por el cual, junto al avance de las nuevas tecnologías e informática, estos, han influenciado casi todas las áreas de la vida social, por lo que nos hemos visto en la obligación de realizar la presente investigación la cual nos va a permitir hacer frente a éste fenómeno informático y así tener un material bibliográfico de consulta de suma importancia.

Conociendo la problemática existente que ha originado en la actualidad el avance de la ciencia, informática y nuevas tecnologías, ha dado lugar a una nueva disciplina dentro de las ramas del Derecho, como es el Derecho Informático; por otro lado han originado nuevas formas de criminalidad, llamadas por algunos autores tanto nacionales y extranjeros como: delitos informáticos, delitos computacionales, delitos a través de medios informáticos y criminalidad informática, por lo que es necesario realizar un estudio riguroso del tema, en aras de permitir una optima administración de Justicia, pues desde el punto de vista social y jurídico, no puede negarse la importancia de esta problemática, dado el incremento e incidencia que tiene en la actualidad en nuestra sociedad.

El Autor

[5] FERNÁNDEZ ESTEBAN Luisa, "Nuevas Tecnologías, Internet y Derechos Fundamentales", Editora McGraw/Interamericana de España. 1998, pág.137.

II. PLANTEAMIENTO TEÓRICO

2. PROBLEMA DE INVESTIGACIÓN

2.1 ENUNCIADO DEL PROBLEMA

En primer lugar es importante precisar que la técnica siempre es un arma y cada avance fue explotado criminalmente, en forma tal que siempre el criminal está más tecnificado que la prevención del crimen[6]. Luis Miguel Bramont-Arias Torres, señala que "…el *fenómeno informático* es una realidad incuestionable y parece que también irreversible, la informática se instalado entre nosotros. El principal problema se traduce en buscar fórmulas efectivas de control respecto a las cuales el Derecho ha de tener un marcado protagonismo, en su papel de regulador de las relaciones y mecanismos sociales para el mantenimiento de un orden social"[7].

Motivo por el cual resulta de suma importancia la función que cumple en la sociedad el Derecho Penal, el cual como última ratio resulta un arma fundamental para realizar una lucha frontal contra la delincuencia informática, en tal sentido debemos resaltar que el Derecho Penal es el único medio de control social para solucionar este problema, que afecta a nuestra sociedad, siendo los legisladores quienes deben de orientar los lineamientos políticos – criminales para poder hacer frente a esta nueva forma de criminalidad.

Con estas consideraciones previas, investigar sobre los delitos informáticos en el Código Penal vigente, resulta ser un tema de gran importancia, debido a la implicancia que tiene en nuestra sociedad, la cual en su conjunto debe de organizarse y realizar mecanismos preventivos del caso para enfrentar a estos delitos de nueva data.

PROLBLEMA PRINCIPAL:

¿En que medida los **delitos informáticos** no son denunciados e investigados en sede policial y judicial, pese a que se encuentran tipificados en el **Código Penal** vigente?.

---

6 REYNA ALFARO, Luis Miguel. "Los Delitos Informáticos – Aspectos Criminológicos, Dogmáticos y de Política Criminal", JURISTA Editores E.I.R.L. Lima – Perú. 2002. pág.125.

7 BRAMON–ARIAS TORRES, Luis Alberto, *"El Delito Informático en el Código Penal Peruano"*, Fondo Editorial de la Pontificia Universidad Católica del Perú. Lima – Perú. 1997. pág. 17

PROBLEMAS SECUNDARIOS:

¿Por qué se incrementa la **piratería informática**, afectando el derecho de autor, así como el **patrimonio** de personas y empresas de software, pese a que se encuentra legislado en el Código Penal?

¿Por qué en la actualidad se viene incrementando los delitos cometidos a través de **medios informáticos**, sabiendo que estos atentan **contra la vida el cuerpo y la salud**?

¿Por qué se incrementa con tanta facilidad y rapidez la **pornografía infantil** por Internet, pese a que se encuentra sancionado en el Código Penal y sabiendo que es un delito que atenta **contra el pudor**, **honor e intimidad de los menores de edad**?

2.2 DESCRIPCIÓN DEL PROBLEMA

En los últimos años el mundo entero ha experimentado un sorprendente y explosivo avance en el desarrollo de la ciencia informática, telemática y el Internet; no cabe duda que la "era digital" ha otorgado y seguirá proporcionado innumerables beneficios a nuestra sociedad, sin embargo no podemos desconocer que este desarrollo tecnológico ha propiciado, también, la aparición de nuevas modalidades delictivas, las que hasta hace poco eran desconocidas en nuestro ordenamiento jurídico.

El cambio social operado en las últimas décadas, resulta íntimamente vinculado a la evolución tecnológica operada en ese transcurso de tiempo, generándose problemas para la protección de intereses sociales no convencionales y para la represión de las conductas delictivas realizadas a través de medios no convencionales, pues como bien precisa ZAFFARONI: "…el impacto de la explosión tecnológica es un problema de política criminal que conoce sobradamente".

Cuando diversos especialistas e investigadores han tratado respecto a los delitos informáticos, podemos apreciar que estos ilícitos implican actividades

criminales que en un primer momento los países han tratado de encuadrar en figuras típicas de carácter tradicional, tales como robos o hurtos, fraudes, falsificaciones, espionaje, sabotaje, estafa, etc.; sin embargo, debe destacarse que tanto el avance tecnológico y el uso de nuevas técnicas informáticas, han creado nuevas posibilidades para el uso indebido de las computadoras, las mismas que han originado a su vez la necesidad de tipificar estas nuevas formas de criminalidad, denominados delitos de nueva data por parte del Derecho Penal como última ratio.

En la actualidad las empresas utilizan con más frecuencia las computadoras para manejar y almacenar su información vital que constituye el activo más valioso, esto les trae muchos beneficios, pero también los hace vulnerables a los diferentes delitos que se pueden cometer por medio de las computadoras si no se cuentan con un sistema de seguridad. Entre ellos, se pueden mencionar el robo, destrucción o modificación de información, fraude, etc. Que son realizados por personas con algún conocimiento de computación, ya sea dentro o fuera de la empresa[8].

Uno de los puntos más controvertidos en la doctrina del derecho informático, es la demostración de la existencia de los delitos informáticos, motivo por el cual diversos investigadores y especialistas en la materia han propugnado la tesis negativa, pues aducen que no existen delitos informáticos como tal, sino que simplemente son conductas no éticas y antijurídicas cuyos medios de ejecución se verifican con modernos sistemas, afirmando que la valoración de la existencia de tales delitos es nula, ya que todas las conductas son asimilables o están tipificadas en el actual Código Penal de 1991.

Es importante precisar que la doctrina mundial al respecto reconoce que, hay casos donde la tipicidad se vuelve más difícil de apreciar. Paralelamente y en forma opuesta crece la corriente doctrinal que sí cree en la existencia de los delitos informáticos como tales con una estructura propia y carente de normativa jurídica penal. Es así, que en sus planteamientos establecen que ninguna ley protegió jurídicamente la información que, hoy por hoy, frente a los avances y desarrollos de la teoría de la comunicación de la información, dentro de la sociedad tecnológica, ha devenido en un nuevo bien jurídico merecedor de la correspondiente tutela.

[8] Instituto Nacional de Estadística e Informática – INEI, "Conceptos de Seguridad de la Información", Lima –Perú Marzo 2000, Pág. 7

¿Por qué entonces fue materia olvidada?, no fue más que el simple hecho de que el hurto, fraude, espionaje, sabotaje o la creación de armas intangibles que destruyan esa información era algo no sólo inesperado sino de ciencia ficción. Entonces el olvido consistió en que concebir ese tipo de bienes era casi imposible de erosionar, mutilar o usar con los métodos convencionales de archivo y búsqueda. Mal entonces se hubiera legislado sobre una materia que en aquel momento carecía de importancia práctica.[9]

Con la invención de los computadores, el marco socioeconómico, legal y tecnológico cambió considerablemente, por lo que el hecho de que toda la actividad contraria a derecho, en lo que tiene que ver con la informática, se concrete en su mayoría como delito a distancia, una forma jurídica hasta hoy cuasi inaplicable, es una comprobación más de la diversidad de modalidad con que opera un delito informático y por ende con existencia y estructura propias diversas de las conocidas hasta ahora.

El manejo de un bien inmaterial como es la información, acarrea como consecuencia que el actuar delictivo contra él se elabore también inmaterialmente; así por ejemplo el crear un programa para delinquir mediante el uso de una computadora o de sus derivados, hace que el objeto con el cual se realiza el delito sea también inmaterial, otra nota detonante y demostrativa de qué tan lejos se encuentra la tipicidad penal en el área de la informática.

Es bien sabido, que el Derecho en general y el penal en particular, parten de un concepto de objeto material tangible frente a conductas punibles contra el patrimonio económico y aún contra la fe pública[10], se puede apreciar que existen casos que son realmente claros, como la fabricación de una bomba de tiempo, así como la bombas lógicas, que es un programa de computación por el cual todo un sistema puede desaparecer, en este caso el soporte lógico del sistema llamado software o inclusive dañar el soporte físico denominado Hardware, utilizando la red para ingresar al sistema o ingresándola directamente al ordenador.

Este tipo de programas, así como las diferentes clases de virus existentes logran destruir a distancia el bien jurídico información y otros bienes jurídicos protegidos como el honor, intimidad, patrimonio, el orden económico,

[9] RIVERA LLANO, Abelardo. Dimensiones de la informática en el Derecho. Jurídica Radar Ediciones 1995, Pág. 90
[10] Ibid., pág. 91

pudiendo llegar hasta atentar contra la vida el cuerpo y la salud, para ello se utiliza un objeto inmaterial, algo que carece de forma corpórea. Es aquí donde la necesaria tipicidad penal peca por inexistente.

Sin embargo hay todavía quienes consideran que los delitos informáticos, como tales, no existen. Argumentan que tan sólo son delitos normales que en lo único que se pueden diferenciar, de otro delito cualquiera, es en las herramientas empleadas o en los objetos sobre los que se producen, siendo duda, una visión demasiado limitada de la realidad, debido a que existen muchos otros delitos que difícilmente se pueden tipificar con leyes actuales ya que tendrán que adaptarse rápidamente a la realidad.[11]

Hay que recordar también que las compañías de seguros, de varios países, ofrecen cobertura concreta contra este tipo de delitos. Sólo en Estados Unidos se calcula que se generan perjuicios económicos, por los delitos informáticos, que superan los 10.000 millones de dólares o más de 5.000 millones de libras esterlinas en el Reino Unido.

Asimismo, el 90% de los delitos informáticos que investiga el FBI tienen que ver con la Internet, en la actualidad la Unión Europea está trabajando por la unificación de criterios, en razón de coordinar una política internacional, destinada a la penalización mundial de conductas a través de la red de Internet.

Si bien es cierto que la Internet es fruto del avance tecnológico, no estaba pensada y desarrollada para lo que está ocurriendo: su propio diseño no está basado sobre protocolos hiper-seguros, hoy en día se estima que no existe un sólo servidor en el mundo que no haya sufrido un ataque contra su seguridad por parte de hackers y crackers.

Dar una definición de los delitos informáticos, es difícil, pues son delitos de nueva data y no existe una definición que sea aceptada por el Derecho Penal de manera unánime. La delincuencia informática comprende una serie de comportamientos que tanto doctrinarios como tratadistas han intentado definir.

[11] Como lo ocurrido en Norte América con el famoso gusano de Internet, que lanzó Robert Morris Jr. en Noviembre de 1.988 que acabó bloqueando más de 6.000 ordenadores, que de no existir en ese momento el Acta sobre Fraude y Abuso Informático en los Estados Unidos, esta conducta altamente perjudicial quedaría al margen de la regulación penal.

Esta situación ha sido puesto de relieve en los últimos tiempos, lo que ha originado la necesidad de tipificar y sancionar a los infractores, que cometan delitos informáticos, "….ante esta situación, el legislador se encuentra se sitúa ante una doble opción, o crear nuevos tipos penales donde se criminalicen específicamente estas conductas, como delitos autónomos, o bien, incorporarlos como modalidades de comisión dentro de las conductas delictivas ya tipificadas. Esta última posición es asumida por el Código Penal Peruano…."[12]. En la actualidad son más los países que están incorporando en su legislación penal, esta nueva forma de criminalidad, algunos tratadistas afirman que estos delitos cometidos a través de medios informáticos, afectan un bien jurídico protegido que es la "Información", reconocido y tutelado por la Constitución.

En este sentido tanto el Código Penal Peruano vigente de 1991 y el anterior de 1924, no han regulado esta nueva forma de criminalidad, teniendo que adaptarse a los cambios, siendo recién en el año 2000 se publica en el Diario Oficial el Peruano, la Ley Nº 27309, la cual incluye dentro de "Los Delitos Contra el Patrimonio", el Capítulo, denominado "Delitos Informáticos", donde se tipifica "El Intrusismo Informático", "Sabotaje Informático" y sus "Agravantes".

2.3 JUSTIFICACIÓN E IMPORTANCIA DEL PROBLEMA

1.3.1 JUSTIFICACIÓN

Las razones y motivos que impulsaron la presente investigación se debe a la rapidez con que se viene incrementando los denominados delitos informáticos en la actualidad, tanto a nivel nacional e internacional, alterando el normal desenvolvimiento de la sociedad, debido a que si bien es cierto que el avance científico y tecnológico, desde la llegada de la computadora, la informática, telemática e Internet, traen consigo desarrollo y progreso, también traen problemas que afectan a nuestra sociedad, a través de lo delitos informáticos, los cuales afectan diversos bienes jurídicos protegidos como son el patrimonio, el honor, intimidad, la vida el cuerpo y la salud entre otros.

[12] BRAMONT - ARIAS TORRES, Luis Alberto, Ob. cit. pág. 79.

La presente investigación se justifica en el sentido, que una vez concluida permitirá esclarecer la problemática existente y determinar una mejor aplicación de la norma, debido a que el "Derecho Penal, en los últimos treinta años, ha variado en gran medida sus formas y ámbitos de intervención…"[13], incrementándose los delitos realizados a través y por medios informáticos, por lo que para "…poder determinar la posible existencia de los delitos informáticos, es necesario determinar que se debe recurrir precisamente a las dos materias que integran la relación … como son la informática y el derecho, en la cual cada una aporta su horizonte de proyección"[14]. Asimismo, es importante debido a que en la actualidad el reto es por parte de los legisladores quienes son los encargados en buscar nuevas alternativas de solución al problema que acarrea los delitos informáticos, puesto que "…el principal problema se traduce en buscar fórmulas efectivas de control, respecto a las cuales el derecho ha de tener un marcado protagonismo, en su papel de regulador de las relaciones y mecanismos sociales para el mantenimiento de un orden social."

Desde el punto de vista doctrinario, es importante debido a que permitirá tener un mayor conocimiento respecto a los delitos informáticos, la misma que servirá como fuente de derecho, estando dirigido en primer lugar a todas las personas que tengan interés en conocer y profundizar respecto al tema de investigación y especialmente dirigido a los legisladores, debido a que son ellos los encargados de crear o modificar las normas legales, siendo su responsabilidad el que éstas resulten conformes con las necesidades de nuestra sociedad.

1.3.2 IMPORTANCIA

La presente investigación resulta de especial importancia por lo antes expuesto, debido que permitirá que los estudiantes de Derecho, Abogados y diversos profesionales, así como los funcionarios estatales, los miembros de la Policía Nacional, Ministerio Público y Poder Judicial, puedan tener los conocimientos y herramientas necesarias que permitan hacer frente a los delitos informáticos.

---

13 REYNA ALFARO, Luis Miguel, Ob. cit. 123.

14 RIOS ESTAVILO, José Luis, *"Derecho e Informática en México – Informática Jurídica y Derecho de la Informática"*, Universidad Nacional Autónoma de México. México - 1997. pág. 114.

3. ANALISIS DE ANTECEDENTES INVESTIGATIVOS

2.1 Tesis para optar el Grado de Abogado: "LAS NUEVAS TECNOLOGÍAS DE LA INFORMACIÓN Y LA PROBLEMÁTICA JURÍDICA DEL COMERCIO ELECTRÓNICO", sustentado por Ángel Alfonso Arata Salinas, Universidad Nacional Mayor de San Marcos. Facultad de Derecho y Ciencia Política, Lima 2002.

La creación y uso de los medios electrónicos, teléfono, fax, beeper, computadoras, entre otros soportes convergentes con las redes de comunicación, han convertido a la información en un derecho humano básico y en una herramienta de investigación científica fundamental, generando características peculiares en la forma de comunicarnos, tanto a las personas naturales y jurídicas de sus actividades personales, laborales, sociales, académicas, profesionales y comerciales, por medio de la tecnología informática, a través de los diversos soportes informáticos inventados en la actualidad, encaminándonos a un mundo informatizado gracias a la versatilidad de la computadora, que por ende se va a expresar en un bienestar social acorde con el respeto de los derechos individuales de las personas.

En este sentido, consideramos necesario implementar una nueva asignatura en las facultades de derecho: tomándose en cuenta la sinergia de las tecnologías de la información y comunicación en una sola disciplina de estudio, siendo ésta el Derecho Telemático, que tendrá como objeto de estudio y análisis conceptual las reglas, principios y consecuencias que genera el uso de las tecnologías del procesamiento y transmisión de la información, a través de su forma multimedia, por las disciplinas y especialidades jurídicas de nuestro derecho positivo, brindando una visión esclarecedora de los efectos que generan dichas tecnologías en la sociedad y el derecho.

Se ha concluido que, el desarrollo de las tecnologías aplicadas a la actividad comercial, ha llevado al uso de soportes informáticos con inteligencia artificial incorporada, y para determinar su alcance, hay que determinar la naturaleza jurídica del comercio electrónico, partiendo de sus particularidades, como las tecnologías a utilizar, la manifestación de voluntad virtual, el uso de certificados digitales, el pago virtual, los bienes inmateriales, la firma

electrónico o digital, el repudio entre otras particularidades propias del comercio electrónico. Para ello es necesario que la regulación del acto de comercio virtual parta de la neutralidad del derecho en cuanto a las tecnologías a utilizar, del punto de vista del servicio a brindar, más no partir de la tecnología aplicada al servicio, para una regulación eficaz; por existir la posibilidad de brindar un mismo servicio con diversas tecnologías convergentes, o nuevas tecnologías.

Es de suma importancia para el Derecho Informático o Derecho Telemático, regular sistemáticamente los actos del comercio electrónico, como lo viene haciendo la Ley de Firmas y Certificados Digitales y su Reglamento, teniendo en cuenta la particularidad de sus elementos virtuales más relevantes, como el acto jurídico virtual, la libertad contractual, los sujetos virtuales, el domicilio virtual, las ofertas virtuales, publicidad virtual, venta virtual, pago y factura virtual como el repudio.

Debiéndose tener en cuenta, al mensaje de datos como el acto jurídico virtual de contenido patrimonial, la clasificación de los sujetos virtuales intervinientes, en remitente, destinatario e intermediario, al dominio se le debe dar la calidad de domicilio virtual, las ofertas virtuales a través de Internet contenidas en servidores peruanos deberá someterse a las reglas de la publicidad que la legislación peruana establece. La compraventa por Internet debe ser comprendida y regulada con las reglas de una venta a distancia por estar ausentes físicamente los contratantes, otorgarle plena validez al pago virtual cuando se haga a través de un medio idóneo y/o mediante cualquier tecnología puede contenerse en un soporte electrónico para su posterior demostración.

Se deberá regular los servicios brindados a través de los servidores web peruanos para su pago al fisco como contribución al desarrollo del país, mediante el control de ficheros que contengan las facturas virtuales en el orden de pedidos, a través de la Superintendencia de Administración Tributaria - SUNAT, dándosele todos sus atributos, a dichas facturas como medio de prueba de la propiedad del bien o servicio adquirido. Se deberá analizar jurídicamente al repudio, por su relevancia en el comercio electrónico, al ser un factor perturbador en el crecimiento del comercio electrónico, donde la carga de la prueba corresponda a quien alega no haber

hecho el pedido, pues así se le estaría dando mayor estabilidad jurídica al floreciente comercio electrónico en el Perú.

Se concluye en la necesidad que se regule la participación de los fedatarios informáticos en el peritaje y verificación de los documento electrónico en cualquiera de sus formas en que haya sido elaborado por cualquier tecnología, como nueva forma de contener un mensaje convencional expresado en microformas, sistema analógico o sistema binario que puedan estar alojados en películas, cintas discos magnéticos flexibles o duros, memorias circuitales comunicables a terceros y duraderos en el tiempo.

Para un comercio electrónico más seguro, es indispensable determinar los lineamientos en que va actuar la Autoridad Administrativa Competente, como Entidad Superior para otorgar el visto bueno del uso de tecnologías estándares utilizados en los mensaje de datos, generado, enviado o recibido, a través de un sistema de información electrónico u óptico, efectuado por el remitente o intermediario al destinatario, a través de las Entidades de Certificación a efectos que tenga plena validez en el acto de comercio virtual, al margen del intercambio electrónico de datos firmados electrónicamente o digitalmente.

En cuanto al acuse de recibido, que es la confirmación de la recepción del mensaje de datos como medio probatorio, se deberá tener en cuenta para su regulación, el tiempo, lugar, la designación del sistema de información a donde se envío del mensaje de datos y bajo el control de quien está, remitente, intermediario o destinatario.

Se ha llegado a la conclusión que, es necesario e impostergable plantear propuestas de regulación del comercio electrónico mediante una directiva marco en la región, que comprenda las diversas etapas de la contratación electrónica, donde se contemplen los elementos esenciales en cuanto a la forma y al fondo de la contratación mediante el uso de soportes informáticos, detallar su ámbito de aplicación, las definiciones de los nuevos conceptos y preceptos jurídicos que introduce el comercio electrónico. Esta directiva marco regional en primer término deberá unificar criterios en cuanto al comercio electrónico entre otros aspectos sustanciales y no dejar a leyes y reglamentos aislados internos de los países, regular actos de comercio

virtuales trascendentes, sino de todo un proyecto integral para una legislación más coherente, de acorde con la legislación regional comparada y afín en lo posible con los países de Europa y Asia, que poseen tecnologías puntas para el comercio electrónico en el mundo.

Debiendo ser consciente el profesional del derecho que la estabilidad jurídica es un elemento vital en el desarrollo del intercambio comercial y económico en cualquier parte del mundo, más aún en nuestra sociedad, siendo ello un reto y respuesta del derecho peruano dar estabilidad jurídica en cuanto al tema del comercio electrónico para poder generar confianza y su uso masivo en beneficio de todos los peruanos, así como desarrollar las bases para toda la cyberlegislación que dentro de poco regulara la vida virtual que estamos viviendo en el mundo sideral.

2.2 Tesis para optar el Grado Académico de Magíster: "SISTEMA DE CONTRATACIÓN POR MEDIOS ELECTRÓNICOS: MANIFESTACIÓN DE LA VOLUNTAD Y PERFECCIONAMIENTO CONTRACTUAL", sustentado CARLOS EDUARDO ARMAS MORALES, Universidad Nacional Mayor de San Marcos. Facultad de Derecho y Ciencia Política, Lima, 2002.

Con relación a la normatividad general, confirmamos que la tecnología se conduce mas adelante que la ley, siendo la actitud del jurista y/o legislador objetivar los puntos de conflicto o divergentes entre los hechos tecnológicos de avanzada con la tradición normativa en desfase a fin de facilitar soluciones legislativas y en consecuencia aminorar la brecha del hecho tecnológico con la norma reguladora. Se evidencian en el ámbito peruano, debido a los impactos de la electrónica digital y tecnologías telemáticas, cambios en la forma de realizar los negocios y transacciones que indudablemente se plasman en innovaciones de la normativa jurídica contractual de acorde con esta realidad tecnológica, que ha sensibilizado al legislador, promulgando desde luego este, sendas leyes en el afán de regular estos hechos, siendo estas leyes recientes, y aun no esclarecido su suficiencia operativa, por lo que nos reservamos la opción hacia una regulación especial inmediata, salvo las modificaciones necesarias asumidas.

Carecemos de doctrina nacional que se ocupa de evaluar y analizar el desarrollo de la normativa en función del crecimiento de los hechos electrónicos digitales, en todo caso los estudios doctrinales son insuficientes

en el país, para ofrecer una mayor referencia teórica necesaria para el debate doctrina l, que a la postre permita al Juzgador tener los elementos de juicios teóricos adecuados para interpretar y desde luego aplicar la normatividad correcta, ante una eventual situación innovada por estas tecnologías, y en consecuencia asumir con eficacia su rol de administrar justicia. Los proceso tecnológicos electrónicos digitales seguirán siendo una suerte de resultante de cambios acelerados y permanentes, factores que caracterizan a la sociedad de información y del conocimiento, no como una mera enunciación o retórica de conclusión académica, sino como una realidad fáctica y palpable que lo percibimos hoy día y estaremos comprobando en los próximos años.

Los medios técnicos que facilitan, auxilian al agente capaz, son efectivamente los únicos que han evolucionado en el sentido de facilitar el acto jurídico contractual, así en la formulación expresa, se puede apreciar los diversos sistemas para manifestar la voluntad, tal como son los naturales, manuales y electrónicos digitales que aun persisten y coexisten.

En lo que se refiere a la manifestación de la voluntad, sean estos por medios mecánicos, electrónicos digitales u ópticos, nosotros guardamos reserva de que cierto sector de la doctrina convalide a la formulación tacita como una manifestación indirecta de la voluntad, desde la óptica que las voluntades son expresadas por los propios manifestantes de la voluntad que ponen en una misma dirección interactiva sus inteligencias y sus acciones, posición asumida por un sector de la doctrina, prefiriendo el investigador la denominación de manifestación de voluntad no codificada, innovación que se propuso en un acápite de este trabajo. La forma y formalidad en los actos jurídicos amplia y enriquece su perspectiva al permitir la legislación el uso del documento sobre soporte electrónico digital alternativo con el documento sobre soporte material basado en el papel o símiles, igual situación se presenta con la firma manuscrita y la firma digital y/o electrónica, de tal manera que se conjuga una equiparidad y equivalencia funcional entre ambas formas ante el cumplimiento de una formalidad ad solemnitatem.

Las legislaciones sobre este tipo de contratos, convergen entre la iniciativa unilateral del oferente plasmadas en contratos de adhesión o con cláusulas generales de contratación y las normas tutelares concerniente

a los usuarios y consumidores, buscando el equilibrio regulador para evitar abusos de cláusulas que contravengan el principio de la equidad y el sentido de la justicia, por lo que habiendo dudas se deberá favorecer al consumidor o usuario, siendo esta la tendencia actual de las legislaciones más recientes en el mundo, ante el surgimiento de los derechos de los consumidores y usuarios.

El lugar y momento del perfeccionamiento contractual en los tiempos de tecnoglobalización, desterritorialización y espacio virtual, donde se alzaprima la contratación por medios electrónicos digitales, tienen singular importancia en las relaciones entre países, no habiendo problemas cuando se realiza o las partes se encuentren en lugares físicos y fijos; la problemática se presenta en una realización dinámica, debido que las partes están ubicados en puntos o lugares diferentes y aun variando constantemente de posición física y tiempo horario, como es el caso de la contratación que se hace desde un avión, crucero en navegación o servicios móviles, donde se tiene que resolver el lugar y el momento que concluye o perfecciona el contrato, mas aun cuando por la rapidez y la dinámica contractual de estos contratos es factible que en algunos casos se omitan de indicar la ley que rige el contrato, siendo que la solución deberá alternar entre la opción de aplicar, habiéndolos, los tratados especiales que los países suscriban para contratar por estos medios, la legislación especifica de una de las partes o recurrir a la norma internacional privada.

Están surgiendo cuestiones o conceptos que los doctrinarios en una primera apreciación reflexionan y evalúan como novedosas, no siendo así, tal como la denominada deshumanización del contrato que no es mas que la contratación automatizada sin presencia humana inmediata, producto del máximo auxilio tecnológico electrónico, así como la consolidación, en cuanto a la manifestación de la voluntad, de las criterios teóricos de la declaración combinado con la confianza, fundamentada en la oferta plasmada sobre la base de la apariencia y la aceptación sobre la confianza, que es propio de una sociedad muy dinámica y globalizada, y que constituyen gestas de este nuevo escenario cultural.

2.3 Tesis para optar el Grado de Abogado. "ATIPICIDAD RELATIVA EN LOS DELITOS DE FALSEDAD, HURTO, ESTAFA Y DAÑO INFORMÁTICOS", sustentada por: María Clara Fernández de Soto, Universidad Sergio Arboleda, Escuela de Derecho Rodrigo de Bastidas, Santa Marta D.C. 2001.

La cifra negra de la criminalidad, en materia de delitos informáticos, no puede seguir en la penumbra, de allí la necesidad imperiosa para el derecho penal y organismos gubernamentales la investigación de una nueva modalidad comisiva de amplias repercusiones sociales y económicas. Existe una necesidad urgente de incluir en el derecho penal vigente una tipificación básica de los delitos informáticos que afecten el interés social y el patrimonio público. En primer término en lo que concierne a las conductas punibles, sería imprescindible crear nuevos tipos penales y en otros casos modificar los ya existentes.

De otra parte, sería importante, resolver el problema de la atipicidad relativa generada por la ausencia de uno de los elementos del tipo cuando se trata de subsumir la conducta ilícita. Las infracciones ostensiblemente antijurídicas que recaen sobre ciertos bienes informáticos como el caso del Software, por lo que ésta tesis se circunscribe a algunos delitos contra el patrimonio económico especialmente: el Hurto, la Estafa y el Daño informático, aunque toca el ineludible tema de la falsedad informática, de inusitadas repercusiones en lo atinente a documento electrónico, pues en materia probatoria, la noción de documento no resuelve el problema de este tipo de documentos, es decir de aquellos que no se encuentran en soporte "papel" y en los que es controvertible en qué momento es original y en cuál copia. El punto fundamental es sin duda, no concebir todavía jurídicamente los bienes informáticos que tienen naturaleza incorpórea.

Actualmente se requieren serias modificaciones y en otros casos nuevas normas para disminuir en cierta forma la incertidumbre jurídica en que se encuentran sumergidas las nuevas disposiciones penales en materia de delito informático, pese a algunos avances, como la tipificación del acceso abusivo a sistemas informáticos en el nuevo estatuto represor. Cada vez más, se hace necesario el respaldo legal como la mejor y más adecuada forma de reprimir y castigar estos delitos, tal como se expondrá en el capítulo de la conveniencia de su incriminación y el sistema más adecuado para Colombia, según su

tradición jurídico- legal. Las conductas reprochables, resultan en la mayoría de los casos impunes debido a la inidoneidad de las figuras incriminatorias tradicionales, al no ser castigados dichos comportamientos ilícitos, debido a la carencia de claridad sobre la naturaleza jurídica de los bienes objeto material de los delitos ni del interés jurídico protegido, como se verá en el capítulo de atipicidad relativa de la acción.

Finalmente se expondrán cada una de las modificaciones a las conductas punibles contra el patrimonio ajeno objeto de esta tesis, que necesitan de verdaderos cambios, con miras de que exista en este país una penalización de la criminalidad informática. Al igual que un capítulo de recomendaciones donde se expondrán ideas, sobre la forma como enfrentar esta problemática social. Es oportuno aclarar, que esta investigación se circunscribe únicamente a delitos contra el patrimonio ajeno y se hará mención de otras conductas que lesionan otros bienes jurídicos.

El estado actual de adecuación normativa está en una categoría sui generis, ya que dichas infracciones no son de recibo en las actuales formas descriptivas, pese a que ya las contienen la mayoría de legislaciones penales. Crear o modificar es el dilema, decidir si conviene crear una ley individual sobre la materia o si los diversos tipos penales deben ser encasillados en diferentes capítulos del Código Penal mediante la ampliación de algunos tipos penales. Esta es la situación que se va a desarrollar en la investigación.

2.4 Tesis para obtener Licenciatura en Sistemas: "SEGURIDAD INFORMÁTICA: SUS IMPLICANCIAS E IMPLEMENTACIÓN", sustentado por Cristian Fabián Borghello, Universidad Tecnológica Nacional, Septiembre 2001.

El amplio desarrollo de las nuevas tecnologías informáticas está ofreciendo un nuevo campo de acción a conductas antisociales y delictivas manifestadas en normas antes imposibles de imaginar, ofreciendo la posibilidad de cometer delitos tradicionales en formas no tradicionales.

El motivo del presente es desarrollar un estudio completo del estado actual y futuro posible de Seguridad Informática, que continuamente se pone sobre el tapete y en realidad se conoce muy poco; se suele manejar con el amarillismo de los medios no especializados, dificultando esto su accionar y colocando

en tela de juicio el arduo trabajo de los especialistas. También intentaré brindar un completo plan de estrategias y metodologías, que sin bien no brindan la solución total (como muchos prometen), podrá cubrir parte del "agujero" que hoy se presenta al hablar de Seguridad Informática.

La mayoría del mundo informático desconoce la magnitud del problema con el que se enfrenta y, generalmente no se invierte ni los capitales humanos ni económicos necesarios para prevenir, principalmente, el daño y/o pérdida de la información que, en última instancia es el Conocimiento con que se cuenta. Paradójicamente, en el mundo informático, existe una demanda constante y muy importante que está esperando a que alguien los atienda.

2.5 Tesis para obtener el Diploma de Doctor en Derecho: "LA FIRMA ELECTRÓNICA Y LAS ENTIDADES DE CERTIFICACIÓN", sustentado por Alfredo Alejandro Reyes Krafft, Universidad Panamericana, Facultad de Derecho, México D.F. 2002

Internet es un medio, no un fin en sí mismo. El comercio no deja de ser comercio aún cuando tenga el calificativo de electrónico; asimismo, para que un mensaje de datos en el que se consignen contratos, convenios o compromisos que den nacimiento a derechos y obligaciones, pueda considerarse legalmente válido, es necesario asegurar que la información en él contenida reúna las siguientes características:

INTEGRIDAD: Entendida en dos vertientes, la primera respecto de la fiabilidad del método para generarla, comunicarla, recibirla o archivarla. Y la segunda como la forma de garantizar que la información en él contenida no fue alterada. Al respecto la Secretaría de Economía elaboró un proyecto de Norma Oficial Mexicana que establecerá los requisitos que deban observarse para la conservación de mensajes de datos, con fundamento en lo dispuesto por el artículo 49 segundo párrafo del Código de Comercio.

ATRIBUCIÓN: La forma en que podemos garantizar que las partes que se obligan en la relación jurídica son quienes dicen ser y expresan su voluntad libre de vicios. Esta atribución a las personas obligadas en la relación jurídica que se pretende formalizar en un mensaje de datos, no es más que una "Firma Electrónica".

ACCESIBILIDAD: Se refiere a que el contenido de un mensaje de datos en el que se consignen contratos, convenios o compromisos que den nacimiento a derechos y obligaciones, pueda estar disponible al usuario (emisor, receptor, juez, auditor, autoridades, etc.) para su ulterior consulta, siempre y cuando reúna las dos características anteriormente anotadas. Para lo cual deberá establecerse en la legislación federal que al efecto deberá emitirse la forma de presentar a "los usuarios" estos mensajes de datos, la cual podría hacerse previa certificación de atribución e integridad por parte del prestador de servicios de certificación.

Por otro lado existe falta de técnica legislativa que se hace patente en la redacción del primer párrafo del artículo 49 del Código de Comercio, que señala: "Los comerciantes están obligados a conservar por un plazo mínimo de diez años los originales de aquellas cartas, telegramas, mensajes de datos o cualesquiera otros documentos en que se consignen contratos, convenios o compromisos que den nacimiento a derechos y obligaciones. " , toda vez que el Código Civil Federal en su artículo 1793 establece que "los convenios que producen o transfieren las obligaciones y derechos, toman el nombre de contratos". Actualmente se está trabajando en algunos proyectos legislativos como son las reformas al Código de Comercio en materia de firmas electrónicas y prestadores de servicios de certificación, Reformas en materia penal en lo relativo al "crimen electrónico", Protección de datos personales, etc.

En cuanto a la firma es importante destacar que su función más importante es la de ser el instrumento por medio del cual el firmante expresa su voluntad, es la exteriorización de la declaración de voluntad de una persona. Esta exteriorización de la declaración de voluntad puede hacerse por medios electrónicos, siempre que legalmente se atribuya al firmante, es aquí donde cobra fuerza la función identificativa de la misma, para dar certeza de que es él y no un tercero quien asume la obligación.

La firma electrónica, como comentamos, podemos clasificarla de la siguiente manera: SIMPLE definida como los datos en forma electrónica consignados en un mensaje de datos, o adjuntados o lógicamente asociados al mismo, que puedan ser utilizados para identificar al firmante en relación

con el mensaje de datos (partiendo de la presunción, en materia mercantil, de que el mensaje ha sido enviado usando medios de identificación como claves o contraseñas por ambas partes conocidas, para lo cual se requerirá de un acuerdo previo y firmado en forma autógrafa por las partes) o AVANZADA que podemos conceptuar como la firma electrónica que permite la identificación del firmante y ha sido generada bajo su exclusivo control que vincula exclusivamente al mismo con el mensaje de datos al que se adjunta o se asocia, lo que permite que sea detectable cualquier modificación ulterior de éste (entendida como proceso electrónico que permite al receptor de un mensaje de datos identificar formalmente a su autor, el cual mantiene bajo su exclusivo control los medios para crear dicha firma, de manera que esté vinculada únicamente a él y a los datos a que se refiere el mensaje, permitiendo detectar cualquier modificación ulterior al contenido del mismo, garantizando así la identidad del titular y que éste no pueda desconocer la autoría del documento. Por lo que será necesario que se expida legislación federal relativa a la firma electrónica "avanzada" en la que se regule la actividad de los prestadores de servicios de certificación, a los propios certificados de firmas electrónicas, así como la admisibilidad y forma de presentar como prueba en juicio a los mensajes de datos firmados y se establezcan los requisitos técnicos necesarios.

Debemos distinguir entre lo que comúnmente se denomina "firma digital" y la "firma electrónica avanzada", ya que la primera es una especie de la segunda, esto es, la firma digital es una firma electrónica avanzada elaborada bajo los estándares de la tecnología PKI. Esto quiere decir que denominarla firma digital nos limitaría a una tecnología de encriptación y violaríamos el principio internacional de Neutralidad Tecnológica. Por último presentamos un proyecto concreto de reformas al Código de Comercio en materia de firma electrónica y prestadora de servicios de certificación.

2.6 **ERICK IRIARTE AHON**, publicó una artículo respecto a la "Violencia en Internet, ¿Quién defiende a los Internautas?. Sobre el abuso del Correo Electrónico" en la Revista Electrónica de Derecho Informático Alfa – Redi No. 006 - Enero del 1999, donde indica que: "La Violencia es reconocida como tal tanto por la víctima como por el perpetrador, y por todos aquellos que tienen conocimiento de ella. La atrocidad nunca equilibra ni rectifica errores del pasado. La violencia simplemente arma al futuro para mayores violencias. Se

perpetúa en sí misma. Una forma bárbara de incesto. Cualquiera que comete una violencia comete también todas las violencias futuras generadas por ella. Los Apócrifos de Muad'Dib".

2.7 **LUIS MIGUEL REYNA ALFARO**, publicó un artículo llamado “El Bien Jurídico en el Delito Informático”, en la Revista Electrónica de Derecho Informático – ALFA REDI, N° 33 Abril de 2001, donde señala que: “Los constantes avances tecnológicos en materia informática han propiciado la aparición de nuevos conceptos, generando asimismo la modificación de otros tantos, enriqueciéndolos la mayoría de ocasiones, así el contenido del término información, que según la definición de la Real Academia de la Lengua Española significa: enterar, dar noticia de algo y que en términos legos hubiera significado tan sólo una simple acumulación de datos, se ha ampliado, transformándose como advierte Gutiérrez Francés: "en un valor, un interés social valioso, con frecuencia cualitativamente distinto, dotado de autonomía y objeto del tráfico". Asimismo, indica que: Hoy en día no resulta suficiente poseer la información, es necesario además tener la capacidad de almacenarla, tratarla y transmitirla eficientemente, de allí que la información deba ser entendida como un proceso en el cual se englobe los tres supuestos (almacenamiento, tratamiento y transmisión).

2.8 **RENATO JAVIER JIJENA**, publicó un artículo titulado “Sobre la no protección de la intimidad en Chile”, en la Revista Electrónica de Derecho Informático – ALFA – REDI, N° 39, octubre 2001, quien indica que si bien es cierto el problema de la protección legal de datos personales frente al tratamiento computacional de los mismos es un tema con bastante perspectiva en países extranjeros, en Chile constituye una realidad desconocida y poco estudiada jurídicamente. Digamos desde ya que este tema, el de los "datos personales o nominativos procesados computacionalmente" va mucho más allá que el problema de los protestos, de la morosidad comercial y de los archivos históricos almacenados en bancos de datos. En el Capítulo I se plantean los elementos conceptuales y doctrinarios necesarios para entender cuál es el problema de fondo que pretende solucionar el denominado "Derecho de la Protección de Datos", asimismo, en el Capítulo II, recogiéndose los elementos previamente expuestos se revisa brevemente cuál es el contenido y los alcances de los artículos que la conforman, para cerrar los comentarios formulando algunas observaciones generales a la ley.

3. OBJETIVOS DE LA INVESTIGACIÓN

3.1 OBJETIVO GENERAL

Demostrar que el problema de los **delitos informáticos** se debe a que su tipificación en el **Código Penal** vigente, es deficiente e inoperante frente a los ilícitos que originan el avance tecnológico.

3.2 OBJETIVOS ESPECÍFICOS

1. Comprobar que el incremento de la **piratería informática** afecta el derecho de autor y el **patrimonio** de personas y empresas de software, debido a la inadecuada tipificación en la legislación penal.
2.- Demostrar que el incremento de los delitos realizados por **medios informáticos**, se debe a consecuencia del avance y desarrollo tecnológico e informático, originando ilícitos que atente **contra la vida el cuerpo y la salud** de las personas.
3.- Demostrar que el incremento de la **pornografía infantil por Internet**, se debe a la inoperancia de la legislación penal, originando el incremento de ilícitos que atentan **contra pudor, honor e intimidad** de los menores de edad.

4. HIPÓTESIS

4.1 HIPOTESIS GENERAL

Si se incrementa la comisión de los **delitos informáticos**, entonces el **Código Penal** vigente tiene deficiencias en su aplicación.

4.2 HIPOTESIS SECUNDARIAS

1. El incremento de la **piratería informática** se debe a que la legislación penal actual es deficiente, originando el incremento y desprotección del derecho de autor y **patrimonio.**

2. A mayor incremento de los delitos realizados por **medios informáticos**, mayor incremento de delitos que atentados contra **la vida el cuerpo y la salud**.

3. El incremento de la **pornografía infantil por Internet** se debe a la deficiente e inoperancia de la legislación penal, originando el incremento de delitos que **atentan contra el pudor, honor y la intimidad** de menores de edad**.**

4.3 IDENTIFICACIÓN Y CLASIFICACIÓN DE LAS VARIABLES

VARIABLES INDEPENDIENTES	DEFINCIÓN	INDICADORES
Variable Independiente: X **"**Delitos Informáticos**"**	***Los Delitos Informáticos*** son "…actitudes ilícitas en que se tienen a las computadoras como instrumento o fin" (concepto atípico) o las "conductas típicas, antijurídicas y culpables en que se tienen a las computadoras como instrumento *o* fin…'' (concepto típico).	X1 Difícil control e investigación X2 Crea caos social X3 Atenta contra bienes jurídicos protegidos
Variable Independiente: VI1 "Piratería Informática"	**Piratería Informática,** consiste en copiar, reproducir, vender, entrega un programa de software que no le pertenece o que no tiene licencia de uso, a pesar de que el programa está correctamente registrado como propiedad intelectual en su país de origen o en otro país; asimismo adultera su estructura, su procedimiento de instalación, copiándo directamente y reproduciendo por cualquier medio la documentación que acompaña al mismo programa.	
Variable Independiente: VI2 "Medios Informáticos"	**Medios Informáticos**, son todos los dispositivo o grupo de elementos relacionados que realiza el tratamiento automatizado de datos, que implica el generar, enviar, recibir, procesar, o almacenar información.	
Variable Independiente: VI3 "Pornografía infantil por Internet"	**Pornografía Infantil**, consiste con o sin su conocimiento, obligar o induzca a realizar actos de exhibicionismo corporal, lascivos, o pornográficos con el objeto y fin de videograbarlos, fotografiarlos o exhibirlos mediante medios impresos, electrónicos o de un sistema de datos a través de cómputo o de cualquier otro mecanismo de archivos de datos, con o sin el fin de obtener un lucro.	
VARIABLES DEPENDIENTES	**DEFINCIÓN**	**INDICADORES**
Variables Dependientes: Y "Código Penal"	**Código Penal,** es el conjunto unitario y sistematizado de las normas jurídicas punitivas de un Estado, es decir, un compendio ordenado de la legislación aplicable en materia penal, que busca la eliminación de redundancias, la ausencia de lagunas y la universalidad: esto es, que no existan normas penales vigentes fuera del compendio.	Y1 Vacío legal Y2 ineficiente Y3 No acorde con avance tecnológico
Variable Dependiente: VD1 "Patrimonio"	**Patrimonio,** desde el punto de vista jurídico, es la universalidad constituida por el conjunto de derechos y obligaciones que corresponden a una persona y pueden ser apreciables en dinero (Osorio	
Variable Dependiente: VD2 "Delitos contra la vida el cuerpo y la salud"	**Los Delitos Contra la Vida el Cuerpo y la Salud, se encuentran tipificados en el "Artículo 121º del Código Penal:** El que causa a otro daño grave en el cuerpo o en la salud, será reprimido con pena privativa de libertad no menor de tres ni mayor de ocho años".	
Variable Dependiente: VD3 "Honor e intimidad"	**Honor**, jurídicamente constituye el derecho que cada ser humano tiene al reconocimiento y respeto, antes él mismo y ante las demás personas, de su dignidad humana y de los demás méritos y cualidades que han ido adquiriendo como fruto de su desarrollo personal y social. ***Intimidad,*** como amistad intima. Es causa de recusación testimonial, pericial y judicial. Parte personalísima y reservado de un caso o persona, su revelación puede originar responsabilidad cuando cause perjuicio y haya dolo o grave imprudencia; pero, si se trata de actividad preliminar del delito, entonces la denuncia resulta a veces deber.	

III. PLANTEAMIENTO OPERACIONAL

1. TÉCNICAS, INSTRUMENTOS Y MATERIALES DE VERIFICACIÓN

1.1 Tipo de Investigación

El presente trabajo es una investigación APLICATIVA, que requiere de una descripción de las características más significativas de los delitos informáticos y el Código Penal, por lo que se propone que el Estado realice denodados esfuerzos para hacer frente a estos delitos de nueva data, es así que incluyó en el Código Penal vigente a los Delitos Informáticos; así como la creación de la División de Investigación de Delitos de Alta Tecnología, no es suficiente para hacer frente a esta nueva forma de criminalidad, al respecto con la finalidad de hacer frente en una forma más eficiente, es recomendable la creación de una ley especial contra los delitos informáticos, donde se encuentre tipificado las diferentes formas de criminalidad, así como las sanciones correspondientes y atribuciones de la Policía Nacional al momento de realizar la investigación en una forma más rápida y eficiente.

1.2 Nivel de Investigación

Descriptivo, por cuanto se describirá a los delitos informáticos, los mismos que en la actualidad se vienen incrementando de forma muy rápida y que existe una deficiente intervención por parte de la Policía Nacional, Ministerio Público y Poder Judicial, al momento de la comisión de estos ilícitos por parte de los delincuentes informáticos, los cuales se incremente debido a la falta de tecnología y capacitación del personal encargado de realizar las investigaciones. En cuanto a la legislación penal, se advierte que tenemos un Código Penal obsoleto, por cuanto no va acorde con el avance de estos delitos de nueva data.

Explicativo, por cuanto explicarán las causas que originan el incremento de los delitos informáticos y las deficiencias existentes en la legislación penal vigente, asimismo, cuales son las causas que originan que estos delitos no sean denunciados, investigaciones o sancionados de forma eficiente tanto a nivel policial y judicial.

Correlativo, debido a que contrastaremos la legislación peruana con la legislación española, argentina y venezolana entre otras; asimismo, contrastaremos el enfoque que tienen los diferentes Códigos Penales respecto a los delitos informáticos de algunos países de América y Europa, lo que nos permitirá un mayor panorama del tema.

1.3 Método:

Los métodos utilizados en la presente investigación permitirán describir y analizar las características de **Los Delitos Informáticos** y el **Código Penal,** lo que permite presentar una síntesis del trabajo de investigación que será reforzada con una constatación estadística nacional, siendo los métodos aplicados en el presente trabajo de investigación son:

- **Descriptivo**, la presente investigación describe y analiza las características y diferentes formas y clases de **Delitos Informáticos,** así como los delitos que pueden ser realizados por medios informáticos en el **Código Penal** vigente**,** lo que nos permitirá tener un panorama más amplio sobre el tema de investigación, así como una síntesis del trabajo de investigación que será reforzada con una constatación estadística nacional.

- **Explicativo,** debido a que explicaremos cuales son las causas que originan el incremento de los delitos informáticos y su tipificación de los delitos informáticos en el Código Penal, con la finalidad de establecer cuales son los efectos que ocasionan en la sociedad y menores de edad.

- **Inductivo – Deductivo,** indicaremos cuales son las razones que han originado el incremento de los delitos informáticos y las deficiencias existentes en el Código Penal vigente, siendo en la actualidad la principal razón el incremento de la tecnología y su falta de regulación.

- **Analítico**, analizaremos como se ha tratado y se viene tratando en la actualidad; así como cual sería la forma más adecuada para contrarrestar el incremento de los delitos informáticos, dicho análisis se efectuará tanto a nivel nacional e internacional.

1.4 Diseño

El diseño que utilizaré en mi investigación será por objetivos conforme al esquema siguiente:

OG – OBJETIVO GENERAL

OE – OBJETIVO ESPECÍFICO

CP – CONCLUSIÓN PARCIAL

HG – HIPÓTESIS GENERAL

CF – CONCLUSIÓN FINAL

	Objetivo Especifico 1 Comprobar que el incremento de la **piratería informática** afecta el derecho de autor y el **patrimonio** de personas y empresas de software, debido a la inadecuada tipificación en la legislación penal.	**Conclusión Parcial 1** Existe deficiencia en la legislación penal vigente y falta de una política por parte del Estado para poder combatir la piratería informática.	
OBJETIVO GENERAL Demostrar que el problema de los **delitos informáticos** se debe a que su tipificación en el **Código Penal** vigente, es deficiente e inoperante frente a los ilícitos que originan el avance tecnológico.	**Objetivo Especifico 2** Demostrar que el incremento de los delitos realizados por **medios informáticos**, se debe a consecuencia del avance y desarrollo tecnológico e informático, originando ilícitos que atente **contra la vida el cuerpo y la salud** de las personas.	**Conclusión Parcial 2** La legislación penal actual es ineficiente frente incremento de los delitos realizados por medios informáticos	**HIPÓTESIS GENERAL** Si se incrementa la comisión de los **delitos informáticos**, entonces el **Código Penal** vigente tiene deficiencias en su aplicación.
	Objetivo Especifico 3 Demostrar que el incremento de la **pornografía infantil por Internet**, se debe a la inoperancia de la legislación penal, originando el incremento de ilícitos que atentan **contra pudor, honor e intimidad** de los menores de edad.	**Conclusión Parcial 3** Existe inoperancia en la legislación penal vigente, originado el incremento de los delitos informáticos	**CONCLUSIÓN FINAL** El incremento de los delitos informáticos se debe al avance de la ciencia tecnología, telemática e Internet, lo cual origina que el Código Penal vigente se vea rebasado, por lo que urge que legisle al respecto y se fomente una política de prevención por parte del Estado.

2. CAMPO DE VERIFICACIÓN

2.1 UBICACIÓN ESPACIAL

El presente trabajo de investigación, tiene por delimitación espacial, la Ciudad de Lima.

2.2 UBICACIÓN TEMPORAL

La presente investigación va ha realizada desde enero del 2007 a fines del 2009, tiempo suficiente para poder recolectar y analizar la información obtenida.

2.3 UNIDAD DE ESTUDIO

2.3.1 POBLACIÓN

La población seleccionada en la presente investigación está constituida en la siguiente unidad de análisis:

- El ámbito es la Ciudad de Lima, específicamente Personal de la Policía Nacional, Jueces, Fiscales, Abogados.

2.3.2 MUESTRA

Para la selección de la Muestra se identificarán los siguientes procedimientos y técnicas:

- 10 Efectivos policiales
- 05 Fiscales Penales
- 05 Jueces Penales
- 24 Abogados

3. ESTRATEGIA DE RECOLECCIÓN DE DATOS

Para realizar la presente investigación se utilizará las técnicas más típicas y que son aplicables a la ciencia del Derecho.

3.1 ENCUESTA

Este instrumento se ha elaborado en función del problema planteado, la hipótesis y las variables identificadas, para lo cual se han precisado las preguntas más adecuadas en el instrumento cuestionario, teniendo en cuenta el tipo de población y siguiendo los criterios científicos a efectos de recoger concienzudamente esta información.

3.2 ANÁLISIS DOCUMENTAL

Esta técnica estará en función del análisis doctrinario, teórico, procesal respectivo de las diversas obras, así como de la legislación comparada a países europeos y americanos.

3.3 ANÁLISIS MICRO COMPARATIVO DE SISTEMAS JURÍDICOS EXTRANJEROS

Para el mejor cumplimiento de esta técnica he visto por conveniente elegir adecuadamente cuáles van a ser los sistemas jurídicos extranjeros que van a ser objeto de comparación y confrontación, a fin de determinar las semejanzas y diferencias que pudieran existir entre ellas, para lo cual hemos planteado un Diseño que ha permitido identificarlos.

3.4 FICHAS DE INFORMACIÓN JURÍDICA

Considerando los criterios metodológicos al momento de recolectar la información hemos trabajado con fichas a fin de almacenar y procesarla en la elaboración del Informe Final.

3.5 OBSERVACIÓN

Acudiremos ha observar in situ cómo se vienen ejecutando actualmente las investigaciones tanto a nivel Policial, Fiscal y/o Judicial de los delitos cometidos por medios informáticos, a fin de conocer su realidad objetivamente.

3.6 ESTUDIOS DE CASOS

En esta parte se analizó diversos casos de delitos informáticos, con el fin de conocer las deficiencias y dificultades en estas acciones para proponer alternativas validas y confiables al problema.

4. TÉCNICAS DE PROCESAMIENTO Y ANÁLISIS DE DATOS RECOLECTADOS

4.1 SELECCIÓN Y REPRESENTACIÓN POR VARIABLES.

Luego de haber realizado el trabajo de campo y concluido con la toma de las encuestas, se han seleccionado las respuestas de acuerdo a las variables formuladas.

4.2 MATRIZ TRIPARTITA DE DATOS

En este instrumento almacenamos provisionalmente la información obtenida y que previamente ha sido seleccionada o representada por el investigador.

4.3 UTILIZACIÓN DE PROCESADOR SISTEMATIZADO

La información clasificada y almacenada en la Matriz de datos, la hemos trasladado a un procesador de sistema de cómputo que nos ha permitido realizar las técnicas estadísticas apropiadas, teniendo en cuenta el Diseño formulado para la Contrastación de las hipótesis; en este caso hemos trabajado con el Programa Microsoft Word y Excel de Office.

4.4 PRUEBA ESTADÍSTICAS

Se trabajó en función de las diversas técnicas estadísticas de acuerdo al seguimiento del Diseño respectivo: Distribución de frecuencias, tablas cruzadas, la asociación y correlación entre variables.

IV. CRONOGRAMA DE TRABAJO Y PRESUPUESTO

1. CRONOGRAMA DE TRABAJO

	2009									2010		
Actividades	**A**	**M**	**J**	**J**	**A**	**S**	**O**	**N**	**D**	**E**	**F**	**M**
1. Determinación del Problema	X											
2. Acopio bibliográfico	X											
3. Selección bibliográfica	X											
4. Elaboración de la matriz de consistencia		X										
5. Redacción de antecedentes de investigación			X									
6. Elaboración de Instrumentos de investigación			X									
7. Revisión y aprobación de proyecto de investigación				X								
8. Encuesta				X								
9. Codificación				X								
10. Tabulación					X							
11. Análisis e interpretación de datos						X	X					
12. Redacción preliminar del informe final								X	X	X		
13. Presentación del Proyecto de Tesis para su aprobación											X	
14. sustentación												X

2. PRESUPUESTO

BIENES		
CANTIDAD	**DESCRIPCIÓN DE LOS BIENES**	**TOTAL**
02 Millares	Papel bond A4 80 gramos	50.00
01 unidad	USB 2 Gigas	100.00
10 unidades	Plumones Faver Castell Nro. 47	20.00
06 litros	Obras básicas de Consulta	400.00
SERVICIOS		
04 ejemplares	Empastados del Informe de tesis	80.00
1000 unidades	Copias Fotostática	50.00
250 unidades	Digitación	300.00
01 un	Programador	250.00
01	Movilidad e imprevistos	200.00
	TOTAL	**1.450.00**

V. ANEXOS

ANEXO “A”

MATRIZ DE CONSISTENCIA (ESTRUCTURA ANALÍTICA)

ANEXO "B"

"UNIVERSIDAD CATÓLICA DE SANTA MARÍA"
ESCUELA DE POST GRADO
MAESTRÍA EN DERECHO PENAL

ENCUESTA

DIAGNÓSTICO SITUACIONAL SOBRE LOS DELITOS INFORMÁTICOS EN EL CÓDIGO PENAL

ENCUESTA DIRIGIDA A: JUECES, FISCALES, ABOGADOS Y EFECTIVOS PNP

Estimado Sr., con fines estrictamente académicos se ha elaborado el presente cuestionario, a efectos de que con vuestra valiosa ayuda se haga un diagnóstico sobre LOS DELITOS INFORMÁTICOS EN EL CÓDIGO PENAL, agradeciendo su colaboración por señalar la respuesta que crea pertinente.

I.- DATOS DEL ENCUESTADO:

Sexo : ☐ Edad: ☐

Cargo que Ocupa:……

II.- DELITOS INFORMATICOS Y CODIGO PENAL

1. ¿Considera usted que a través de las computadoras, el Internet y la informática se pueden realizar algunos delitos informáticos?

   Si No

   Explique: _____
   _____

2. ¿Considera usted que con la aparición del Internet y el desarrollo de la tecnología e informática han ocasionado el incremento de los delitos informáticos?

   Si No

   Explique: _____
   _____

3. ¿Qué tipos de delitos informáticos en Lima conoce usted?

   _____
   _____
   _____

4. De estos delitos, ¿Cuáles considera que son menos denunciados?

   _____

   Explique: _____
   _____

5. Según usted, marque con una "X" a que y quienes afecta los delitos informáticos:
   a. A la persona, a la Sociedad
   b. A la intimidad, al honor
   c. A lo económico, al patrimonio
   d. A la información, al Software, al Hardware
   e. Otros:_____

6. ¿Quiénes considera que son los más afectados?

_____

7. Según usted, marque con una "X" a los delitos que pueden ser cometidos a través de medios informáticos (computadora, Internet, sistemas informáticos):
   a. Delitos contra la vida, el cuerpo y la salud, contra la sociedad
   b. Delitos contra la intimidad y el honor
   c. Delitos contra el orden económico, patrimonio, robo, hurto
   d. Delito de Secuestro
   e. Delito contra la fe pública
   f. Lavado de dinero, terrorismo
   g. Otros: _____

8. Durante su experiencia en esta actividad de la computación e informática, ¿cómo se han presentado estos delitos?

_____
_____
_____

9. ¿Considera usted que algunos delitos informáticos tienden a quedarse impunes?

Explique: _____
_____
_____

10. Dentro de nuestro Código Penal, ¿considera usted que los delitos informáticos más frecuentes se dan en el sector económico o patrimonial?

Si No

Explique: _____
_____

11. ¿De qué manera se presenta el delito informático en el trabajo que usted realiza?

_____
_____
_____

12. ¿Qué aportes puede usted brindar respecto a los delitos informáticos, basándose en su experiencia?

_____
_____
_____

Fecha de aplicación

Día	Mes	Año

ANEXO "C"

FICHA BIBLIOGRAFICA (A)

Nº: _____

NOMBRE DE AUTOR:

TITULO DE LIBRO:

EDITORIAL LUGAR AÑO:

NOMBRE DE LA BIBLIOTECA:

CODIGO:

ANEXO "D"

FICHA BIBLIOGRAFICA (B)

Nº: _____

NOMBRE DEL PORTAL:

TITULO DEL ITEM:

AUTOR:

LUGAR, AÑO:

ANEXO "E"

FICHA BIBLIOGRAFICA (C)

INDICADOR:
SUBINDICADOR:

TITULO:
NOMBRE DEL AUTOR:
TIPO DE PRODUCCIÓN:
FECHA:
COMENTARIO O CITA:

ANEXO (02)

LEGISLACIÓN PERUANA RELACIONADA CON EL TEMA DE INVESTIGACIÓN

1. LEY Nº 27269 DE FIRMAS Y CERTIFICADOS DIGITALES, aprobado con fecha 04 mayo 2000 (con la modificación del art.11 introducido por la ley 27310 del 26.6.21001)

Artículo 1- Objeto de la ley
La presente ley tiene por objeto regular la utilización de la firma electrónica otorgándole la misma validez y eficacia jurídica que el uso de una firma manuscrita u otra análoga que conlleve manifestación de voluntad.
Entiéndase por firma electrónica a cualquier símbolo basado en medios electrónicos utilizado o adoptado por una parte con la intención precisa de vincularse o autenticar un documento cumpliendo todas o algunas de las funciones características de una firma manuscrita.

Artículo 2 - Ámbito de aplicación
La presente ley se aplica a aquellas firmas electrónicas que, puestas sobre un mensaje de datos o añadidas o asociadas lógicamente a los mismos, puedan vincular e identificar al firmante, así como garantizar la autenticación e integridad de los documentos electrónicos.

De la firma digital

Artículo 3 - Firma digital
La firma digital es aquella firma electrónica que utiliza una técnica de criptografía asimétrica, basada en el uso de un par de claves único; asociadas una clave privada y una clave pública relacionadas matemáticamente entre sí, de tal forma que las personas que conocen la clave pública no puedan derivar de ella la clave privada.

Del titular de la firma digital

Artículo 4 - Titular de la firma digital
El titular de la firma digital es la persona a la que se le atribuye de manera exclusiva un certificado digital que contiene una firma digital, identificándolo objetivamente en relación con el mensaje de datos.

Artículo 5 - Obligaciones del titular de la firma digital
El titular de la firma digital tiene la obligación de brindar a las entidades de certificación y a los terceros con quienes se relacione a través de la utilización de la firma digital, declaraciones o manifestaciones materiales exactas y completas.

De los certificados digitales

Artículo 6 - Certificado digital
El certificado digital es el documento electrónico generado y firmado digitalmente por una entidad de certificación, la cual vincula un par de claves con una persona determinada confirmando su identidad.

Artículo 7 - Contenido del certificado digital
Los certificados digitales emitidos por las entidades de certificación deben contener al menos:
1. Datos que identifiquen indubitablemente al suscriptor.
2. Datos que identifiquen a la Entidad de Certificación.
3. La clave pública.
4. La metodología para verificar la firma digital del suscriptor impuesta a un mensaje de datos.
5. Número de serie del certificado.
6. Vigencia del certificado.
7. Firma digital de la Entidad de Certificación.

Artículo 8 - Confidencialidad de la información
La entidad de registro recabará los datos personales del solicitante de la firma digital directamente de éste y para los fines señalados en la presente ley.
Asimismo la información relativa a las claves privadas y datos que no sean materia de certificación se mantiene bajo la reserva correspondiente. Sólo puede ser levantada por orden judicial o pedido expreso del suscriptor de la firma digital.

Artículo 9 - Cancelación del certificado digital
La cancelación del certificado digital puede darse:
1. A solicitud del titular de la firma digital.
2. Por revocatoria de la entidad certificante.
3. Por expiración del plazo de vigencia.
4. Por cese de operaciones de la Entidad de Certificación.

Artículo 10 - Revocación del certificado digital
La Entidad de Certificación revocará el certificado digital en los siguientes casos:
1. Se determine que la información contenida en el certificado digital es inexacta o ha sido modificada.
2. Por muerte del titular de la firma digital.
3. Por incumplimiento derivado de la relación contractual con la Entidad de Certificación.

Artículo 11 - Reconocimiento de certificados emitidos por entidades extranjeras
Los Certificados de Firmas Digitales emitidos por Entidades Extranjeras tendrán la misma validez y eficacia jurídica reconocidas en la presente Ley, siempre y cuando tales certificados sean reconocidos por la autoridad administrativa competente. **(Nuevo texto conforme modificación dispuesta por la ley 27310 del 26.6.2001)**
El texto anterior que fue modificado decía: *"Los Certificados de Firmas Digitales emitidos por entidades extranjeras tendrán la misma validez y eficacia jurídica reconocida en la presente ley, siempre y cuando tales certificados sean reconocidos por una entidad de certificación nacional que garantice, en la misma forma que lo hace con sus propios certificados, el cumplimiento de los requisitos, del procedimiento, así como la validez y la vigencia del certificado. "*

De las Entidades de Certificación y de Registro

Artículo 12 - Entidad de Certificación
La Entidad de Certificación cumple con la función de emitir o cancelar certificados digitales, así como brindar otros servicios inherentes al propio certificado o aquellos que brinden seguridad al sistema de certificados en particular o del comercio electrónico en general.
Las Entidades de Certificación podrán igualmente asumir las funciones de Entidades de Registro o Verificación.

Artículo 13 - Entidad de Registro o Verificación
La Entidad de Registro o Verificación cumple con la función de levantamiento de datos y comprobación de la información de un solicitante de certificado digital; identificación y autenticación del suscriptor de firma digital; aceptación y autorización de solicitudes de emisión de certificados digitales; aceptación y autorización de las solicitudes de cancelación de certificados digitales.

Artículo 14 - Depósito de los Certificados Digitales
Cada Entidad de Certificación debe contar con un Registro disponible en forma permanente, que servirá para constatar la clave pública de determinado certificado y no podrá ser usado para fines distintos a los estipulados en la presente ley.
El Registro contará con una sección referida a los certificados digitales que hayan sido emitidos y figurarán las circunstancias que afecten la cancelación o vigencia de los mismos, debiendo constar la fecha y hora de inicio y fecha y hora de finalización.
A dicho Registro podrá accederse por medios telemáticos y su contenido estará a disposición de las personas que lo soliciten.

Artículo 15 - Inscripción de Entidades de Certificación y de Registro o Verificación
El Poder Ejecutivo, por Decreto Supremo, determinará la autoridad administrativa competente y señalará sus funciones y facultades.
La autoridad competente se encargará del Registro de Entidades de Certificación y Entidades de Registro o Verificación, las mismas que deberán cumplir con los estándares técnicos internacionales.
Los datos que contendrá el referido Registro deben cumplir principalmente con la función de identificar a las Entidades de Certificación y Entidades de Registro o Verificación.

Artículo 16 - Reglamentación
El Poder Ejecutivo reglamentará la presente ley en un plazo de 60 (sesenta) días calendario, contados a partir de la vigencia de la presente ley.

Disposiciones Complementarias, Transitorias y Finales

Primera.- Mientras se cree el Registro señalado en el artículo 15.°, la validez de los actos celebrados por Entidades de Certificación y Entidades de Registro o Verificación, en el ámbito de la presente ley, está condicionada a la inscripción respectiva dentro de los 45 (cuarenta y cinco) días siguientes a la creación el referido Registro.

Segunda.- El Reglamento de la presente ley incluirá un glosario de términos referidos a esta ley y a las firmas electrónicas en general, observando las definiciones establecidas por los organismos internacionales de los que el Perú es parte.

Tercera.- La autoridad competente podrá aprobar la utilización de otras tecnologías de firmas electrónicas siempre que cumplan con los requisitos establecidos en la presente ley, debiendo establecer el Reglamento las disposiciones que sean necesarias para su adecuación."

2. REGLAMENTARIO DE LA LEY Nº 27269 LEY DE FIRMAS Y CERTIFICADOS DIGITALES, APROBADO MEDIANTE DECRETO SUPREMO Nº 019-2002

EL PRESIDENTE DE LA REPÚBLICA
CONSIDERANDO:
Que, mediante Ley Nº 27269, se aprobó la Ley de Firmas y Certificados Digitales; disponiendo en su Artículo 16º. que el Poder Ejecutivo reglamentará la citada Ley.

Que, mediante Ley No. 27310, se modificó el Artículo 11º. de la referida Ley, en el sentido, que los Certificados de Firmas Digitales emitidos por Entidades Extranjeras tendrán la misma validez y eficacia jurídica reconocidas en la Ley N0 27289, siempre y cuando, tales certificados sean reconocidos por la Autoridad Administrativa Competente;

Que, la Autoridad Administrativa Competente de conformidad con lo establecido en el Artículo 15º. de la Ley No. 27269, será determinada por el Poder Ejecutivo, estableciendo sus funciones;

Que, por Resolución Suprema N' 098-2000-JUS, se designó la Comisión Multisectorial encargada de elaborar el Reglamento de la Ley de Firmas y Certificados Digitales;

Que, mediante Resolución Suprema N' 280-2001 -JUS, se dio por concluida la labor de la Comisión Multisectorial citada en el considerando anterior, publicándose el Proyecto de Reglamento en el Diario Oficial para los comentarios y sugerencias del caso;

Que, el Ministerio de Justicia ha cumplido con evaluar los diversos comentarios y sugerencias recibidas, incorporándose los aportes pertinentes que han enriquecido y mejorado el Reglamento;

Que, es necesario aprobar el Reglamento de la Ley de Firmas y Certificados Digitales - Ley N' 27269, que permitirá poner en práctica y difundir en el más breve el uso de las Firmas Electrónicas, así como las Firmas y Certificados Digitales, a través de la adecuada regulación de las Entidades de Certificación y de las Entidades de Registro o Verificación;
De conformidad con lo dispuesto en el inciso 8) del Artículo 118' de la Constitución Política del Perú;

DECRETA:
Articulo 1º. - Aprobar el Reglamento de la Ley de Firmas y Certificados Digitales - Ley N' 27269, que consta de tres (3) Títulos, cincuenta (50) Artículos y dos (2) Disposiciones Finales.

Artículo 2º. - Designar al instituto Nacional de Defensa de la Competencia y la Protección de la Propiedad Intelectual (INDECOPI) como la autoridad administrativa competente, conforme a lo establecido en el Artículo 15'de la Ley N'27269

Articulo 3º.- El presente Decreto Supremo será refrendado por el Presidente del Consejo de Ministros y por el Ministro de Justicia.
Dado en la Cesa de Gobierno, a los diecisiete días del mes de mayo del año dos mil dos.
RAÚL DIEZ CANSECO TERRY
Primer Vicepresidente de la República
Encargado del Despacho Presidencial

ROBERTO DAÑINO ZAPATA
Presidente del Consejo de Ministros
FERNANDO ROSPIGLIOSI C.
Ministro del Interior
Encargado de la Cartera de Justicia

REGLAMENTO DE LEY Nº 27269
"LEY DE FIRMAS Y CERTIFICADOS DIGITALES"
TITULO 1
NORMAS GENERALES
CAPITULO 1

Artículo 1º. - Objeto
El Reglamento regula, para el sector público y privado, la utilización de firmas electrónicas en mensaje de datos y documentos electrónicos, generadas bajo la Infraestructura Oficial de Firma Electrónica comprendiendo el régimen de acreditación y supervisión de las entidades de certificación, así como do las entidades de registro o verificación, establecidas en la Ley Nº 27269 - Ley de Firmas y Certificados Digitales, modificada en su Artículo 11 por la Ley Nº 27310.

Cuando en el Reglamento so haga referencia a la Ley, debe entenderse referida a la Ley N' 27269, Ley de Firmas y Certificados Digitales. Cuando se mencione el Reglamento debe entenderse referido al presente Reglamento, de la Ley N' 27269.

Las firmas electrónicas aprobadas por la autoridad administrativa competente, tienen, desde su aprobación los mismos efectos que las firmas generadas bajo la Infraestructura Oficial de Firma Electrónica conforme a lo establecido en el Reglamento.

Artículo 2º. - Principio de la autonomía de la voluntad
Las disposiciones contenidas en el Reglamento no restringen la autonomía privada para el uso de otras firmas electrónicas generadas fuera de la Infraestructura Oficial de Firma Electrónica, ni afecta los pactos que acuerden las partes sobre validez y eficacia jurídica de la firma electrónica conforme a lo establecido en el Artículo 1' de la Ley.

Artículo 3º. Régimen de servicios de certificación
La prestación de servicios de certificación así como los de registro o verificación se sustenta en el principio de libre competencia y en el marco de una economía social de mercado.

Artículo 4º. - Definiciones
Para efectos del Reglamento, entiéndase por:
Acreditación.- Proceso a través dei cual la autoridad administrativa competente, previo cumplimiento de las exigencias establecidas en la Ley, faculta a las entidades solicitantes reguladas en el Reglamento a prestar los servicios solicitados en el marco de la Infraestructura Oficial de Firma Electrónica.

Agente automatizado.- Procesos y equipos programados para atender requerimientos predefinidos y dar una respuesta automática sin Intervención humana, en dicha fase.
Algoritmo.- Conjunto ordenado y finito de operaciones matemáticas que permiten hallar la solución a un problema.

Autenticación.- Proceso técnico que permite determinar la identidad de la persona que firma electrónicamente, en función del mensaje firmado por éste y al cual se le vincula; este proceso no otorga certificación notarial ni fe pública.

Autoridad Administrativa Competente.- Organismo público responsable de acreditar a las entidades de certificación y a las entidades de registro o verificación, de reconocer los estándares tecnológicos aplicables en la Infraestructura Oficial de Firma Electrónica, de supervisar dicha Infraestructura, y las otras funciones señaladas en el Reglamento o aquéllas que requiera en el trans-curso de sus operaciones.

Certificado digital.- Documento electrónico generado y firmado digitalmente por una entidad de certificación el cual vincula un par de claves con una persona natural o jurídica confirmando su identidad.

Certificación Cruzada.- Acto por el cual una entidad de certificación acreditada reconoce la corrección y validez de un certificado digital emitido por otra entidad de certificación, sea nacional, extranjera o internacional, previa autorización de la autoridad administrativa competente; y asume tal certificado como si fuera de propia emisión, bajo su responsabilidad.

Clave privada.- En un sistema de criptografía asimétrica, es aquella que se emplea para generar una firma digital sobre un mensaje de datos y es mantenida en reserva por el titular de la firma digital.

Clave pública.- En un sistema de criptografía asimétrica, es aquella usada por el destinatario de un mensaje de datos para verificar la firma digital puesta en dicho mensaje y que puede ser conocida por cualquier persona.

Código de verificación.- Secuencia de bits de longitud fija obtenida como resultado de procesar un mensaje de datos con un algoritmo, de tal manera que: (1) El mensaje de datos produzca siempre el mismo código de verificación cada vez que se le aplique dicho algoritmo. (2) Sea improbable, a través de medios técnicos, que el mensaje de datos pueda ser derivado o reconstruido a partir del código de verificación producido por el algoritmo. (3) Sea Improbable que, por medios técnicos, se pueda encontrar dos mensajes de datos que produzcan el mismo código de verificación al usar el mismo algoritmo.

Criptografía asimétrica.- Es una técnica basada en el uso do un único par de claves; una clave privada y una clave pública relacionadas matemáticamente entre sí de tal manera que una no pueda operar sin la otra y de tal forma que las personas que conocen la clave pública no puedan derivar de ella la clave privada.

Declaración de prácticas de certificación.- Documento oficialmente presentado por una entidad de certificación a la Autoridad Administrativa Competente, mediante la cual define sus Prácticas de Certificación.

Declaración de Prácticas de Registro o Verificación: Documento oficialmente presentado por una Entidad de Registro o Verificación a la Autoridad Administrativa Competente, mediante la cual define sus Prácticas de Registro o Verificación.

Depósito de certificados digitales.- Sistema de almacenamiento y recuperación de certificados digitales, así como de la información relativa a éstos, disponible por medios telemáticos.

Destinatario.- Persona designada por el iniciador para recibir un mensaje de datos o un documento electrónico, siempre y cuando no actúe a título de Intermediario.

Documento Electrónico.- Conjunto de datos basados en bits o impulsos electromagnéticos, elaborados, generados, transmitidos, comunicados y archivados a través de medios electrónicos, ópticos o cualquier otro análogo.

Entidad de Certificación.- Persona jurídica que presta Indistintamente servicios de producción, emisión, gestión, cancelación u otros servicios inherentes a la certificación digital. Asimismo, puede asumir las funciones de registro o verificación.

Entidad de Certificación Extranjera.- La que no se encuentra domiciliada en el país, ni inscrita en los Registros Públicos del Perú, conforme a la legislación de la materia.

Entidad de Registro o Verificación.- Persona jurídica encargada del levantamiento de datos, la comprobación de éstos respecto a un solicitante de certificado digital, la aceptación y autorización de las solicitudes para la emisión de certificados digitales, así como de la aceptación y 9utorizaclón de las solicitudes de cancelación de certificados digitales.

Estándares Técnicos Internacionales.- Requisitos de orden técnico y de uso internacional que deben observarse en las Prácticas de Certificación para garantizar el intercambio de claves públicas, y la emisión de firmas y certificados digitales, mediante criptografía asimétrica.

Estándares Técnicos Nacionales.- Estándares técnicos aprobados mediante Normas Técnicas Peruanas por la Comisión de Reglamentos Técnicos y Comerciales - CRT del INDECOPI, en su calidad de Organismo Nacional de Normalización.

Firma digital.- Aquella firma electrónica que utiliza una técnica de criptografía asimétrica y que tiene la finalidad de asegurar la Integridad del mensaje de datos a través de un código de verificación, así como la vinculación entre el titular de la firma digital y el mensaje de datos remitido.

Firma electrónica.- Cualquier símbolo basado en medios electrónicos utilizado o adoptado por una parte con la intención precisa de vincularas, autenticar y garantizar la integridad de un documento electrónico o un mensaje de datos cumpliendo todas o algunas de las funciones características de una firma manuscrita.

Reconocimiento.- Proceso a través del cual la autoridad administrativa competente, equipara y reconoce oficialmente a las entidades de certificación extranjeras.

Infraestructura Oficial de Firma Digital.- Sistema confiable, acreditado, regulado, y supervisado por la autoridad administrativa competente en el marco de la Infraestructura Oficial de Firma Electrónica mediante el uso de tecnología de firma digital, en la que participan entidades de certificación y entidades de registro o verificación acreditadas ante la autoridad administrativa competente.

Infraestructura Oficial de Firma Electrónica.- Sistema confiable, acreditado, regulado, y supervisado por la autoridad administrativa competente constituido por programas, equipos, estándares, políticas, procesos, procedimientos u otros recursos que permiten la generación de firmas electrónicas y que garantizan la autenticación e integridad de los documentos electrónicos.

Iniciador.- Persona que haya actuado por su cuenta o a cuyo nombre se haya actuado para enviar o generar un mensaje de datos antes de ser archivado, pero que no haya actuado a título de Intermediario.

Integridad.- Característica que Indica que un mensaje de datos o un documento electrónico no han sido alterados desde la transmisión por el Iniciador hasta su recepción por el destinatario.

Intermediario.- Persona que, actuando por cuenta de otra, envía, recibe o archiva un mensaje de datos o presta otro servicio respecto de él.

Medios Telemáticos.- Conjunto de bienes y elementos técnicos informáticos que en unión con las telecomunicaciones permiten la generación, procesamiento, transmisión, comunicación y archivo de datos e información.

Mensaje de datos.- Es la información generada, transmitida, recibida, archivada, comunicada por medios electrónicos, ópticos o cualquier otro análogo; tales como, el intercambio electrónico de datos (EDI, por sus siglas en inglés), el correo electrónico, el telegrama, el telex, o el telefax, entre otros.
Neutralidad Tecnológica.- Principio que fomenta la creación y uso de diversas tecnologías, sin preferir, restringir, ni discriminar a ninguna de ellas.

Par de claves.- En un sistema de criptografía asimétrica, comprende una clave privada y su correspondiente clave pública, ambas asociadas matemáticamente.
Servicio de Valor Añadido en Firmas Electrónicas. Servicio complementario a las funciones de certificación, verificación o registro al interior de la Infraestructura Oficial de Firma Electrónica, como fuera de ella.

Tiempo Universal Coordinado (UTC). - Hora relacionada con el Meridiano de Greenwich.Titular de certificado digital, - Persona natural o jurídica a quien se le atribuye de manera exclusiva un certificado digital.

Titular de firma digital.- Persona natural a quien se le vincula de manera exclusiva con un mensaje de datos firmado digitalmente utilizando su clave privada.

Por excepción, en el caso de firmas digitales generadas a través de agentes automatizados, se considera titular de la firma digital a la persona natural o jurídica titular del certificado digital a partir del cual se generan dichas firmas digitales.

CAPÍTULO II
VALIDEZ Y EFECTOS JURÍDICOS DE LAS FIRMAS Y DOCUMENTOS ELECTRÓNICOS

Artículo 5º. - Firmas en la Infraestructura Oficial de Firme Electrónica
Toda firma electrónica añadida o asociada lógicamente a un mensaje de datos o a un documento electrónico y generada bajo la infraestructura Oficial de Firma Electrónica, cumple con lo dispuesto en la Ley y el Reglamento.

Artículo 6º. - Validez de otras firmas electrónicas
Para efectos de la manifestación de voluntad, las firmas electrónicas añadidas o asociadas lógicamente a un mensaje de datos o un documento electrónico y generadas fuera de la infraestructura Oficial de Firma Electrónica tendrán la misma validez y eficacia jurídica que las firmas manuscritas, siempre que sean acreditadas o reconocidas por la autoridad administrativa competente.

Artículo 7º. Documentos Firmados Electrónicamente como medio de prueba
Las firmas electrónicas así como los mensajes de datos y documentos firmados electrónicamente podrán ser admitidas como prueba en toda clase de procesos o procedimientos. El Juez podrá solicitar a la autoridad administrativa competente el nombramiento de un perito especializado en firmas electrónicas.

Articulo 8º. - Presunciones acerca de las firmas electrónica, bajo la Infraestructura Oficial de Firme Electrónica
Tratándose de mensaje de datos o documentos firmados electrónicamente con firmas generadas bajo la Infraestructura Oficial de Firma Electrónica, se presume que el documento o mensaje de datos fue enviado y firmado por su titular, de manera tal que identifica y vincula al firmante, y garantiza la autenticación e integridad del mismo.
Las disposiciones y presunciones del Reglamento no excluyen el cumplimiento de las formalidades específicas requeridas para los actos jurídicos y el otorgamiento de fe pública.

Artículo 9º. Tecnologías de firmas electrónicas al Interior de l~ Infraestructura Oficial de Firma Electrónica
La Infraestructura Oficial de Firma Electrónica se puede basar en las siguientes tecnologías de firmas electrónicas:
a) Tecnologías de firmas digitales, sobre la cual se basa la Infraestructura Oficial de Firma Digital.
b) Otras tecnologías de firmas electrónicas que sean aprobadas por la autoridad administrativa competente de acuerdo con el principio de neutralidad tecnológica.

Artículo 10º. - Conservación de mensaje de datos o documentos electrónicos
Cuando el y usuario lo solicite o la legislación exija que los documentos y registros o informaciones requieran de una formalidad adicional para la conservación de mensaje de datos o documentos electrónicos firmados electrónicamente, deberá cumplirse con lo siguiente:
a) Que sean accesibles para su posterior consulta.
b) Que sean conservados con su formato original de generación, envío, recepción u otro formato que reproduzca en forma demostrable la exactitud e integridad del contenido digital o electrónico.
c) Que sea conservado todo dato que permita determinar el origen, destino, fecha y hora el envío y recepción, en concordancia con lo establecido en el Decreto Legislativo N’ 681 y sus normas complementarias.
Cuando los documentos y mensajes de datos firmados electrónicamente sean conservados mediante micro formas y almacenados en micro archivos, se sujetarán a lo dispuesto por el Decreto Legislativo N’ 681 y sus normas modificatorias y reglamentarias. El notarlo o fedatario responsable, que cuente con certificado o diploma de idoneidad técnica, certifica el cumplimiento de los requisitos establecidos en el presente artículo.

TÍTULO II
DE LA INFRAESTRUCTURA OFICIAL DE FIRMA DIGITAL
CAPÍTULO I
ASPECTOS GENERALES

Artículo 11º.- Elemento, de la Infraestructura Oficial de Firma Digital
La infraestructura Oficial de Firma Digital está constituida por:
a) Prácticas de certificación basadas en estándares internacionales o compatibles a los empleados internacionalmente, de acuerdo con lo establecido por la autoridad administrativa competente.
b) El soporte lógico o conjunto de instrucciones para los equipos de cómputo y comunicaciones, los

elementos físicos y demás componentes adecuados a las prácticas de certificación y a las condiciones de seguridad adicionales, comprendidas en los estándares señalados en el literal a).
c) Personal competente para la conducción de las prácticas de certificación y el mantenimiento de la Infraestructura Oficial de Firma Digital.
d) Sistema de gestión que permita el mantenimiento de las condiciones señaladas en los literales anteriores, así como la seguridad, confidencialidad, transparencia y no discriminación en la prestación de sus servicios.
e) autoridad administrativa competente, así como entidades de certificación y entidades de registro o verificación debidamente acreditadas o reconocidas.

Artículo 12º.- Estándares aplicables bajo la Infraestructura Oficial de Firma Digital
Las prácticas de certificación comprendidas en la Infraestructura Oficial de Firma Digital deben estar basadas sobre los estándares técnicos internacionales vigentes que aseguren la interoperabilidad y las funciones exigidas en la Ley como en el Reglamento.
La autoridad administrativa competente determinará los estándares compatibles aplicando el principio de neutralidad tecnológica con la necesidad de cumplir los requisitos mencionados en el párrafo anterior.

CAPÍTULO II
DE LA FIRMA DIGITAL

Artículo 13º.- Firmas digitales generadas bajo la Infraestructura Oficial de Firma Digital
Las firmas digitales que gozan de las presunciones establecidas en los Artículos 6' y 8' del Reglamento son las generadas a partir de certificados digitales:
a) Emitidos conforme a lo dispuesto en el Reglamento por entidades de certificación acreditadas arte la autoridad administrativa competente. -
b) Incorporados a la Infraestructura Oficial de Firma Digital bajo acuerdos de certificación cruzada, conforme al Artículo 49º. del Reglamento.
c) Reconocidos al amparo de acuerdos de reconocimiento mutuo suscritos por la autoridad administrativa competente conforme al Artículo 47º. del Reglamento.
d) Emitidos por entidades de certificación extranjeras que hayan sido incorporados por reconocimiento a la Infraestructura Oficial de Firma Digital conforme al Artículo 48' del Reglamento.

Artículo 14º.- Características de la firma digital
Las características mínimas de la firma digital generadas bajo la Infraestructura Oficial de Firma Digital son:
a) Se genere al cifrar el código de verificación de un mensaje de datos usando la clave privada del titular del certificado digital.
b) Es única al titular de la firma digital y a cada mensaje de datos firmado por éste.
c) Es susceptible de ser verificada usando la clave pública del titular de la firma digital.
d) Su generación está bajo el control exclusivo del titular de la firma digital.
e) Está añadida o asociada lógicamente al mensaje de datos de tal manera que es posible detectar si la firma digital o el mensaje de datos ha sido alterado.

Articulo 15º.- Funciones de la firma digital
Dadas las características señaladas en el artículo anterior, técnicamente la firma digital debe garantizar:
a) Que el mensaje de datos fue enviado y firmado con la clave privada del titular de la firma digital.
b) La integridad del mensaje de datos firmado digitalmente, dado que cualquier alteración en el mensaje de datos o en la firma digital puede ser detectada.
c) Que el titular de la firma digital no pueda repudiar o desconocer un mensaje de datos que ha sido firmado digitalmente usando su clave privada dado que ésta se mantiene bajo su control exclusivo.

Artículo 16º.- Del titular de la firma digital
Dentro de la Infraestructura Oficial de Firma Digital, la responsabilidad sobre los efectos jurídicos generados por la utilización de una firma digital corresponde al titular del certificado digital.
Tratándose de personas naturales, éstas son titulares del certificado y de las firmas digitales que se generen a partir de aquél, Incluyendo las firmas digitales que genere a través de agentes automatizados.
En el caso de personas jurídicas, son éstas las titulares del certificado digital, y sus representantes los titulares de la firma digital, con excepción de las firmas digitales que se generen a través de agentes automatizados, situación en la cual las personas jurídicas son titulares del certificado y de las firmas digitales generadas a partir de éstos.

Artículo 17º.- Obligaciones del titular de la firma digital
Las obligaciones del titular de la firma digital son:
a) Entregar Información veraz bajo su responsabilidad.
b) Generar la clave privada y firmar digitalmente mediante los procedimientos señalados por la entidad de certificación.
c) Mantener el control y la reserva de la clave privada bajo su responsabilidad. -
d) Observar las condiciones establecidas por la entidad de certificación para la utilización del certificado digital y la generación de firmas digitales.

Artículo 18º.- Invalidez de la firma digital
Una firma digital generada bajo la Infraestructura Oficial de Firma Digital pierde validez si es utilizada:
a) En fines distintos para el que fue extendido el certificado digital.
b) Cuando el certificado haya sido cancelado conforme a lo establecido en el Capítulo IV del presente Título.

CAPÍTULO III
DEL CERTIFICADO DIGITAL

Artículo 19º.- Requisitos para obtener un certificado digital
Para la obtención de un certificado digital el solicitante deberá acreditar lo siguiente:
a) Tratándose de personas naturales, tener plena capacidad de ejercicio de sus derechos civiles.
b) Tratándose de personas jurídicas, acreditar la existencia de la misma y su vigencia mediante los instrumentos públicos o norma legal respectivos.

Artículo 20º.- Especificaciones adicionales para ser titular de un certificado digital
Para ser titular de un certificado digital adicionalmente se deberá cumplir con:
Entregar la información solicitada por la entidad de certificación o la entidad de registro o verificación, asumiendo responsabilidad por la veracidad y exactitud de la información proporcionada, sin perjuicio de la respectiva comprobación.
En el caso de personas naturales, la solicitud del certificado digital y el registro o verificación de su Identidad son estrictamente personales. La persona natural solicitante se constituirá en titular del certificado digital y de las firmas digitales que se generen.
Para el caso de personas jurídicas, la solicitud del certificado digital del cual ésta será titular y el registro o verificación de su identidad deben ser realizados a través de un representante debidamente acreditado. Conjuntamente con la solicitud debe indicarse el representante, persona natural, al cual se le asignará la facultad de generar y usar la clave privada, señalando para tal efecto las atribuciones y los poderes de representación correspondientes. Dicha persona natural será el titular de las firmas digitales. Tratándose de certificados digitales solicitados por personas jurídicas para su utilización a través de agentes automatizados, la titularidad del certificado digital y de las firmas digitales generadas a partir de dicho certificado digital corresponderá a la persona jurídica. La atribución de responsabilidad, para tales efectos, corresponde al representante legal, que en nombre de la persona jurídica solicita el certificado digital.

Artículo 21º.- Procedimiento para ser titular de un certificado digital
Para el caso de personas naturales, éstas deberán presentar una solicitud a la entidad de registro o verificación, según sea el caso; dicha solicitud deberá estar acompañada de toda la información requerida por la declaración de prácticas de certificación o en los procedimientos declarados. La entidad de registro o verificación deberá comprobar la identidad del solicitante a través de su documento oficial de identidad. La entidad de certificación cumplirá lo dispuesto en el presente articulo, en el supuesto previsto en el segundo párrafo del

Artículo 12' de la Ley.
En el caso de una persona jurídica, la solicitud deberá ser presentada por la persona facultada para tal fin, debiendo acreditar la existencia y vigencia de la persona jurídica mediante los Instrumentos públicos o norma legal respectiva, así como las facultades del representante. Asimismo, deberá presentar toda la información requerida por la declaración de prácticas de la entidad correspondiente.

Artículo 22º.- Obligaciones del titular de certificado digital
a) Actualizar permanentemente la información proveída tanto a la entidad de certificación como a la entidad de registro o verificación, asumiendo responsabilidad por la veracidad y exactitud de ésta.
b) Solicitar de inmediato la cancelación de su certificado digital en caso de que la reserva sobre la clave privada se haya visto comprometida, bajo responsabilidad.

c) Observar permanentemente las condiciones establecidas por la entidad de certificación para la utilización del certificado digital.

Artículo 23º.- Contenido del certificado digital
Los certificados digitales emitidos dentro de la Infraestructura Oficial de Firma Digital deberán contener como mínimo lo establecido en el Artículo 7º. de la Ley.
La entidad de certificación podrá incluir, a pedido del solicitante del certificado digital, información adicional siempre y cuando la entidad de registro o verificación compruebe fehacientemente la veracidad de ésta.

Artículo 24º. Período de Vigencia
El período de vigencia de los certificados digitales comienza y finaliza en las fechas indicadas en él, salvo en los supuestos de cancelación conforme al Artículo 9º. de la Ley.

CAPÍTULO IV
DE LA CANCELACIÓN DE CERTIFICADOS DIGITALES

Artículo 25º.- Causales de cancelación del certificado digital
a) Por solicitud del titular sin previa justificación, siendo necesario para tal efecto la aceptación y autorización de la entidad de certificación o la entidad de registro o verificación, según sea el caso. La misma que deberá ser aceptada y autorizada como máximo dentro del plazo establecido por. la autoridad administrativa competente, si en el plazo indicado la entidad no se pronuncia, se entenderá la cancelación del certificado; la misma que no podrá ser opuesta al tercero de buena fe.
b) Por revocatoria de la entidad de certificación, con expresión de causa.
c) Por expiración del plazo de vigencia.
d) Por el cese de operaciones de la entidad de certificación que lo emitió.
e) Por resolución administrativa o judicial que lo ordene.
f) Por interdicción civil judicialmente declarada, declaración de ausencia o de muerte presunta, del titular del certificado digital.
g) Por extinción de la personería jurídica o declaración judicial de quiebra.
h) Otras causales que establezca la autoridad administrativa competente.

Artículo 26º.- Cancelación del certificado digital a solicitud de su titular
La solicitud de cancelación de un certificado digital puede ser realizada por su titular o a través de un representante debidamente acreditado; pudiendo realizarse mediante documento electrónico firmado digitalmente, de acuerdo con los procedimientos definidos en cada caso por las entidades de certificación.
El titular del certificado digital está obligado, bajo responsabilidad, a solicitar la cancelación al tomar conocimiento de la ocurrencia de alguna de las siguientes circunstancias:
a) Por exposición, puesta en peligro o uso indebido de la clave privada.
b) Por deterioro, alteración o cualquier otro hecho u acto que afecte la clave privada.

Artículo 27º.- Cancelación por revocación
Para efectos de la cancelación de oficio o revocación de certificados digitales, la entidad de certificación debe contar con procedimientos detallados en su declaración de prácticas de certificación.
La revocación también puede ser solicitada por un tercero que informe fehacientemente de alguno de los supuestos de revocación contenidos en los numerales 1) y 2) del Artículo 10o. de la Ley.
La revocación debe indicar el momento desde el cual se aplica, precisando como mínimo la fecha y el tiempo dei mismo, que deberá estar expresado en minutos y segundos. La revocación no puede ser aplicada retroactivamente y debe ser notificada al titular del certificado digital. La entidad de certificación debe inmediatamente incluir la revocación del certificado en la relación que corresponda.

CAPÍTULO V
DE LA ENTIDAD DE CERTIFICACIÓN

Artículo 28º. De las funciones de la entidad de certificación
Las entidades de certificación tendrán las siguientes funciones:
a) Emitir certificados digitales manteniendo su numeración correlativa.
b) Cancelar certificados digitales.
c) Gestionar certificados digitales emitidos en el extranjero.
d) Adicionalmente a las anteriores las señaladas en el Articulo 32o. del Reglamento, en caso opten

por asumir las funciones de entidad de registro o verificación.
Las entidades de certificación podrán brindar otros servicios inherentes a los de certificación, cuyas características y procedimientos estarán contenidos en su declaración de prácticas de certificación.

Artículo 29º. De la, obligaciones de la entidad de certificación
Las entidades de certificación tienen las siguientes obligaciones:
a) Cumplir con su declaración de prácticas de certificación.
b) Informar a los usuarios todas las condiciones de emisión y de uso de sus certificados digitales, incluyendo las referidas a la cancelación de éstos.
c) Mantener el control y la reserva de la clave privada que emplea para firmar los certificados digitales que emite, bajo responsabilidad.
d) Mantener depósito de los certificados digitales emitidos y cancelados, consignando su fecha de emisión y vigencia.
e) Publicar permanente e ininterrumpidamente por medios telemáticos la relación de los certificados digitales emitidos y cancelados.
f) Cancelar el certificado digital a solicitud de su titular o, de ser el caso, a solicitud del titular de la firma digital; o cuando advierta que la información contenida en el certificado digital fuera inexacta o hubiera sido modificada, o que el titular incurriera en alguna de las causales previstas en el Artículo 25' del Reglamento.
g) Mantener la confidencialidad de la información relativa a los solicitantes y titulares de certificados digitales, limitando su empleo a las necesidades propias del servicio de certificación, salvo orden judicial o pedido expreso del titular del certificado digital.
h) Brindar todas las facilidades al personal autorizado por la autoridad administrativa competente para efectos de supervisión y auditoría.
i) Mantener la información relativa a los certificados digitales que hubieren sido cancelados, por un período minino de diez (10) años a partir de su cancelación.
j) Cumplir los términos bajo los cuales obtuvo la acreditación, así como los requerimientos adicionales que establezca la autoridad administrativa competente conforme a lo establecido en el Reglamento.
k) Informar y solicitar autorización a la autoridad administrativa competente para realizar acuerdos de certificación cruzada que proyecte celebrar, así como los términos bajo los cuales dichos acuerdos se suscribirían.
l) informar y solicitar autorización a la autoridad administrativa competente para efectos del reconocimiento de certificados emitidos por entidades extranjeras.
m) Cumplir sus funciones dentro de los plazos señalados en su declaración de prácticas de certificación.
n) Contratar los seguros o garantías bancarias necesarias que permitan indemnizar al titular por los daños que pueda ocasionar como resultado de las actividades de certificación.

Artículo 30º.- Respaldo financiero
Las entidades de certificación acreditadas o reconocidas deberán contar con el respaldo económico suficiente para operar bajo la Infraestructura Oficial de Firma Digital, así como para afrontar el riesgo de responsabilidad por daños, de conformidad con lo dispuesto en la Ley y en el Reglamento. La autoridad administrativa competente definirá los criterios para evaluar el cumplimiento de este requisito.

Artículo 31º.- Del cose do operaciones de la entidad de certificación
La entidad de certificación cesa sus operaciones en el marco de la Infraestructura Oficial de Firma Digital, en los siguientes casos:
a) Por decisión unilateral comunicada ante la autoridad administrativa competente, asumiendo la responsabilidad del caso por dicha decisión.
b) Por extinción dé su personería jurídica.
c) Por revocación de su registro.
d) Por decisión motivada de la autoridad administrativa competente.
e) Por resolución judicial.
f) Por liquidación, decidida por la junta de acreedores en el marco de la legislación concursal, o resolución judicial de quiebra.

Para los supuestos contemplados en los incisos a) y b) la autoridad administrativa competente establecerá el plazo en el cual las entidades de certificación notificarán tanto a aquélla como a los titulares de certificados digitales el cese de sus actividades. La autoridad administrativa competente deberá adoptar las medidas necesarias para p reservar las obligaciones contenidas en los incisos d), g) e i) del Artículo 29º. del Reglamento.

La autoridad administrativa competente reglamentará los procedimientos para hacer público el cese de operaciones de las entidades de certificación.

Los certificados digitales emitidos por una entidad de certificación cuyas operaciones han cesado deben ser cancelados a partir del día, hora, minuto y segundo en que se aplica el cese. El uso de certificados digitales con posterioridad a su cancelación implica la pérdida de las presunciones descritas en los Artículos 6' y 8' del Reglamento.

CAPÍTULO VI
DE LA ENTIDAD DE REGISTRO O VERIFICACIÓN

Artículo 32º.- De las funciones de la entidad de registro o verificación
Las entidades de registro o verificación tienen las siguientes funciones:
a) Identificar al solicitante del certificado digital mediante el levantamiento de datos y la comprobación de la Información brindada por aquél.
b) Aceptar, autorizar según sea el caso, la conformidad de las solicitudes de emisión, modificación o cancelación de certificados digitales, comunicándolo a la entidad de certificación bajo responsabilidad.

Artículo 33º.- De las obligaciones de la entidad de registro o verificación
Las entidades de registro o verificación acreditadas tienen las siguientes obligaciones:
a) Cumplir los procedimientos declarados para la prestación del servicio.
b) Determinar objetivamente y en forma directa la veracidad de la información proporcionada por el solicitante de certificado digital bajo responsabilidad.
c) Mantener la confidencialidad de la información relativa a los solicitantes y titulares de certificados digitales limitando su empleo a las necesidades propias del servicio de registro o verificación, salvo orden judicial o pedido expreso del titular del Certificado digital.
d) Recoger únicamente información o datos personales de relevancia para la emisión de los certificados.
e) Informar y solicitar autorización a la autoridad administrativa, especialmente en el supuesto previsto en el Artículo 48' del Reglamento.
f) Acreditar domicilio en el Perú
g) Contratar los seguros necesarios que le permitan indemnizar por los daños que puedan ocasionar como resultado de las actividades de registro o verificación.

Artículo 34º.- Respaldo financiero
Las entidades de registro o verificación acreditada deberán contar con el respaldo económico suficiente para operar bajo la infraestructura Oficial de Firma Digital; así como para afrontar el riesgo de responsabilidad por daños de conformidad con lo dispuesto en la Ley y por el Reglamento. La autoridad administrativa competente definirá los criterios para evaluar el cumplimiento de este requisito.

Artículo 35º.- Del cese de operaciones de la entidad de registro o verificación
La entidad de registro o verificación cesa de operar en el marco de la Infraestructura Oficial de Firma Digital:
a) Por decisión unilateral comunicada ante la autoridad administrativa competente asumiendo la responsabilidad del caso por dicha decisión
b) Por extinción de su personería jurídica.
c) Por revocación de su registro.
d) Por sanción dispuesta país autoridad administrativa competente.
e) Por orden judicial.
f) Por liquidación, decidida por la junta de acreedores en el marco de la legislación concursal o resolución judicial de quiebra.

Para los supuestos contenidos en los incisos a) y b) la entidad de registro ó verificación debe notificar el cese de sus actividades a la autoridad administrativa competente con una anticipación mínima que será establecida por ésta, debiendo dejar constancia ante aquella de los mecanismos utilizados para preservar el cumplimiento de lo dispuesto en el inciso c) del artículo 33º. del Reglamento.

TITULO III
DE LA AUTORIDAD ADMINISTRATIVA COMPETENTE
CAPITULO I
FUNCIONES DE LA AUTORIDAD ADMINISTRATIVA COMPETENTE

Artículo 36º.- Designación y funciones
Conforme a lo establecido en el artículo 15º. de la Ley, se designa al Instituto Nacional de Defensa de la Competencia y la Protección de la propiedad Intelectual (INDECOPI) como la autoridad administrativa competente.
La autoridad administrativa competente tiene las siguientes funciones:
a) Aprobar la política de certificados y la declaraciones de prácticas de certificación.
b) Acreditar entidades de certificación nacionales y reconocer a las entidades de certificación extranjeras.
c) Acreditar entidades de registro o de verificación
d) Supervisar a las entidades de certificación y a las entidades de registro o verificación estableciendo de ser el caso las sanciones correspondientes.
e) Cancelar las acreditaciones otorgadas a las entidades de certificación y a las entidades de registro o verificación conforme a lo dispuesto en el Reglamento.
f) Publicar ininterrumpidamente la relación de entidades acreditadas.
g) Aprobar el empleo de estándares técnicos internacionales dentro de la Infraestructura oficial de Firma Electrónica y determinar la compatibilidad de otros estándares técnicos con los estándares Internacionales.
h) Formular los criterios para el establecimiento de la idoneidad técnica que deberán cumplir quienes presten servicios en las materias reguladas por la Ley y el Reglamento, así como aquellas relacionadas con la prevención y solución de conflictos.
i) Establecer los requisitos mínimos para la prestación de los servicios de certificación y los servicios de registro o verificación.
j) Impulsar la solución de conflictos por medio de la conciliación y el arbitraje
k) Definir los criterios para evaluar la suficiencia del respaldo financiero con el que deben contar las entidades de certificación y las entidades de registro o verificación.
l) Aprobar la utilización de otras tecnologías de firmas electrónicas distintas a las firmas digitales, previa verificación del cumplimiento de ida requisitos establecidos en el Articulo 2' de la Ley y regular su utilización al interior de la Infraestructura Oficial de Firma Electrónica.
m) Suscribir acuerdos de reconocimiento mutuo con autoridades administrativas extranjeras que cumplen funciones similares a las de la autoridad administrativa competente.
n) Autorizar la realización de certificaciones cruzadas con entidades de certificación extranjeras.
o) Delegar a terceros bajo sus órdenes y responsabilidad las funciones que determine.
p) Fomentar y coordinar el uso y desarrollo de la Infraestructura Oficial de Firma electrónica en las entidades del sector público nacional. -
q) Aprobar y regular los servicios de valor añadido al interior de la Infraestructura Oficial de Firma Electrónica.
r) Las demás que sean necesarias para el buen funcionamiento de la infraestructura Oficial de Firma Electrónica.

CAPÍTULO II
RÉGIMEN DE ACREDITACIÓN DE ENTIDADES DE CERTIFICACION Y DE LAS ENTIDADES DE REGISTRO O VERIFICACION

Artículo 37º.- Acreditación do Entidades de Certificación
Las entidades que soliciten su acreditación como entidades de certificación ante la autoridad administrativa competente deben contar con los elementos de la infraestructura Oficial de Firma Digital señalados en los incisos a), b), c) y d) del Artículo 11º. y someterse al procedimiento de evaluación comprendido en el Articulo 41º. del Reglamento.
Cuando alguno de los elementos señalados en el párrafo precedente sea administrado por un tercero, la entidad solicitante deberá demostrar tu vinculación con aquél, asegurando la viabilidad de sus servicios bajo dichas condiciones, y la disponibilidad de estos elementos para la evaluación y supervisión que la autoridad administrativa competente considere necesarias. La autoridad administrativa competente, de ser el caso, precisará los términos bajo los cuales se rigen estos supuestos del servicio de certificación.

Artículo 38º.- Presentación de la solicitud de acreditación de entidad de certificación
La solicitud de acreditación de entidades de certificación debe presentarse a la autoridad administrativa competente, observando lo dispuesto en el artículo anterior y adjuntando lo siguiente:
a) Acreditación de la existencia y vigencia de la persona jurídica mediante los instrumentos públicos o norma legal respectivos, así como las facultades del representante.
b) Acreditar domicilio en el país.
a) Declaración jurada de contar con la infraestructura e Instalaciones necesarias para la prestación del servicio, así como la declaración jurada de aceptación de la visita comprobatoria de la autoridad administrativa competente.
d) Declaración de prácticas de certificación y documentación que comprende el sistema de gestión Implementado conforme a los Incisos a) y d) del Articulo 11o. del Reglamento.
e) Declaración jurada del cumplimiento de los requisitos señalados en los Incisos b) y c) del Artículo 11o. del Reglamento; información qué será comprobada porte autoridad administrativa competente.
f) Documentación que acredite el cumplimiento de lo dispuesto en los Artículos 29' y 30' del Reglamento y demás que la autoridad administrativa competente señale.
g) Informe favorable de la entidad sectorial correspondiente, cuando lo solicite la autoridad administrativa competente, para el caso de personas jurídicas supervisadas, respecto de la legalidad y seguridad para el desempeño de actividades de certificación.

Artículo 39º.- Acreditación de Entidades de Registro o Verificación
Las entidades que soliciten su acreditación como entidades de registro o verificación ante la autoridad administrativa competente deben contar con procedimientos para la prestación de sus servicios, los mismos que tendrán que asegurar la verificación directa de la Identidad del solicitante.

Artículo 40º.- Presentación de la solicitud de acreditación de Entidades de Registro o Verificación
La solicitud para la acreditación de entidades de registro o verificación debe presentarse a la autoridad administrativa competente, observando lo dispuesto en el artículo anterior y adjuntando la información y documentos siguientes:
a) Acreditación de la existencia y vigencia de la persona jurídica mediante los instrumentos públicos o norma legal respectivos, así como las facultades del representante.
b) Acreditar domicilio en el país.
c) Declaración jurada de contar con la Infraestructura e instalaciones necesarias para la prestación del servicio, así como la declaración jurada de aceptación de la visita comprobatoria de la autoridad administrativa competente.
d) Procedimientos detallados que garanticen el cumplimiento de las funciones establecidas en el Reglamento.
e) Declaración de prácticas de verificación o registro.
f) Declaración jurada del cumplimiento de los requisitos señalados en los Artículos 33º y 34º del Reglamento.

Articulo 41º.- Procedimiento Administrativo de la Acreditación
Admitida la solicitud, la autoridad administrativa competente procederá a la evaluación del cumplimiento de os requisitos establecidos en la Ley como en el Reglamento.
La evaluación de los requisitos de competencia técnica de la entidad de certificación o de registro o verificación solicitante podrá ser realizada directamente por la autoridad administrativa competente, o a través de terceros, o reconociendo aquéllas realizadas en el extranjero por otras autoridades extranjeras que cumplan funciones equivalentes a las de la autoridad administrativa competente, y siempre que los requisitos evaluados por ellas sean equivalentes a los requisitos comprendidos en el Reglamento.

Artículo 42º.- Reconocimiento de evaluaciones en el extranjero
La autoridad administrativa competente reconocerá las evaluaciones sobre los requisitos de competencia técnica de la entidad de certificación solicitante realizadas en el extranjero siempre y cuando se cumplan con las normas establecidas por la autoridad administrativa competente en el marco del Reglamento.

Artículo 43º.- Subsanación de observaciones
- Dentro del procedimiento podrán subsanarse las deficiencias técnicas observadas durante la evaluación. Las entidades podrán solicitar la suspensión del procedimiento a fin de implementar las medidas necesarias para superar estas dificultades. Si culminada la etapa de evaluación, se mantienen observaciones, se denegará el Registro y se archivará el procedimiento.

Artículo 44º.- Costos del Registro y otro, procedimientos
Las entidades solicitantes asumirán los costos por la tramitación del procedimiento, y aquellos por evaluación, auditoría y demás previstos por la autoridad administrativa competente.

Artículo 45º.- Otorgamiento y vigencia de la Acreditación
La acreditación se otorga por un período de 10 años, renovables por períodos similares. Durante dicho período la Entidad beneficiaria estará sujeta a evaluaciones técnicas anuales para mantener la vigencia de la referida acreditación.

Artículo 46º.- Cancelación de la Acreditación
La cancelación de la acreditación procede por:
A) Solicitud de la entidad de certificación o de la entidad de verificación o de registro.
b) Extinción de su personería jurídica.
c) Sanción impuesta por la autoridad administrativa competente o por decisión judicial.
d) Por liquidación, decidida por la junta de acreedores en el marco de la legislación concursal o resolución judicial de quiebra.

CAPÍTULO III
DE LOS CERTIFICADOS EMITIDOS POR ENTIDADES EXTRANJERAS

Artículo 47º. Acuerdos de reconocimiento mutuo
La autoridad administrativa competente podrá suscribir acuerdos de reconocimiento mutuo con entidades similares, a fin de reconocer la validez de certificados digitales otorgados en el extranjero y extender la validez de la Infraestructura Oficial de Firma Digital. Los acuerdos de reconocimiento mutuo deben garantizar en forma equivalente las funciones exigidas por la Ley como en el Reglamento.

Artículo 48º. Reconocimiento de certificados emitidos por entidades extranjeras
La autoridad administrativa competente podrá reconocer certificados digitales emitidos por entidades extranjeras, de acuerdo con las prácticas y políticas que para tal efecto apruebe, las mismas que deben vela' por el cumplimiento de las obligaciones y responsabilidades establecidas en el Reglamento u otra norma posterior. Asimismo, podrá autorizar la operación de aquellas entidades de certificación nacionales que utilicen los servicios de entidades de certificación extranjera, de verificarse tal supuesto, las entidades nacionales asumirán las responsabilidades del caso.
Para los efectos de lo dispuesto en el párrafo precedente, la entidad extranjera deberá comunicar a la autoridad administrativa competente el nombre de aquellas entidades de certificación que autorizarán las solicitudes de emisión de certificados digitales así como la gestión de los mismos.
La autoridad administrativa competente emitirá las normas que aseguren el cumplimiento de lo establecido en el presente artículo; así corno los mecanismos adecuados de información a los agentes del mercado.

Artículo 49º.- Certificación cruzada
Las entidades de certificación acreditadas pueden realizar certificaciones cruzadas con entidades de certificación extranjeras a fin de reconocer los certificados digitales que éstas emitan en el extranjero incorporándolos como suyos dentro de la Infraestructura Oficial de Firma Digital de conformidad con el Articulo 11' de la Ley, siempre y cuando obtengan autorización previa de la autoridad administrativa competente. Las entidades que presten servicios de acuerdo a lo establecido en el párrafo precedente, asumirán responsabilidad de daños y perjuicios por la gestión de tales certificados.
Las entidades de certificación acreditadas que realicen certificaciones cruzadas conforme al primer párrafo del presente artículo, garantizarán ante la autoridad administrativa competente que los certificados digitales reconocidos han sido emitidos bajo requisitos equivalentes a los exigidos en la Infraestructura Oficial de Firma Digital, y que cumplen las funciones señaladas en el Artículo 2' de la Ley.

CAPÍTULO IV
SUPERVISION DE ENTIDADES ACREDITADAS

Artículo 50º - Facultades de Supervisión
La autoridad administrativa competente tiene la facultad de verificar la correcta prestación de los servicios de certificación así como de los servicios de registro o verificación y el cumplimiento de las obligaciones legales y técnicas por parte de las entidades acreditadas que operen bajo la Infraestructura Oficial de Firma Electrónica, así como la facultad de verificar el cumplimiento de las disposiciones establecidas en la Ley, el Reglamento, y en sus Resoluciones.

DISPOSICIONES FINALES

Artículo Primero.- Las entidades del Sector Público Nacional pueden suscribir acuerdos de cooperación con sus similares a nivel mundial o con instituciones de cooperación, para recibir apoyo, asesoría y financiamiento para el desarrollo del comercio electrónico en general, las firmas electrónicas y las firmas y certificados digitales en particular.

Artículo Segundo.- Las entidades de certificación deben establecer procedimientos ágiles y sencillos para que sus usuarios puedan presentar directamente reclamaciones por la prestación de sus servicios, las mismas que deberán ser atendidas en el más breve plazo. La autoridad administrativa competente aprueba o reforma estos procedimientos y regula todo lo relativo a las reclamaciones. Agotada la vía previa de la reclamación ante la entidad de certificación, procede recurrir en vía administrativa ante la autoridad administrativa competente, con sujeción a la Ley N' 27444 - Ley del Procedimiento Administrativo General. La autoridad administrativa competente determinará todos aquellos procedimientos y políticas necesarios para la aplicación del Reglamento. En los casos que proceda la reclamación, adoptará las medidas correctivas pertinentes.

3. LEY 27291 - MODIFICA EL CODIGO CIVIL PERMITIENDO LA UTILIZACION DE LOS MEDIOS ELECTRONICOS PARA LA COMUNICACION DE LA MANIFESTACION DE VOLUNTAD Y LA UTILIZACION DE LA FIRMA ELECTRÓNICA. Promulgada el 23.6.2000 y publicada en el Diario Oficial El Peruano 24.6.2000

Artículo 1º.- Modificación del Código Civil
Modifícanse los artículos 141o y 1374o del Código Civil, con los siguientes textos:

Artículo 141º.- Manifestación de voluntad
La manifestación de voluntad puede ser expresa o tácita. Es expresa cuando se realiza en forma oral o escrita, a través de cualquier medio directo, manual, mecánico, electrónico u otro análogo. Es tácita cuando la voluntad se infiere indubitablemente de una actitud o de circunstancias de comportamiento que revelan su existencia.
No puede considerarse que existe manifestación tácita cuando la ley exige declaración expresa o cuando el agente formula reserva o declaración en contrario.

Artículo 1374º.- Conocimiento y contratación entre ausentes
La oferta, su revocación, la aceptación y cualquier otra declaración contractual dirigida a determinada persona se consideran conocidas en el momento en que llegan a la dirección del destinatario, a no ser que este pruebe haberse encontrado, sin su culpa, en la imposibilidad de conocerla.
Si se realiza a través de medios electrónicos, ópticos u otro análogo, se presumirá la recepción de la declaración contractual, cuando el remitente reciba el acuse de recibo.

Artículo 2º.- Adición de artículo al Código Civil
Adiciónase el artículo 141º-A al Código Civil, con el siguiente texto:

Artículo 141º-A.- Formalidad
En los casos en que la ley establezca que la manifestación de voluntad deba hacerse a través de alguna formalidad expresa o requiera de firma, ésta podrá ser generada o comunicada a través de medios electrónicos, ópticos o cualquier otro análogo.
Tratándose de instrumentos públicos, la autoridad competente deberá dejar constancia del medio empleado y conservar una versión íntegra para su ulterior consulta.

Artículo 3º.- Reglamentación para relaciones con el Estado
El Poder Ejecutivo, por decreto supremo refrendado por el Ministro de Justicia y dentro del plazo de 90 (noventa) días, reglamentará la aplicación de la presente Ley en las relaciones entre el Estado y los particulares.

4. LEY Nº 27419 LEY SOBRE NOTIFICACIÓN POR CORREO ELECTRÓNICO
Promulgada el 6.2.2001 y Publicada el 7.2.2001

Artículo único.- Objeto de la ley
Modifícanse los artículos 163° y 164° del Código Procesal Civil, con el siguiente texto:

"Artículo 163°.- Notificación por telegrama o facsímil, correo electrónico u otro medio
En los casos del artículo 157°, salvo el traslado de la demanda o de la reconvención, citación para absolver posiciones y la sentencia, las otras resoluciones pueden, a pedido de parte, ser notificadas, además, por telegrama, facsímil, correo electrónico u otro medio idóneo, siempre que los mismos permitan confirmar su recepción.

La notificación por correo electrónico sólo se realizará para la parte que lo haya solicitado. Los gastos para la realización de esta notificación quedan incluidos en la condena de costas.

Artículo 164°.- Diligenciamiento de la notificación por facsímil, correo electrónico u otro medio
El documento para la notificación por facsímil, correo electrónico u otro medio, contendrá los datos de la cédula. El facsímil u otro medio se emitirá en doble ejemplar, uno de los cuales será entregado para su envío y bajo constancia al interesado por el secretario respectivo, y el otro con su firma se agregará al expediente. La fecha de la notificación será la de la constancia de la entrega del facsímil al destinatario. En el caso del correo electrónico, será, en lo posible, de la forma descrita anteriormente, dejándose constancia en el expediente del ejemplar entregado para su envío, anexándose además el correspondiente reporte técnico que acredite su envío.

El Consejo Ejecutivo del Poder Judicial podrá disponer la adopción de un texto uniforme para la redacción de estos documentos."

Comuníquese al señor Presidente de la República para su promulgación.

5. LEY N° 27444 "LEY DE PROCEDIMIENTOS ADMINISTRATIVOS GENERAL"
Artículo 20° inciso 20.1 numeral 20.1.2, Regula el uso del correo electrónico como medio de notificación en los procedimientos administrativos, promulgada el 10 abril 2001 y publicado en el Diario Oficial El Peruano el 11 abril 2001

Artículo 20 - Modalidades de notificación

20.1 Las notificaciones serán efectuadas a través de las siguientes modalidades, según este respectivo orden de prelación:

20.1.1 Notificación personal al administrado interesado o afectado por el acto, en su domicilio.

20.1.2 Mediante telegrama, correo certificado, telefax, correo electrónico; o cualquier otro medio que permita comprobar fehacientemente su acuse de recibo y quien lo recibe, siempre que el empleo de cualquiera de estos medios hubiese sido solicitado expresamente por el administrado.

20.1.3 Por publicación en el Diario Oficial y en uno de los diarios de mayor circulación en el territorio nacional, salvo disposición distinta de la ley.

20.2 La autoridad no podrá suplir alguna modalidad con otra, bajo sanción de nulidad de la notificación. Podrá acudir complementariamente a aquellas u otras, si así lo estimare conveniente para mejorar las posibilidades de participación de los administrados.

20.3 Tratamiento igual al previsto en este capítulo corresponde a los citatorios, los emplazamientos, los requerimientos de documentos o de otros actos administrativos análogos.

6. LEY N° 28493 – LEY QUE REGULA EL USO DEL CORREO ELECTRÓNICO COMERCIAL NO SOLICITADO (SPAM) 18 marzo 2005

Artículo 1.- Objeto de la Ley
La presente Ley regula el envío de comunicaciones comerciales publicitarias o promocionales no solicitadas, realizadas por correo electrónico, sin perjuicio de la aplicación de las disposiciones vigentes en materia comercial sobre publicidad y protección al consumidor.

Artículo 2.- Definiciones
Para efectos de la presente Ley se entiende por:
a) Correo electrónico: Todo mensaje, archivo, dato u otra información electrónica que se transmite a una o más personas por medio de una red de interconexión entre computadoras o cualquier otro equipo de tecnología similar. También se considera correo electrónico la información contenida en forma de remisión o anexo accesible mediante enlace electrónico directo contenido dentro del correo electrónico.

b) Correo electrónico comercial: Todo correo electrónico que contenga información comercial publicitaria o promocional de bienes y servicios de una empresa, organización, persona o cualquier otra con fines lucrativos.

c) Proveedor del servicio de correo electrónico: Toda persona natural o jurídica que provea el servicio de correo electrónico y que actúa como intermediario en el envío o recepción del mismo.

d) Dirección de correo electrónico: Serie de caracteres utilizado para identificar el origen o el destino de un correo electrónico.

Artículo 3.- Derechos de los usuarios
Son derechos de los usuarios de correo electrónico:
a) Rechazar o no la recepción de correos electrónicos comerciales.
b) Revocar la autorización de recepción, salvo cuando dicha autorización sea una condición esencial para la provisión del servicio de correo electrónico.
c) Que su proveedor de servicio de correo electrónico cuente con sistemas o programas que filtren los correos electrónicos no solicitados.

Artículo 4.- Obligaciones del proveedor
Los proveedores de servicio de correo electrónico domiciliados en el país están obligados a contar con sistemas o programas de bloqueo y/o filtro para la recepción o la transmisión que se efectúe a través de su servidor, de los correos electrónicos no solicitados por el usuario.

Artículo 5.- Correo electrónico comercial no solicitado
Todo correo electrónico comercial, promocional o publicitario no solicitado, originado en el país, debe contener:
a) La palabra "PUBLICIDAD", en el campo del "asunto" (o subject) del mensaje.
b) Nombre o denominación social, domicilio completo y dirección de correo electrónico de la persona natural o jurídica que emite el mensaje.
c) La inclusión de una dirección de correo electrónico válido y activo de respuesta para que el receptor pueda enviar un mensaje para notificar su voluntad de no recibir más correos no solicitados o la inclusión de otros mecanismos basados en Internet que permita al receptor manifestar su voluntad de no recibir mensajes adicionales.

Artículo 6.- Correo electrónico comercial no solicitado considerado ilegal
El correo electrónico comercial no solicitado será considerado ilegal en los siguientes casos:
a) Cuando no cumpla con alguno de los requisitos establecidos en el artículo 5 de la presente Ley.
b) Contenga nombre falso o información falsa que se oriente a no identificar a la persona natural o jurídica que transmite el mensaje.
c) Contenga información falsa o engañosa en el campo del asunto (o subject), que no coincida con el contenido del mensaje.
d) Se envíe o transmita a un receptor que haya formulado el pedido para que no se envíe dicha publicidad, luego del plazo de dos (2) días.

Artículo 7.- Responsabilidad
Se considerarán responsables de las infracciones establecidas en el artículo 6 de la presente Ley y deberán compensar al receptor de la comunicación:
1. Toda persona que envíe correos electrónicos no solicitados conteniendo publicidad comercial.
2. Las empresas o personas beneficiarias de manera directa con la publicidad difundida.
3. Los intermediarios de correos electrónicos no solicitados, tales como los proveedores de servicios de correos electrónicos.

Artículo 8.- Derecho a compensación pecuniaria
El receptor de correo electrónico ilegal podrá accionar por la vía del proceso sumarísimo contra la persona que lo haya enviado, a fin de obtener una compensación pecuniaria, la cual será equivalente al uno por ciento (1%) de la Unidad Impositiva Tributaria por cada uno de los mensajes de correo electrónico transmitidos en contravención de la presente Ley, con un máximo de dos (2) Unidades Impositivas Tributarias.

Artículo 9.- Autoridad competente
El Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual - INDECOPI, a través de la Comisión de Protección al Consumidor y de la Comisión de Represión de la Competencia Desleal, será la autoridad competente para conocer las infracciones contempladas en el artículo 6 de la presente Ley; cuyas multas se fijarán de acuerdo a lo establecido en el Decreto Legislativo Nº 716, Ley de Protección al Consumidor, o en el Decreto Legislativo Nº 691, Normas de la Publicidad en Defensa del Consumidor, según corresponda.

Artículo 10.- Reglamento
El Poder Ejecutivo mediante decreto supremo, refrendado por el Ministro de Transportes y Comunicaciones, reglamentará la presente Ley en un plazo máximo de noventa (90) días desde su vigencia.

Artículo 11.- Vigencia
La presente Ley entrará en vigencia a los noventa (90) días de su publicación en el Diario Oficial "El Peruano".

7. LEY Nº 27310 - LEY QUE MODIFICA EL ARTÍCULO 11º DE LA LEY Nº 27269

Artículo Único.- Objeto de la ley
Modifícase el Artículo 11º de la Ley Nº 27269, el mismo que quedará redactado de la siguiente manera:
"Artículo 11.- Los Certificados de Firmas Digitales emitidos por Entidades Extranjeras tendrán la misma validez y eficacia jurídica reconocidas en la presente Ley, siempre y cuando tales certificados sean reconocidos por la autoridad administrativa competente."

Comuníquese al señor Presidente de la República para su promulgación.
En Lima, a los veintiséis días del mes de junio del dos mil.

MARTHA HILDEBRANDT PÉREZ TREVIÑO
Presidenta del Congreso de la República

LUIS DELGADO APARICIO
Segundo Vicepresidente del Congreso de la República

AL SEÑOR PRESIDENTE CONSTITUCIONAL DE LA REPÚBLICA

POR TANTO:
Mando se publique y cumpla.
Dado en la Casa de Gobierno, en Lima, a los quince días del mes de julio del año dos mil.

ALBERTO FUJIMORI FUJIMORI
Presidente Constitucional de la República

ALBERTO BUSTAMANTE BELAUNDE
Presidente del Consejo de Ministros y Ministro de Justicia

ANEXO (03)

REPÚBLICA BOLIVARIANA DE VENEZUELA
Ley Especial Contra los Delitos Informáticos
Título I
Disposiciones Generales

Artículo 1.- Objeto de la ley.
La presente ley tiene por objeto la protección integral de los sistemas que utilicen tecnologías de información, así como la prevención y sanción de los delitos cometidos contra tales sistemas o cualquiera de sus componentes o los cometidos mediante el uso de dichas tecnologías, en los términos previstos en esta ley.

Artículo 2.- Definiciones.
A los efectos de la presente ley y cumpliendo con lo previsto en el art. 9 de la Constitución de la República Bolivariana de Venezuela, se entiende por:

a. Tecnología de Información: rama de la tecnología que se dedica al estudio, aplicación y procesamiento de data, lo cual involucra la obtención, creación, almacenamiento, administración, modificación, manejo, movimiento, control, visualización, distribución, intercambio, transmisión o recepción de información en forma automática, así como el desarrollo y uso del "hardware", "firmware", "software", cualesquiera de sus componentes y todos los procedimientos asociados con el procesamiento de data.

b. Sistema: cualquier arreglo organizado de recursos y procedimientos diseñados para el uso de tecnologías de información, unidos y regulados por interacción o interdependencia para cumplir una serie de funciones específicas, así como la combinación de dos o más componentes interrelacionados, organizados en un paquete funcional, de manera que estén en capacidad de realizar una función operacional o satisfacer un requerimiento dentro de unas especificaciones previstas.

c. Data: Hechos, conceptos, instrucciones o caracteres representados de una manera apropiada para que sean comunicados, transmitidos o procesados por seres humanos o por medios automáticos y a los cuales se les asigna o se les puede asignar significado.

d. Información: Significado que el ser humano le asigna a la data utilizando las convenciones conocidas y generalmente aceptadas.

e. Documento: Registro incorporado en un sistema en forma de escrito, video, audio o cualquier otro medio, que contiene data o información acerca de un hecho o acto capaces de causar efectos jurídicos.

f. Computador: dispositivo o unidad funcional que acepta data, la procesa de acuerdo con un programa guardado y genera resultados, incluidas operaciones aritméticas o lógicas.

g. Hardware: Equipos o dispositivos físicos considerados en forma independiente de su capacidad o función, que forman un computador o sus componentes periféricos, de manera que pueden incluir herramientas, implementos, instrumentos, conexiones, ensamblajes, componentes y partes.

h. Firmware: Programa o segmento de programa incorporado de manera permanente en algún componente de hardware.

i. Software: Información organizada en forma de programas de computación, procedimientos y documentación asociados, concebidos para realizar la operación de un sistema, de manera que pueda proveer de instrucciones a los computadores así como de data expresada en cualquier forma, con el objeto de que éstos realicen funciones específicas.

j. Programa: Plan, rutina o secuencia de instrucciones utilizados para realizar un trabajo en particular o resolver un problema dado a través de un computador.

k. Procesamiento de data o de información: Realización sistemática de operaciones sobre data o sobre información, tales como manejo, fusión, organización o cómputo.

l. Seguridad: Condición que resulta del establecimiento y mantenimiento de medidas de protección que garanticen un estado de inviolabilidad de influencias o de actos hostiles específicos que puedan propiciar el acceso a la data de personas no autorizadas o que afecten la operatividad de las funciones de un sistema de computación.

m. Virus: Programa o segmento de programa indeseado que se desarrolla incontroladamente y que genera efectos destructivos o perturbadores en un programa o componente del sistema.

n. Tarjeta inteligente: Rótulo, cédula o carnet que se utiliza como instrumento de identificación, de acceso a un sistema, de pago o de crédito y que contiene data, información o ambas, de uso restringido sobre el usuario autorizado para portarla.

o. Contraseña (password): Secuencia alfabética, numérica o combinación de ambas, protegida por reglas de confidencialidad utilizada para verificar la autenticidad de la autorización expedida a un usuario para acceder a la data o a la información contenidas en un sistema.

p. Mensaje de datos: Cualquier pensamiento, idea, imagen, audio, data o información, expresados en un lenguaje conocido que puede ser explícito o secreto (encriptado), preparados dentro de un formato adecuado para ser transmitido por un sistema de comunicaciones.

Artículo 3.- Extraterritorialidad.
Cuando alguno de los delitos previstos en la presente ley se cometa fuera del territorio de la República, el sujeto activo quedará sujeto a sus disposiciones si dentro del territorio de la República se hubieren producido efectos del hecho punible y el responsable no ha sido juzgado por el mismo hecho o ha evadido el juzgamiento o la condena por tribunales extranjeros.

Artículo 4.- Sanciones.
Las sanciones por los delitos previstos en esta ley serán principales y accesorias. Las sanciones principales concurrirán con las accesorias y ambas podrán también concurrir entre sí, de acuerdo con las circunstancias particulares del delito del cual se trate, en los términos indicados en la presente ley.

Artículo 5.- Responsabilidad de las personas jurídicas.
Cuando los delitos previstos en esta Ley fuesen cometidos por los gerentes, administradores, directores o dependientes de una persona jurídica, actuando en su nombre o representación, éstos responderán de acuerdo con su participación culpable.

La persona jurídica será sancionada en los términos previstos en esta Ley, en los casos en que el hecho punible haya sido cometido por decisión de sus órganos, en el ámbito de su actividad, con sus recursos sociales o en su interés exclusivo o preferente.

Título II
De los Delitos
Capítulo I
De los Delitos Contra los Sistemas que Utilizan Tecnologías de Información

Artículo 6.- Acceso indebido.
El que sin la debida autorización o excediendo la que hubiere obtenido, acceda, intercepte, interfiera o use un sistema que utilice tecnologías de información, será penado con prisión de uno a cinco años y multa de diez a cincuenta unidades tributarias.

Artículo 7.- Sabotaje o daño a sistemas.
El que destruya, dañe, modifique o realice cualquier acto que altere el funcionamiento o inutilice un sistema que utilice tecnologías de información o cualquiera de los componentes que lo conforman, será penado con prisión de cuatro a ocho años y multa de cuatrocientas a ochocientas unidades tributarias.

Incurrirá en la misma pena quien destruya, dañe, modifique o inutilice la data o la información contenida en cualquier sistema que utilice tecnologías de información o en cualquiera de sus componentes.

La pena será de cinco a diez años de prisión y multa de quinientas a mil unidades tributarias, si los

efectos indicados en el presente artículo se realizaren mediante la creación, introducción o transmisión, por cualquier medio, de un virus o programa análogo.

Artículo 8.- Sabotaje o daño culposos.
Si el delito previsto en el artículo anterior se cometiere por imprudencia, negligencia, impericia o inobservancia de las normas establecidas, se aplicará la pena correspondiente según el caso, con una reducción entre la mitad y dos tercios.

Artículo 9.- Acceso indebido o sabotaje a sistemas protegidos.
Las penas previstas en los artículos anteriores se aumentarán entre una tercera parte y la mitad cuando los hechos allí previstos o sus efectos recaigan sobre cualquiera de los componentes de un sistema que utilice tecnologías de información protegido por medidas de seguridad, que esté destinado a funciones públicas o que contenga información personal o patrimonial de personas naturales o jurídicas

Artículo 10.- Posesión de equipos o prestación de servicios de sabotaje.
El que, con el propósito de destinarlos a vulnerar o eliminar la seguridad de cualquier sistema que utilice tecnologías de información, importe, fabrique, posea, distribuya, venda o utilice equipos, dispositivos o programas; o el que ofrezca o preste servicios destinados a cumplir los mismos fines, será penado con prisión de tres a seis años y multa de trescientas a seiscientas unidades tributarias.

Artículo 11.- Espionaje informático.
El que indebidamente obtenga, revele o difunda la data o información contenidas en un sistema que utilice tecnologías de información o en cualquiera de sus componentes, será penado con prisión de cuatro a ocho años y multa de cuatrocientas a ochocientas unidades tributarias.

La pena se aumentará de un tercio a la mitad, si el delito previsto en el presente artículo se cometiere con el fin de obtener algún tipo de beneficio para sí o para otro.

El aumento será de la mitad a dos tercios, si se pusiere en peligro la seguridad del Estado, la confiabilidad de la operación de las instituciones afectadas o resultare algún daño para las personas naturales o jurídicas como consecuencia de la revelación de las informaciones de carácter reservado.

Artículo 12.- Falsificación de documentos.
El que, a través de cualquier medio, cree, modifique o elimine un documento que se encuentre incorporado a un sistema que utilice tecnologías de información; o cree, modifique o elimine datos del mismo; o incorpore a dicho sistema un documento inexistente, será penado con prisión de tres a seis años y multa de trescientas a seiscientas unidades tributarias.

Cuando el agente hubiere actuado con el fin de procurar para sí o para otro algún tipo de beneficio, la pena se aumentará entre un tercio y la mitad.

El aumento será de la mitad a dos tercios si del hecho resultare un perjuicio para otro.

Capítulo II
De los Delitos Contra la Propiedad

Artículo 13.- Hurto.
El que a través del uso de tecnologías de información, acceda, intercepte, interfiera, manipule o use de cualquier forma un sistema o medio de comunicación para apoderarse de bienes o valores tangibles o intangibles de carácter patrimonial sustrayéndolos a su tenedor, con el fin de procurarse un provecho económico para sí o para otro, será sancionado con prisión de dos a seis años y multa de doscientas a seiscientas unidades tributarias.

Artículo 14.- Fraude.
El que, a través del uso indebido de tecnologías de información, valiéndose de cualquier manipulación en sistemas o cualquiera de sus componentes o en la data o información en ellos contenida, consiga insertar instrucciones falsas o fraudulentas que produzcan un resultado que permita obtener un provecho injusto en perjuicio ajeno, será penado con prisión de tres a siete años y multa de trescientas a setecientas unidades tributarias.

Artículo 15.- Obtención indebida de bienes o servicios.

El que, sin autorización para portarlos, utilice una tarjeta inteligente ajena o instrumento destinado a los mismos fines, o el que utilice indebidamente tecnologías de información para requerir la obtención de cualquier efecto, bien o servicio o para proveer su pago sin erogar o asumir el compromiso de pago de la contraprestación debida, será castigado con prisión de dos a seis años y multa de doscientas a seiscientas unidades tributarias.

Artículo 16.- Manejo fraudulento de tarjetas inteligentes o instrumentos análogos.
El que por cualquier medio, cree, capture, grabe, copie, altere, duplique o elimine la data o información contenidas en una tarjeta inteligente o en cualquier instrumento destinado a los mismos fines; o el que, mediante cualquier uso indebido de tecnologías de información, cree, capture, duplique o altere la data o información en un sistema con el objeto de incorporar usuarios, cuentas, registros o consumos inexistentes o modifique la cuantía de éstos, será penado con prisión de cinco a diez años y multa de quinientas a mil unidades tributarias.
En la misma pena incurrirá quien, sin haber tomado parte en los hechos anteriores, adquiera, comercialice, posea, distribuya, venda o realice cualquier tipo de intermediación de tarjetas inteligentes o instrumentos destinados al mismo fin, o de la data o información contenidas en ellos o en un sistema.

Artículo 17.- Apropiación de tarjetas inteligentes o instrumentos análogos.
El que se apropie de una tarjeta inteligente o instrumento destinado a los mismos fines, que se hayan perdido, extraviado o hayan sido entregados por equivocación, con el fin de retenerlos, usarlos, venderlos o transferirlos a persona distinta del usuario autorizado o entidad emisora, será penado con prisión de uno a cinco años y multa de diez a cincuenta unidades tributarias. La misma pena se impondrá a quien adquiera o reciba la tarjeta o instrumento a que se refiere el presente artículo.

Artículo 18.- Provisión indebida de bienes o servicios. El que a sabiendas de que una tarjeta inteligente o instrumento destinado a los mismos fines, se encuentra vencido, revocado, se haya indebidamente obtenido, retenido, falsificado, alterado, provea a quien los presente de dinero, efectos, bienes o servicios o cualquier otra cosa de valor económico, será penado con prisión de dos a seis años y multa de doscientas a seiscientas unidades tributarias.

Artículo 19.- Posesión de equipo para falsificaciones.
El que sin estar debidamente autorizado para emitir, fabricar o distribuir tarjetas inteligentes o instrumentos análogos, reciba, adquiera, posea, transfiera, comercialice, distribuya, venda, controle o custodie cualquier equipo de fabricación de tarjetas inteligentes o de instrumentos destinados a los mismos fines o cualquier equipo o componente que capture, grabe, copie o transmita la data o información de dichas tarjetas o instrumentos, será penado con prisión de tres a seis años y multa de trescientas a seiscientas unidades tributarias.

Capítulo III
De los delitos contra la privacidad de las personas y de las comunicaciones

Artículo 20.- Violación de la privacidad de la data o información de carácter personal.
El que por cualquier medio se apodere, utilice, modifique o elimine, sin el consentimiento de su dueño, la data o información personales de otro o sobre las cuales tenga interés legítimo, que estén incorporadas en un computador o sistema que utilice tecnologías de información, será penado con prisión de dos a seis años y multa de doscientas a seiscientas unidades tributarias.

La pena se incrementará de un tercio a la mitad si como consecuencia de los hechos anteriores resultare un perjuicio para el titular de la data o información o para un tercero.

Artículo 21.- Violación de la privacidad de las comunicaciones.
El que mediante el uso de tecnologías de información, acceda, capture, intercepte, interfiera, reproduzca, modifique, desvíe o elimine cualquier mensaje de datos o señal de transmisión o comunicación ajena, será sancionado con prisión de dos a seis años y multa de doscientas a seiscientas unidades tributarias.

Artículo 22.- Revelación indebida de data o información de carácter personal.
El que revele, difunda o ceda, en todo o en parte, los hechos descubiertos, las imágenes, el audio o, en general, la data o información obtenidos por alguno de los medios indicados en los artículos precedentes, aún cuando el autor no hubiese tomado parte en la comisión de dichos delitos, será sancionado con prisión de dos a seis años y multa de doscientas a seiscientas unidades tributarias.

Si la revelación, difusión o cesión se hubieren realizado con un fin de lucro o si resultare algún perjuicio para otro, la pena se aumentará de un tercio a la mitad.

Capítulo IV
De los delitos contra niños, niñas o adolescentes

Artículo 23.- Difusión o exhibición de material pornográfico.
El que por cualquier medio que involucre el uso de tecnologías de información, exhiba, difunda, transmita o venda material pornográfico o reservado a personas adultas, sin realizar previamente las debidas advertencias para que el usuario restrinja el acceso a niños, niñas y adolescentes será sancionado con prisión de dos a seis años y multa de doscientas a seiscientas unidades tributarias.

Artículo 24.- Exhibición pornográfica de niños o adolescentes.
El que por cualquier medio que involucre el uso de tecnologías de información, utilice a la persona o imagen de un niño, niña o adolescente con fines exhibicionistas o pornográficos, será penado con prisión de cuatro a ocho años y multa de cuatrocientas a ochocientas unidades tributarias.

Capítulo V
De los delitos contra el orden económico

Artículo 25.- Apropiación de propiedad intelectual.
El que sin autorización de su propietario y con el fin de obtener algún provecho económico, reproduzca, modifique, copie, distribuya o divulgue un software u otra obra del intelecto que haya obtenido mediante el acceso a cualquier sistema que utilice tecnologías de información, será sancionado con prisión de uno a cinco años y multa de cien a quinientas unidades tributarias.

Artículo 26.- Oferta engañosa.
El que ofrezca, comercialice o provea de bienes o servicios mediante el uso de tecnologías de información y haga alegaciones falsas o atribuya características inciertas a cualquier elemento de dicha oferta de modo que pueda resultar algún perjuicio para los consumidores, será sancionado con prisión de uno a cinco años y multa de cien a quinientas unidades tributarias, sin perjuicio de la comisión de un delito más grave.

Título III
Disposiciones comunes

Artículo 27.- Agravantes.
La pena correspondiente a los delitos previstos en la presente Ley se incrementará entre un tercio y la mitad:
1º Si para la realización del hecho se hubiere hecho uso de alguna contraseña ajena indebidamente obtenida, quitada, retenida o que se hubiere perdido.
2º Si el hecho hubiere sido cometido mediante el abuso de la posición de acceso a data o información reservada o al conocimiento privilegiado de contraseñas en razón del ejercicio de un cargo o función.

Artículo 28.- Agravante especial.
La sanción aplicable a las personas jurídicas por los delitos cometidos en las condiciones señaladas en el artículo 5 de esta Ley, será únicamente de multa, pero por el doble del monto establecido para el referido delito.

Artículo 29.- Penas accesorias.
Además de las penas principales previstas en los capítulos anteriores, se impondrán, necesariamente sin perjuicio de las establecidas en el Código Penal, las accesorias siguientes:

1º El comiso de equipos, dispositivos, instrumentos, materiales, útiles, herramientas y cualquier otro objeto que haya sido utilizado para la comisión de los delitos previstos en los artículos 10 y 19 de la presente ley.

2º El trabajo comunitario por el término de hasta tres años en los casos de los delitos previstos en los artículos 6 y 8 de esta Ley.

3º La inhabilitación para el ejercicio de funciones o empleos públicos, para el ejercicio de la profesión,

arte o industria, o para laborar en instituciones o empresas del ramo por un período de hasta tres (3) años después de cumplida o conmutada la sanción principal cuando el delito se haya cometido con abuso de la posición de acceso a data o información reservadas o al conocimiento privilegiado de contraseñas en razón del ejercicio de un cargo o función públicos, del ejercicio privado de una profesión u oficio o del desempeño en una institución o empresa privadas, respectivamente.

4º La suspensión del permiso, registro o autorización para operar o para el ejercicio de cargos directivos y de representación de personas jurídicas vinculadas con el uso de tecnologías de información hasta por el período de tres (3) años después de cumplida o conmutada la sanción principal, si para cometer el delito el agente se hubiere valido o hubiere hecho figurar a una persona jurídica.

Artículo 30.- Divulgación de la sentencia condenatoria.
El Tribunal podrá disponer, además, la publicación o difusión de la sentencia condenatoria por el medio que considere más idóneo.

Artículo 31.- Indemnización Civil.
En los casos de condena por cualquiera de los delitos previstos en los Capítulos II y V de esta Ley, el Juez impondrá en la sentencia una indemnización en favor de la víctima por un monto equivalente al daño causado. Para la determinación del monto de la indemnización acordada, el Juez requerirá del auxilio de expertos.

Título IV
Disposiciones Finales

Artículo 32.- Vigencia.
La presente Ley entrará en vigencia, treinta días después de su publicación en la Gaceta Oficial de la República Bolivariana de Venezuela.

Artículo 33.- Derogatoria.
Se deroga cualquier disposición que colija con la presente Ley. Dada, firmada y sellada en el Palacio Federal Legislativo, sede de la Asamblea Nacional, en Caracas a los seis días del mes de septiembre de dos mil uno. Año 191° de la Independencia y 142° de la Federación.

Presidente Willian Lara

Primer Vicepresidente Leopoldo Puchi

Segundo Vicepresidente Gerardo Saer Pérez

Secretario Subsecretario Eustoquio Contreras Vladimir Villegas

ANEXO (03)

COLOMBIA

Estatuto para Prevenir y Contrarrestar la Explotación, la Pornografía y el Turismo Sexual con Menores de Edad - en su Capítulo Segundo se refiere a las Redes Globales, publicado el l4 de agosto del 2001, con Ley Nro. 679 – 2001

Artículo 1. Objeto. Esta ley tiene por objeto dictar medidas de protección contra la explotación, la pornografía, el turismo sexual y demás formas de abuso sexual con menores de edad, mediante el establecimiento de normas de carácter preventivo y sancionatorio, y la expedición de otras disposiciones en desarrollo del artículo 44 de la Constitución.

Artículo 2. Definición. Para los efectos de la presente ley, se entiende por menor de edad la persona que no ha cumplido los dieciocho años.

Artículo 3. Ámbito de aplicación. A la presente ley se sujetarán las personas naturales y jurídicas de nacionalidad colombiana, o extranjeras con domicilio en el país, cuya actividad u objeto social tenga relación directa o indirecta con la comercialización de bienes y servicios a través de redes globales de información, los prestadores de servicios turísticos a los que se refiere el artículo 62 de la Ley 300 de 1996 y las demás personas naturales o jurídicas de nacionalidad colombiana, o extranjeras con domicilio en el país, que puedan generar o promover turismo nacional o internacional.

Se sujetarán igualmente a la presente ley las personas naturales que, teniendo su domicilio en el exterior, realicen por sí mismas o en representación de una sociedad las actividades a las que hace referencia el inciso primero del presente artículo, siempre que ingresen a territorio colombiano.

Del mismo modo, en virtud de la cooperación internacional prevista en el artículo 13, el Gobierno Nacional incorporará a los tratados y convenios internacionales que celebre con otros países el contenido de la presente ley, a fin de que su aplicación pueda extenderse a personas naturales o jurídicas extranjeras, domiciliadas en el exterior, cuyo objeto social sea el mismo al que se refiere el inciso primero del presente artículo.

CAPITULO II
Del uso de redes globales de información en relación con menores

Artículo 4. Comisión de expertos. Dentro del mes siguiente a la vigencia de la presente ley, el Instituto Colombiano de Bienestar Familiar conformará una Comisión integrada por peritos jurídicos y técnicos, y expertos en redes globales de información y telecomunicaciones, con el propósito de elaborar un catálogo de actos abusivos en el uso y aprovechamiento de tales redes en lo relacionado con menores de edad. La Comisión propondrá iniciativas técnicas como sistemas de detección, filtro, clasificación, eliminación y bloqueo de contenidos perjudiciales para menores de edad en las redes globales, que serán transmitidas al Gobierno nacional con el propósito de dictar medidas en desarrollo de esta ley.

Los miembros de la Comisión serán funcionarios de la planta de personal ya existente en las entidades públicas cuya función sea la protección del menor y el área de comunicaciones, y su designación corresponderá al representante legal de las mismas. En todo caso, formarán parte de la Comisión, el Director del Instituto Colombiano de Bienestar Familiar, el Defensor del Pueblo, un experto en delitos informáticos del DAS, el Fiscal General de la Nación, y a sus reuniones será invitado el delegado para Colombia de la UNICEF.

La Comisión a la que se refiere el presente artículo, presentará un informe escrito al Gobierno Nacional dentro de los cuatro meses siguientes a su conformación, en el cual consten las conclusiones de su estudio, así como las recomendaciones propuestas.

Parágrafo. La Comisión de Expertos a la que hace referencia el presente artículo dejará de funcionar de manera permanente, una vez rendido el informe para la cual será conformada. No obstante, el Gobierno Nacional podrá convocarla siempre que lo estime necesario para el cabal cumplimiento de los fines previstos en la presente ley.

Artículo 5. Informe de la Comisión. Con base en el informe de que trata el artículo anterior, el Gobierno nacional, con el apoyo de la Comisión de Regulación de Telecomunicaciones, adoptará las medidas administrativas y técnicas destinadas a prevenir el acceso de menores de edad a cualquier modalidad de información pornográfica, y a impedir el aprovechamiento de redes globales de información con fines de explotación sexual infantil u ofrecimiento de servicios comerciales que impliquen abuso sexual con menores de edad.

Las regulaciones sobre medidas administrativas y técnicas serán expedidas por el Gobierno Nacional dentro de los seis (6) meses siguientes a la fecha de vigencia de la presente ley.

Artículo 6. Sistemas de autorregulación. El Gobierno nacional, por intermedio del Ministerio de Comunicaciones, promoverá e incentivará la adopción de sistemas de autorregulación y códigos de conducta eficaces en el manejo y aprovechamiento de redes globales de información. Estos sistemas y códigos se elaborarán con la participación de organismos representativos de los proveedores y usuarios de servicios de redes globales de información.

Para estos efectos, el Ministerio de Comunicaciones convocará a los sujetos a los que hace referencia el artículo tercero de la presente ley, para que formulen por escrito sus propuestas de autorregulación y códigos de conducta.

Los códigos de conducta serán acordados dentro del año siguiente a la vigencia de la presente ley y se remitirá copia a las Secretarías Generales del Senado y de la Cámara.

Artículo 7. Prohibiciones. Los proveedores o servidores, administradores y usuarios de redes globales de información no podrán:

1. Alojar en su propio sitio imágenes, textos, documentos o archivos audiovisuales que impliquen directa o indirectamente actividades sexuales con menores de edad.

2. Alojar en su propio sitio material pornográfico, en especial en modo de imágenes o videos, cuando existan indicios de que las personas fotografiadas o filmadas son menores de edad.

3. Alojar en su propio sitio vínculos o links, sobre sitios telemáticos que contengan o distribuyan material pornográfico relativo a menores de edad.

Artículo 8. Deberes. Sin perjuicio de la obligación de denuncia consagrada en la ley para todos los residentes en Colombia, los proveedores, administradores y usuarios de redes globales de información deberán:

1. Denunciar ante las autoridades competentes cualquier acto criminal contra menores de edad de que tengan conocimiento, incluso de la difusión de material pornográfico asociado a menores.

2. Combatir con todos los medios técnicos a su alcance la difusión de material pornográfico con menores de edad.

3. Abstenerse de usar las redes globales de información para divulgación de material ilegal con menores de edad.

4. Establecer mecanismos técnicos de bloqueo por medio de los cuales los usuarios se puedan proteger a sí mismos o a sus hijos de material ilegal, ofensivo o indeseable en relación con menores de edad.

Artículo 9. Puntos de información. El Ministerio de Comunicaciones creará dentro del mes siguiente a la expedición de la presente ley, una línea telefónica directa que servirá como punto de información para proveedores y usuarios de redes globales de información acerca de las implicaciones legales de su uso en relación con esta ley.

Así mismo, dentro del término arriba señalado, creará una página electrónica en las redes globales, a la cual puedan remitirse los usuarios para formular denuncias contra eventos de pornografía con menores de edad y para señalar las páginas electrónicas en las que se ofrezcan servicios sexuales con menores de edad o de pornografía con menores de edad, así como señalar a los autores o

responsables de tales páginas.

En caso de que el Ministerio de Comunicaciones reciba por vía telefónica o electrónica denuncias que puedan revestir un carácter penal, las mismas deberán ser remitidas de inmediato a las autoridades competentes, con el fin de que adelanten la investigación que corresponda.

Artículo 10. Sanciones administrativas. El Ministerio de Comunicaciones tomará medidas a partir de las denuncias formuladas, y sancionará a los proveedores o servidores, administradores y usuarios responsables que operen desde territorio colombiano, sucesivamente de la siguiente manera:

1. Multas hasta de 100 salarios mínimos legales vigentes.

2. Cancelación o suspensión de la correspondiente página electrónica.

Para la imposición de estas sanciones se aplicará el procedimiento establecido en el Código Contencioso Administrativo con observancia del debido proceso y criterios de adecuación, proporcionalidad y reincidencia.

CAPITULO III
Personería procesal y acciones de sensibilización

Artículo 11. Personería procesal. Toda persona natural o jurídica tendrá la obligación de denunciar ante las autoridades competentes cualquier hecho violatorio de las disposiciones de la presente ley. Las asociaciones de padres de familia y demás organizaciones no gubernamentales cuyo objeto sea la protección de la niñez y de los derechos de los menores de edad, tendrán personería procesal para denunciar y actuar como parte en los procedimientos administrativos y judiciales encaminados a la represión del abuso sexual de menores de edad.

La Defensoría del Pueblo y las personerías municipales brindarán toda la asesoría jurídica que las asociaciones de padres de familia requieran para ejercer los derechos procesales a que se refiere este artículo. La omisión en el cumplimiento de esta obligación constituye falta disciplinaria gravísima.

Artículo 12. Medidas de sensibilización. Las autoridades de los distintos niveles territoriales y el Instituto Colombiano de Bienestar Familiar, implementarán acciones de sensibilización pública sobre el problema de la prostitución, la pornografía y el abuso sexual de menores de edad. El Gobierno Nacional, por intermedio del Ministerio de Educación, supervisará las medidas que a este respecto sean dictadas por las autoridades departamentales, distritales y municipales.

Parágrafo 1°. Por medidas de sensibilización pública se entiende todo programa, campaña o plan tendiente a informar por cualquier medio sobre el problema de la prostitución, la pornografía con menores de edad y el abuso sexual de menores de edad; sobre sus causas y efectos físicos y psicológicos y sobre la responsabilidad del Estado y de la sociedad en su prevención.

Parágrafo 2°. La Procuraduría General de la Nación, a través de la Delegada para la Defensa de la Familia y el Menor y de los Procuradores Judiciales harán el seguimiento y el control respectivo.

CAPITULO IV
Medidas de alcance internacional

Artículo 13. Acciones de cooperación internacional. El Gobierno Nacional tomará las medidas necesarias para defender los derechos fundamentales de los niños y aumentar la eficacia de las normas de la presente ley, mediante acciones de cooperación internacional acordes con el carácter mundial del problema de la explotación sexual, la pornografía y el turismo asociado a prácticas sexuales con menores de edad. En ese sentido, el Presidente de la República podrá adoptar las siguientes medidas:

1. Sugerirá la inclusión de normas para prevenir y contrarrestar el abuso sexual de menores de edad en los Convenios de Cooperación Turística que se celebren con otros países.

2. Tomará la iniciativa para la adopción de acuerdos internacionales que permitan el intercambio de información sobre personas o empresas que ofrezcan servicios relacionados con la explotación

sexual de menores de edad, la pornografía con menores de edad y el turismo asociado a prácticas sexuales con menores, mediante la utilización de redes globales de información o de cualquier otro medio de comunicación.

3. Alentará l a realización de acuerdos de asistencia mutua y cooperación judicial en materia de pruebas sobre crímenes asociados a la explotación sexual, la pornografía con menores de edad y el turismo asociado a prácticas sexuales con menores.

4. Propiciará encuentros mundiales de la Unicef en Colombia con el fin de tratar el problema del abuso sexual con menores de edad.

5. Alentará el intercambio de información, estadísticas y la unificación de la legislación mundial contra la explotación sexual de menores de edad.

6. Ofrecerá o concederá la extradición de ciudadanos extranjeros que estén sindicados de conductas asociadas a la explotación sexual y la pornografía con menores de edad y el turismo asociado a prácticas sexuales con menores. Para tales efectos no será necesaria la existencia de un tratado público, ni se exigirá que el hecho que la motiva esté reprimido con una determinada sanción mínima privativa de la libertad, aunque en lo demás la extradición deberá instrumentarse de conformidad con el Código de Procedimiento Penal.

7. Tomará medidas concretas e inmediatas tendientes a la repatriación de menores de edad que hayan salido ilegalmente del país o con fines de explotación sexual.

Artículo 14. Denegación y cancelación de visas. No podrá otorgarse visa de ninguna clase para ingresar a territorio colombiano a extranjeros contra los cuales se hubieren iniciado en cualquier Estado investigaciones preliminares, proceso penal o de policía, o se hubieren impuesto multas, o dictado medida de aseguramiento, o se hubiere dictado sentencia condenatoria ejecutoriada por delitos de explotación sexual o contra la libertad, el pudor y la formación sexuales de menores de edad.

Así mismo, en cualquier momento se les cancelará la visa ya otorgada, sin perjuicio de la correspondiente acción penal que de oficio debe adelantar el Estado colombiano para asegurar la condigna sanción de tales hechos punibles.

Por las mismas razones procederá la deportación, la expulsión y la in admisión a territorio colombiano.

Estas medidas serán adoptadas también en relación con quienes hayan sido sindicados de promover, facilitar u ocultar tales delitos, en cualquier Estado.

Artículo 15. Sistema de información sobre delitos sexuales contra menores. Para la prevención de los delitos sexuales contra menores de edad y el necesario control sobre quienes los cometen, promuevan o facilitan, el Ministerio de Justicia y del Derecho, el Departamento Administrativo de Seguridad, DAS, el Instituto Colombiano de Bienestar Familiar y la Fiscalía General de la Nación desarrollarán un sistema de información en el cual se disponga de una completa base de datos sobre delitos contra la libertad, el pudor y la formación sexuales cometidos sobre menores de edad, sus autores, cómplices, proxenetas, tanto de condenados como de sindicados.

El Departamento Administrativo de Seguridad y la Fiscalía General de la Nación promoverán la formación de un servicio internacional de información sobre personas sindicad as o condenadas por delitos contra la libertad, el pudor y la formación sexuales sobre menores de edad. Para tal efecto se buscará el concurso de los organismos de policía internacional.

CAPITULO V
Medidas para prevenir y contrarrestar el turismo sexual

Artículo 16. Programas de promoción turística. Los prestadores de servicios turísticos enlistados en el artículo 62 de la Ley 300 de 1996, y las demás personas naturales o jurídicas que puedan generar turismo nacional o internacional, se abstendrán de ofrecer en los programas de promoción turística, expresa o subrepticiamente, planes de explotación sexual de menores. Asimismo, adoptarán medidas para impedir que sus trabajadores, dependientes o intermediarios, ofrezcan orientación

turística o contactos sexuales con menores de edad.

Parágrafo. El Ministerio de Desarrollo Económico exigirá a los prestadores de servicios turísticos que se acojan a compromisos o códigos de conducta, con el fin de proteger a los menores de edad de toda forma de explotación y violencia sexual originada por turistas nacionales o extranjeros.

Los Códigos o compromisos de conducta serán radicados en el Ministerio de Desarrollo Económico en un término máximo de seis (6) meses contados a partir de la vigencia de la presente ley, y se les dará amplia divulgación.

Artículo 17. Deber de advertencia. Los establecimientos hoteleros o de hospedaje incluirán una cláusula en los contratos de hospedaje que celebren a partir de la vigencia de la presente ley, informando sobre las consecuencias legales de la explotación y el abuso sexual de menores de edad en el país.

Las agencias de viaje y de turismo incluirán en su publicidad turística información en el mismo sentido.

Las aerolíneas nacionales o extranjeras informarán a sus usuarios en viajes internacionales con destino Colombia acerca de la existencia de la legislación contra la explotación sexual de menores de edad.

Artículo 18. Inspección y vigilancia. El Ministerio de Desarrollo inspeccionará y controlará las actividades de promoción turística con el propósito de prevenir y contrarrestar la prostitución y el abuso sexual de menores de edad en el sector y sancionará a los prestadores de servicios turísticos involucrados.

Artículo 19. Infracciones. Además de las infracciones previstas en el artículo 71 de la Ley 300 de 1996, los prestadores de servicios turísticos podrán ser objeto de sanciones administrativas, sin perjuicio de las penales, cuando incurran en alguna de las siguientes conductas:

1. Utilizar publicidad que sugiera expresa o subrepticiamente la prestación de servicios turísticos sexuales con menores de edad.

2. Dar información a los turistas, directamente o por intermedio de sus empleados, acerca de lugares desde donde se coordinen o donde se presten servicios sexuales con menores de edad.

3. Conducir a los turistas a establecimientos o lugares donde se practique la prostitución de menores de edad.

4. Conducir a los menores de edad, directamente o por intermedio de sus empleados, a los sitios donde se encuentran hospedados los turistas, incluso si se trata de lugares localizados en altamar, con fines de prostitución de menores de edad.

5. Arrendar o utilizar vehículos en rutas turísticas con fines de prostitución o de abuso sexual con menores de edad.

6. Permitir el ingreso de menores a los hoteles o lugares de alojamiento y hospedaje, bares, negocios similares y demás establecimientos turísticos con fines de prostitución o de abuso sexual de menores de edad.

Artículo 20. Sanciones. El Ministerio de Desarrollo Económico impondrá las siguientes sanciones, de acuerdo con el procedimiento establecido para tal fin en la Ley 300 de 1996:

1. Multas hasta por trescientos (300) salarios mínimos legales mensuales vigentes, que se destinarán al Fondo de Promoción Turística para los fines de la presente ley.

2. Suspensión hasta por noventa (90) días calendario de la inscripción en el Registro Nacional de Turismo.

3. Cancelación de la inscripción en el Registro Nacional de Turismo que implicará la prohibición de ejercer la actividad turística durante cinco (5) años a partir de la sanción.

El Ministerio de Desarrollo Económico podrá delegar esta función de vigilancia y control en las entidades territoriales. Esta delegación, sin embargo, no excluye la responsabilidad del delegante por las acciones u omisiones de los delegatarios.

Parágrafo. Las personas naturales o jurídicas que hubieren sido sancionadas por violación a lo dispuesto en la presente ley, no podrán ser beneficiarias del Certificado de Desarrollo Turístico contemplado en el artículo 48 de la Ley 383 de 1997 y el Decreto 1053 de 1998.

Artículo 21. Fondo de Promoción Turística. Además de las funciones asignadas al Fondo de Promoción Turística creado por el artículo 42 de la Ley 300 de 1996, este tendrá por objeto financiar la ejecución de políticas de prevención y campañas para la erradicación del turismo asociado a prácticas sexuales con menores de edad, las cuales serán trazadas por el Ministerio de Desarrollo Económico en coordinación con el Instituto Colombiano de Bienestar Familiar.

Un porcentaje de los recursos del Fondo de Promoción Turística provenientes de la partida presupuestal que anualmente destina el Gobierno Nacional y el monto total de las multas que imponga el Ministerio de Desarrollo a los prestadores de servicios turísticos, según lo establecido en esta ley y en el numeral 2° del artículo 72 de la Ley 300 de 1996, se destinarán a este propósito. El Gobierno nacional reglamentará la materia.

A las reuniones del Comité Directivo del Fondo será invitado el Director del Instituto Colombiano de Bienestar Familiar, cuando quiera que se discuta la destinación de los recursos a que alude el inciso anterior.

Artículo 22. Impuesto a videos para adultos. Los establecimientos de comercio, cuando alquilen películas de video de clasificación X para adultos, pagarán un impuesto correspondiente al cinco por ciento (5%) sobre el valor de cada video rentado, con destino a la financiación de los planes y programas de prevención y lucha contra la explotación sexual y la pornografía con menores de edad.

Artículo 23. Impuesto de salida. El extranjero, al momento de salida del territorio colombiano, cubrirá el valor correspondiente a un dólar de los Estados Unidos de América, o su equivalente en pesos colombianos, con destino a la financiación de los planes y programas de prevención y lucha contra la explotación sexual y la pornografía con menores de edad.

Artículo 24. Fondo contra la Explotación Sexual de Menores. Créase la cuenta especial denominada Fondo contra la explotación sexual de menores, adscrita al Instituto Colombiano de Bienestar Familiar.

El objetivo principal del Fondo cuenta es proveer rentas destinadas a inversión social con el fin de garantizar la financiación de los planes y programas de prevención y lucha contra la explotación sexual y la pornografía con menores de edad y, más precisamente, con destino a los siguientes fines: construcción de hogares o albergues infantiles, programas de ayuda, orientación, rehabilitación y recuperación física y psicológica de menores de edad que han sido objeto de explotación sexual; financiación de programas de repatriación de colombianos que han sido objeto de explotación sexual, y financiación de mecanismos de difusión para la prevención de acciones delictivas en materia de tráfico de mujeres y niños.

Las fuentes específicas de los recursos destinados al fondo cuenta, serán las siguientes:

1. Las partidas que se le asignen en el presupuesto nacional.
2. Los recursos provenientes de crédito interno y externo.
3. Las donaciones que reciba.
4. Los recursos de cooperación nacional o internacional.
5. Los demás que obtenga a cualquier título.

Parágrafo 1. El Consejo Directivo del ICBF definirá cada año cuáles serán los gastos concretos con cargo al fondo tomando en cuenta las condiciones de inversión fijadas en la presente ley. Habrá siempre una apropiación dentro del presupuesto que se le asigne a ICBF para promover educación especial, que les presente nuevas alternativas vocacionales que los oriente hacia un trabajo digno, para los menores objeto de explotación o prácticas sexuales. También se incluirá una apropiación específica para investigar las causas y soluciones del tema que es objeto de la presente ley.

Las conclusiones de estas investigaciones servirán para definir los programas y proyectos que se ejecutarán en las siguientes vigencias fiscales.

Parágrafo 2. El ordenador del gasto será el mismo ordenador del ICBF.

Parágrafo 3. La administración financiera del fondo cuenta se hará a través de una entidad fiduciaria, vigilada por la Superintendencia Bancaria. El ICBF adelantará el proceso licitatorio y la celebración del contrato de encargo fiduciario.

Parágrafo 4. El Gobierno reglamentará lo relacionado con las funciones y responsabilidades de la Junta Directiva del ICBF y del ordenador del gasto en relación con el Fondo cuenta, mientras que el control interno y fiscal deberá adelantarse de acuerdo con las normas constitucionales y legales vigentes.

Parágrafo 5. Los recaudos a los que hacen referencia los artículos 22 y 23 de la presente ley, se destinarán específicamente a los fines previstos en este estatuto.

CAPITULO VI
Medidas policivas

Artículo 25. Vigilancia y control policivo. La Policía Nacional tendrá, además de las funciones asignadas constitucional y legalmente, las siguientes:

1. Adelantar labores de vigilancia y control de los establecimientos hoteleros o de hospedaje, atractivos turísticos y demás lugares que, a juicio del ICBF, del Ministerio de Desarrollo Económico y de la propia Policía Nacional merezcan una vigilancia especial por existir indicios de explotación sexual de menores de edad.

2. Apoyar las investigaciones administrativas adelantadas por el Ministerio de Desarrollo Económico en cumplimiento de esta ley.

3. Canalizar las quejas que se presenten en violación a lo dispuesto en la presente ley.

4. Inspeccionar e inmovilizar los vehículos en zonas turísticas cuando existan indicios graves de que se utilizan con fines de explotación sexual de menores de edad. Dichos vehículos podrán ser secuestrados y rematados para el pago de las indemnizaciones que se causen por el delito cuya comisión se establezca dentro del respectivo proceso penal.

Artículo 26. La Policía Nacional inspeccionará periódicamente las casas de lenocinio, a fin de prevenir y contrarrestar la explotación sexual, la pornografía y toda clase de prácticas sexuales con menores de edad. Al propietario o administrador de establecimiento que se oponga, se le impondrá el cierre del mismo por quince (15) días hábiles, sin perjuicio de que la inspección se realice y de la acción penal a que haya lugar.

Procede el cierre definitivo e inmediato del establecimiento, cuando se descubran casos de actos sexuales en que participen menores de edad o bien cuando se encuentre cualquier tipo de material pornográfico en el que participen menores de edad.

El cierre temporal y definitivo será de competencia de los inspectores en primera instancia y de los alcaldes en segunda, siguiendo el trámite del Código de Policía respectivo o, en su defecto, del Código Contencioso Administrativo, sin perjuicio de las sanciones penales y pecuniarias a que haya lugar.

Artículo 27. Línea telefónica de ayuda. La Policía Nacional, en un término no mayor a quince (15) días contados a partir de la vigencia de la presente ley, en todos los niveles territoriales, designará una línea exclusiva de ayuda para los menores de edad que sean objeto de maltrato o abuso sexual y para recibir denuncias de actos de abuso sexual con menores de edad, o de generación, comercialización o distribución de materiales como textos, documentos, archivos o audiovisuales con contenido pornográfico de menores de edad.

Artículo 28. Capacitación al personal policial. La Policía Nacional dictará periódicamente cursos y programas de capacitación, con el fin de actualizar al personal policial sobre la legislación vigente en materia de explotación sexual de menores de edad, venta y tráfico de niños, pornografía con menores de edad y atención menores de edad con necesidades básicas totalmente insatisfechas. El Inspector General de la Policía Nacional y el Comisionado Nacional para la Policía realizará los controles necesarios para asegurar el cumplimiento de esta función, sin perjuicio de la vigilancia que corresponde a los organismos de control.

Parágrafo. El Instituto Colombiano de Bienestar Familiar y las demás entidades públicas, en todos los niveles territoriales, cuyas funciones estén relacionadas con la protección de menores de edad, contribuirán a la capacitación de los miembros de la Policía Nacional.

Artículo 29. Registro de menores desaparecidos. La Policía Nacional llevará un registro de menores de edad desaparecidos, en relación con los cuales establecerá prioridades de búsqueda y devolución a sus familias. Los niños desaparecidos durante más de tres meses, deberán ser incluidos en los comunicados internacionales sobre personas desaparecidas en la sede de la INTERPOL.

Artículo 30. Vigilancia aduanera. Se prohíbe la importación de cualquier tipo de material pornográfico en el que participen menores de edad o en el que se exhiban actos de abuso sexual con menores de edad. Las autoridades aduaneras dictarán medidas apropiadas con el fin de interceptar esta clase de importaciones ilegales, sin perjuicio de las funciones que debe cumplir la Policía Nacional.

Artículo 31. Planes y estrategias de seguridad. Los gobernadores y alcaldes incluirán medidas de prevención y erradicación de la explotación sexual de menores de edad, la pornografía y el turismo asociado a prácticas sexuales con menores de edad en los planes y estrategias integrales de seguridad de que trata el artículo 20 de la Ley 62 de 1993 y o normas que la modifiquen. El incumplimiento de este deber será sancionado disciplinariamente como falta grave.

Artículo 32. Comisión Nacional de Policía. Dos (2) representantes de organizaciones no gubernamentales colombianas, cuyo objeto social comprenda la protección y defensa de menores de edad, tendrán asiento en la Comisión Nacional de Policía y Participación Ciudadana.

CAPITULO VII
Medidas penales

Artículo 33. Adiciónese el artículo 303 del Código Penal con el siguiente inciso. “Si el agente realizare cualquiera de las conductas descritas en este artículo con personas menores de catorce años por medios virtuales, utilizando redes globales de información, incurrirá en las penas correspondientes disminuidas en una tercera parte.” Parágrafo transitorio. Tan pronto como entre en vigencia la Ley 599 de 2000 el presente artículo tendrá el número 209.

Artículo 34. Adiciónese un nuevo artículo al Código Penal, con el número 312A, del siguiente tenor:

Artículo 312A. Utilización o facilitación de medios de comunicación para ofrecer servicios sexuales de menores. El que utilice o facilite el correo tradicional, las redes globales de información, o cualquier otro medio de comunicación para obtener contacto sexual con menores de dieciocho (18) años, o para ofrecer servicios sexuales con éstos, incurrirá en pena de prisión de cinco (5) a diez (10) años, y multa de cincuenta (50) a cien (100) salarios mínimos legales mensuales vigentes.

Las penas señaladas en el inciso anterior se aumentarán hasta en la mitad (1/2) cuando las conductas se realizaren con menores de doce (12) años.

Parágrafo transitorio. Tan pronto como entre en vigencia la Ley 599 de 2000, el presente artículo tendrá el número 219A.

Artículo 35. Adiciónese un nuevo artículo al Código Penal, con el número 312B, del siguiente tenor:

Artículo 312B. Omisión de denuncia. El que, por razón de su oficio, cargo, o actividad, tuviere conocimiento de la utilización de menores para la realización de cualquiera de las conductas previstas en el presente capítulo y omitiere informar a las autoridades administrativas o judiciales competentes sobre tales hechos, teniendo el deber legal de hacerlo, incurrirá en multa de diez (10) a cincuenta (50)

salarios mínimos legales mensuales vigentes. Si la conducta se realizare por servidor público, se impondrá, además, la pérdida del empleo.

Parágrafo transitorio. Tan pronto como entre en vigencia la Ley 599 de 2000, el presente artículo tendrá el número 219B.

CAPITULO VIII
Disposiciones finales

Artículo 36. Investigación estadística. Con el fin de conocer los factores de riesgo social, individual y familiar que propician la explotación sexual de los menores, así como las consecuencias del abuso, el Departamento Administrativo Nacional de Estadística, DANE, realizará una investigación estadística que será actualizada periódicamente y que recaudará como mínimo la siguiente información:
1. Cuantificación de los menores explotados sexualmente, por sexo y edad.
2. Lugares o áreas de mayor incidencia.
3. Cuantificación de la clientela por nacionalidad, clase(s) social.
4. Formas de remuneración.
5. Formas de explotación sexual.
6. Ocurrencia del turismo asociado a prácticas sexuales con menores.
7. Nivel de educación de menores explotados sexualmente.

Los gobernadores y los alcaldes distritales y municipales, así como las autoridades indígenas, prestarán al Departamento Administrativo Nacional de Estadística, DANE, toda la colaboración necesaria, a nivel departamental, distrital y municipal, para la realización de la investigación.

Las personas naturales o jurídicas, de cualquier orden o naturaleza, domiciliadas o residentes en el territorio nacional, están obligadas a suministrar al Departamento Administrativo Nacional de Estadística, DANE, los datos solicitados en el desarrollo de su investigación.

Los datos suministrados al Departamento Administrativo Nacional de Estadística, DANE, en el desarrollo de la investigación no podrán darse a conocer al público ni a las entidades u organismos oficiales, ni a las autoridades públicas, sino únicamente en resúmenes numéricos, que no hagan posible deducir de ellos información alguna de carácter individual que pudiera utilizarse para fines de discriminación.
El Departamento Administrativo Nacional de Estadística, DANE, podrá imponer multas por una cuantía entre uno (1) y cincuenta (50) salarios mínimos legales mensuales vigentes, como sanción a las personas naturales o jurídicas o entidades públicas de que trata el presente artículo y que incumplan lo dispuesto en esta norma u obstaculicen la realización de la investigación, previo el trámite de procedimiento breve y sumario que garantice el derecho de defensa.

Esta información servirá de base a las autoridades para prevenir la explotación sexual de menores, y proteger y asistir a las víctimas infantiles con el fin de facilitar su recuperación y reintegración dentro de la sociedad.

Artículo 37. Comisión especial. Las mesas directivas del Senado de la República y de la Cámara de Representantes designarán una comisión especial integrada por cinco (5) senadores y cinco (5) Representantes, incluidos los autores y ponentes de la presente ley, con el fin de asesorar y colaborar con el Gobierno Nacional en el desarrollo de la presente ley, así como evaluar su cumplimiento por parte de las autoridades. Esta Comisión podrá recomendar a las mesas directivas las modificaciones legales que estime pertinentes.

Artículo 38. Operaciones presupuestales. Autorizase al Gobierno Nacional para adoptar las medidas y realizar las operaciones presupuestarias necesarias para la cumplida ejecución de esta ley.

Artículo 39. Vigencia. La presente ley rige a partir de su publicación y deroga todas las normas que le sean contrarias.

ANEXO (04)

LEGISLACIÓN SOBRE DELITOS INFORMATICOS EN ESPAÑA

Artículos del Código Penal Español referentes a Delitos Informáticos
(Ley-Orgánica 10/1995, de 23 de Noviembre/
BOE número 281, de 24 de Noviembre de 1.995)

Artículo 197

1.- El que para descubrir los secretos o vulnerar la intimidad de otro, sin su consentimiento, se apodere de sus papeles, cartas, mensajes de correo electrónico o cualesquiera otros documentos o efectos personales o intercepte sus telecomunicaciones o utilice artificios técnicos de escucha, transmisión, grabación o reproducción del sonido o de la imagen, o de cualquier otra señal de comunicación, será castigado con las penas de prisión de uno a cuatro años y multa de doce a veinticuatro meses.

2.- Las mismas penas se impondrán al que, sin estar autorizado, se apodere, utilice o modifique, en perjuicio de tercero, datos reservados de carácter personal o familiar de otro que se hallen registrados en ficheros o soportes informáticos, electrónicos o telemáticos, o en cualquier otro tipo de archivo o registro público o privado. Iguales penas se impondrán a quien, sin estar autorizado, acceda por cualquier medio a los mismos y a quien los altere o utilice en perjuicio del titular de los datos o de un tercero.

3.- Se impondrá la pena de prisión de dos a cinco años si se difunden, revelan o ceden a terceros los datos o hechos descubiertos o las imágenes captadas a que se refieren los números anteriores. Será castigado con las penas de prisión de uno a tres años y multa de doce a veinticuatro meses, el que, con conocimiento de su origen ilícito y sin haber tomado parte en su descubrimiento, realizare la conducta descrita en el párrafo anterior.

4.- Si los hechos descritos en los apartados 1 y 2 de este artículo se realizan por las personas encargadas o responsables de los ficheros, soportes informáticos, electrónicos o telemáticos, archivos o registros, se impondrá la pena de prisión de tres a cinco años, y si se difunden, ceden o revelan los datos reservados, se impondrá la pena en su mitad superior.

5.- Igualmente, cuando los hechos descritos en los apartados anteriores afecten a datos de carácter personal que revelen la ideología, religión, creencias, salud, origen racial o vida sexual, o la víctima fuere un menor de edad o un incapaz, se impondrán las penas previstas en su mitad superior.

6.- Si los hechos se realizan con fines lucrativos, se impondrán las penas respectivamente previstas en los apartados 1 al 4 de este artículo en su mitad superior. Si además afectan a datos de los mencionados en el apartado 5, la pena a imponer será la de prisión de cuatro a siete años.

Artículo 198

La autoridad o funcionario público que, fuera de los casos permitidos por la Ley, sin mediar causa legal por delito, y prevaliéndose de su cargo, realizare cualquiera de las conductas descritas en el artículo anterior, será castigado con las penas respectivamente previstas en el mismo, en su mitad superior y, además, con la de inhabilitación absoluta por tiempo de seis a doce años.

Artículo 199

1.- El que revelare secretos ajenos, de los que tenga conocimiento por razón de su oficio o sus relaciones laborales, será castigado con la pena de prisión de uno a tres años y multa de seis a doce meses.

2.- El profesional que, con incumplimiento de su obligación de sigilo o reserva, divulgue los secretos de otra persona, será castigado con la pena de prisión de uno a cuatro años, multa de doce a veinticuatro meses e inhabilitación especial para dicha profesión por tiempo de dos a seis años.

Artículo 200

Lo dispuesto en este capítulo será aplicable al que descubriere, revelare o cediere datos reservados de personas jurídicas, sin el consentimiento de sus representantes, salvo lo dispuesto en otros preceptos de este código.

Artículo 201

1.- Para proceder por los delitos previstos en este capítulo será necesaria denuncia de la persona agraviada o de su representante legal. Cuando aquélla sea menor de edad, incapaz o una persona desvalida, también podrá denunciar el Ministerio Fiscal.
2.- No será precisa la denuncia exigida en el apartado anterior para proceder por los hechos descritos en el artículo 198 de este Código, ni cuando la comisión del delito afecte a los intereses generales o a una pluralidad de personas.

3.- El perdón del ofendido o de su representante legal, en su caso, extingue la acción penal o la pena impuesta, sin perjuicio de lo dispuesto en el segundo párrafo del número 4º del artículo 130.

Artículo 211

La calumnia y la injuria se reputarán hechas con publicidad cuando se propaguen por medio de la imprenta, la radiodifusión o por cualquier otro medio de eficacia semejante.

Artículo 212

En los casos a los que se refiere el artículo anterior, será responsable civil solidaria la persona física o jurídica propietaria del medio informativo a través del cual se haya propagado la calumnia o injuria.

Artículo 238

Son reos del delito de robo con fuerza en las cosas los que ejecuten el hecho cuando concurra alguna de las circunstancias siguientes:
1º.- Escalamiento.
2º.- Rompimiento de pared, techo o suelo, o fractura de puerta o ventana.
3º.- Fractura de armarios, arcas u otra clase de muebles u objetos cerrados o sellados, o forzamiento de sus cerraduras o descubrimiento de sus claves para sustraer su contenido, sea en el lugar del robo o fuera del mismo.
4º.- Uso de llaves falsas.
5º.- Inutilización de sistemas específicos de alarma o guarda.

Artículo 239

Se considerarán llaves falsas:
1º.- Las ganzúas u otros instrumentos análogos.
2º.- Las llaves legítimas perdidas por el propietario u obtenidas por un medio que constituya infracción penal.
3º.- Cualesquiera otras que no sean las destinadas por el propietario para abrir la cerradura violentada por el reo.
A los efectos del presente artículo, se consideran llaves las tarjetas, magnéticas o perforadas, y los mandos o instrumentos de apertura a distancia.

Artículo 248

1.- Cometen estafa los que, con ánimo de lucro, utilizaren engaño bastante para producir error en otro, induciéndolo a realizar un acto de disposición en perjuicio propio o ajeno.
2.- También se consideran reos de estafa los que, con ánimo de lucro, y valiéndose de alguna manipulación informática o artificio semejante consigan la transferencia no consentida de cualquier activo patrimonial en perjuicio de tercero.

Artículo 255

Será castigado con la pena de multa de tres a doce meses el que cometiere defraudación por valor superior a cincuenta mil pesetas, utilizando energía eléctrica, gas, agua, telecomunicaciones u otro elemento, energía o fluido ajenos, por alguno de los medios siguientes:
1º.- Valiéndose de mecanismos instalados para realizar la defraudación.
2º.- Alterando maliciosamente las indicaciones o aparatos contadores.
3º.- Empleando cualesquiera otros medios clandestinos.

Artículo 256

El que hiciere uso de cualquier equipo terminal de telecomunicación, sin consentimiento de su titular, ocasionando a éste un perjuicio superior a cincuenta mil pesetas, será castigado con la pena de multa de tres a doce meses.

Artículo 263
El que causare daños en propiedad ajena no comprendidos en otros Títulos de este Código, será castigado con la pena de multa de seis a veinticuatro meses, atendidas la condición económica de la víctima y la cuantía del daño, si éste excediera de cincuenta mil pesetas.

Artículo 264
1.- Será castigado con la pena de prisión de uno a tres años y multa de doce a veinticuatro meses el que causare daños expresados en el artículo anterior, si concurriera alguno de los supuestos siguientes:
1º.- Que se realicen para impedir el libre ejercicio de la autoridad o en venganza de sus determinaciones, bien se cometiere el delito contra funcionarios públicos, bien contra particulares que, como testigos o de cualquier otra manera, hayan contribuido o pueden contribuir a la ejecución o aplicación de las Leyes o disposiciones generales.
2º.- Que se cause por cualquier medio infección o contagio de ganado.
3º.- Que se empleen sustancias venenosas o corrosivas.
4º.- Que afecten a bienes de dominio o uso público o comunal.
5º.- Que arruinen al perjudicado o se le coloque en grave situación económica.
2.- La misma pena se impondrá al que por cualquier medio destruya, altere, inutilice o de cualquier otro modo dañe los datos, programas o documentos electrónicos ajenos contenidos en redes, soportes o sistemas informáticos.

Artículo 270
Será castigado con la pena de prisión de seis meses a dos años o de multa de seis a veinticuatro meses quien, con ánimo de lucro y en perjuicio de tercero, reproduzca, plagie, distribuya o comunique públicamente, en todo o en parte, una obra literaria, artística o científica, o su transformación, interpretación o ejecución artística fijada en cualquier tipo de soporte comunicada a través de cualquier medio, sin la autorización de los titulares de los correspondientes derechos de propiedad intelectual o de sus cesionarios.

La misma pena se impondrá a quien intencionadamente importe, exporte o almacene ejemplares de dichas obras o producciones o ejecuciones sin la referida autorización.

Será castigada también con la misma pena la fabricación, puesta en circulación y tenencia de cualquier medio específicamente destinada a facilitar la supresión no autorizada o la neutralización de cualquier dispositivo técnico que se haya utilizado para proteger programas de ordenador.

Artículo 278
1.- El que, para descubrir un secreto de empresa se apoderare por cualquier medio de datos, documentos escritos o electrónicos, soportes informáticos u otros objetos que se refieran al mismo, o empleare alguno de los medios o instrumentos señalados en el apartado 1 del artículo 197, será castigado con la pena de prisión de dos a cuatro años y multa de doce a veinticuatro meses.
2.- Se impondrá la pena de prisión de tres a cinco años y multa de doce a veinticuatro meses si se difundieren, revelaren o cedieren a terceros los secretos descubiertos.
3.- Lo dispuesto en el presente artículo se entenderá sin perjuicio de las penas que pudieran corresponder por el apoderamiento o destrucción de los soportes informáticos.

Artículo 400
La fabricación o tenencia de útiles, materiales, instrumentos, sustancias, máquinas, programas de ordenador o aparatos, específicamente destinados a la comisión de los delitos descritos en los capítulos anteriores, se castigarán con la pena señalada en cada caso para los autores.

Artículo 536
La autoridad, funcionario público o agente de éstos que, mediando causa por delito, interceptare las telecomunicaciones o utilizare artificios técnicos de escuchas, transmisión, grabación o reproducción del sonido, de la imagen o de cualquier otra señal de comunicación, con violación de las garantías constitucionales o legales, incurrirá en la pena de inhabilitación especial para empleo o cargo público de dos a seis años. Si divulgare o revelare la información obtenida, se impondrán las penas de inhabilitación especial, en su mitad superior y, además, la de multa de seis a dieciocho meses.

ANEXO (05)

ESTADOS UNIDOS DE NORTE AMÉRICA
Acta Federal de Abuso Computacional (18 U.S.C. Sec.1030) que modificó al Acta de Fraude y Abuso Computacional de 1986. (La Sección 1029)

"La Sección 1029" La Sección 1029 prohíbe el fraude y cualquier actividad relacionada que pueda realizarse mediante el acceso o uso de dispositivos falsificados como PINs, tarjetas de crédito, números de cuentas, y algunos tipos más de identificadores electrónicos. Las nueve áreas de actividad criminal que se cubren en la Sección 1029 están listadas abajo. Todas requieren que el delito implique comercio interestatal o con el extranjero.

1. Producción, uso o tráfico de dispositivos de acceso falsificados. (El delito debe ser cometido conscientemente y con voluntad de estafar.) Pena: Multa de $50,000 o dos veces el valor del crimen cometido y/o hasta 15 años de cárcel, $100,000 y/o hasta 20 años de cárcel si se reincide.

2. Uso u obtención sin autorización de dispositivos de acceso para obtener algo de valor totalizando $1000 o más, durante un periodo de un año. (El delito debe ser cometido conscientemente y con voluntad de estafar.) Pena: Multa de $10,000 o dos veces el valor del crimen cometido y/o hasta 10 años de cárcel, $100,000 y/o hasta 20 años de cárcel si se reincide.

3. Posesión de 15 o más dispositivos de acceso no autorizados o falsificados. (El delito debe ser cometido conscientemente y con voluntad de estafar.) Pena: Multa de $10,000 o dos veces el valor del crimen cometido y/o hasta 10 años de cárcel, $100,000 y/o hasta 20 años de cárcel si se reincide.

4. Fabricación, tráfico o posesión de equipo de fabricación de dispositivos de acceso ilegales. (El delito debe ser cometido conscientemente y con voluntad de estafar.) Pena: Multa de $50,000 o dos veces el valor del crimen cometido y/o hasta 15 años de cárcel, $1,000,000 y/o 20 años de cárcel si se reincide.

5. Realización de transacciones con dispositivos de acceso pertenecientes a otra persona con el objetivo de obtener dinero o algo de valor totalizando $1000 o más durante un periodo de un año. (El delito debe ser cometido conscientemente y con voluntad de estafar.) Pena: Multa de $10,000 o dos veces el valor del crimen cometido y/o hasta 10 años de cárcel, $100,000 y/o hasta 20 años si se reincide.

6. Solicitar a una persona con el objetivo de ofrecerle algún dispositivo de acceso o venderle información que pueda ser usada para conseguir acceso a algún sistema. (El delito debe ser cometido conscientemente y con intención de estafar, y sin la autorización del propietario del sistema de acceso.) Pena: Multa de $50,000 o dos veces el valor del crimen y/o hasta 15 años de cárcel, $100,000 y/o hasta 20 años si se reincide.

7. Uso, producción, tráfico o posesión de instrumentos de telecomunicación que hayan sido alterados o modificados para obtener un uso no autorizado de un servicio de telecomunicaciones. (El delito debe ser cometido conscientemente y con ánimo de estafar.) Esto incluiría el uso de "Red Boxes", "Blue Boxes" (sí, todavía funcionan en algunas redes telefónicas) y teléfonos celulares reprogramados, cuando el usuario legítimo del teléfono que se haya reprogramado no esté de acuerdo con esa acción. Pena: Multa de $50,000 o el doble del valor del crimen cometido y/o hasta 15 años de cárcel, $100,000 y/o hasta 20 años de cárcel si se reincide.

8. Uso, fabricación, tráfico o posesión de receptores-escaneadores o hardware o software usado para alterar o modificar instrumentos de telecomunicaciones para obtener acceso no autorizado a servicios de telecomunicaciones. Esto también incluye los scanners que mucha gente usa para interceptar llamadas de teléfonos celulares. Se suscitó un gran escándalo cuando los medios de comunicación tuvieron noticia de una llamada de un celular interceptada (la llamada correspondía al Portavoz de los Representantes de la Casa Blanca, Newt Gingrinch.) Pena: Multa de $50,000 o dos veces el valor del crimen y/o hasta 15 años de cárcel, $100,000 y/o hasta 20 años si se reincide.

9. Hacer creer a una persona el delincuente es un miembro de su compañía de tarjeta de crédito o su agente para obtener dinero o realización de transacciones hechas con un dispositivo de acceso Y viceversa (tratar de hacer creer a la compañía de crédito que se trata de la persona legítima). El delito debe ser cometido conscientemente y con objetivo de estafar, y sin permiso. Pena: Multa y/o hasta 1 año de cárcel, hasta 10 años si se reincide.

"La Sección 1030" 18 USC, Capítulo 47, Sección 1030, como parte de la Ley sobre Abuso y Fraude Informático de 1986, prohíbe el acceso no autorizado o fraudulento a ordenadores gubernamentales, y establece diversas condenas para esa clase de accesos. Esta ley es una de las pocas piezas de legislación federal únicamente referida a ordenadores. Bajo la Ley de Abuso y Fraude Informático, el Servicio Secreto americano y el F.B.I. tienen jurisprudencia para investigar los delitos definidos en este decreto. Las seis áreas de actividad criminal cubiertas por la Sección 1030 son:

1. Adquisición de información restringida relacionada con defensa nacional, asuntos exteriores o sobre energía nuclear con el objetivo o posibilidad de que sean usados para dañar a los Estados Unidos o para aventajar a cualquier otra nación extranjera. (El delito debe ser cometido consciente-mente accediendo a un ordenador sin autorización o exceder el acceso autorizado.)

2. Obtención de información en un registro financiero de una institución fiscal o de un propietario de tarjeta de crédito; o de información de un cliente en un archivo de una agencia de información de clientes. (El delito debe ser cometido conscientemente intencionadamente accediendo a un ordenador sin autorización o excediendo el acceso autorizado.) Pena: Multa y/o hasta 1 año de cárcel, hasta 10 años si se reincide.
3. Atacar un ordenador que sólo corresponda ser usado por algún departamento o agencia del gobierno de los EEUU, para el caso de que no sólo puede ser usada por esta agencia, atacar un ordenador usado por el gobierno en el que la intrusión producida afecte el uso que el gobierno hace de él. (El delito debe ser cometido intencionadamente accediendo a un ordenador sin autorización.)

4. Promover un fraude accediendo a un ordenador de interés federal y obtener algo de valor, a menos que el fraude y la cosa obtenida consistan solamente en el uso de dicho ordenador. (El delito debe ser cometido conscientemente, con intención de cometer dicho fraude, y sin autorización o excediéndose de la autorización obtenida) [La visión que tiene el gobierno de "ordenador de interés federal" está definida abajo] Pena: Multa y/o hasta 5 años de cárcel, hasta 10 años si se reincide.

5. A través del uso de un ordenador utilizado en comercio interestatal, transmitir intencionadamente programas, información, códigos o comandos a otro sistema informático. Existen dos situaciones diferentes:

A.- En esta situación (I) la persona que realiza la transmisión está intentando dañar el otro ordenador o provocar que no se permita a otras personas acceder a él; y (II) la transmisión se produce sin la autorización de los propietarios u operadores de los ordenadores, y causa $1000 o más de pérdidas, o modifica o perjudica, o potencialmente modifica o altera un examen o tratamiento médico. Pena con intento de dañar: Multa y/o hasta 5 años de cárcel, hasta 10 años si se reincide.

B.- En esta situación, (I) la persona que realiza la transmisión no intenta hacer ningún daño, pero actúa imprudentemente despreciando el riesgo que existe de que la transmisión causara daño a los propietarios u operadores de los ordenadores y provoca $1000 o más de pérdidas, modifica o potencialmente modifica un examen o tratamiento médico. Pena por actuación temeraria: Multa y/o hasta 1 año de cárcel.

5. Promover el fraude traficando con passwords o información similar que haga que se pueda acceder a un ordenador sin la debida autorización. Todo esto si ese tráfico afecta al comercio estatal o internacional o si el ordenador afectado es utilizado por o para el Gobierno. (El delito debe ser cometido conscientemente y con voluntad de estafar.) Pena: Multa y/o hasta 1 año de cárcel, hasta 10 años si se reincide.

Para la Sección 1030, un ordenador de interés federal tiene las siguientes características:

1. Un ordenador que es exclusivamente para el uso de una institución financiera o del Gobierno de los EEUU o, si su uso no está restringido a lo anterior, uno usado por una institución financiera o el gobierno de los EEUU en el que el ataque afecte negativamente al servicio que está desarrollando en esas instituciones.

2. Un ordenador de los dos o más que hayan sido usados para cometer el ataque, no estando todos ellos en el mismo estado. Las disposiciones citadas se complementan con los siguientes instrumentos: 18.U.S.C. 875 Interstate Communication Including Threats, kidnapping, Ransom, extortion 18 U.S.C. 1343 Fraud by wire, radio or television 18 U.S.C. 1361 Injury to Goverment Property 18 U.S.C. 1362 Government Communication systems 18 U.S.C. 1831 Economic Espionage Act 18 U.S.C. 1832 Trade Secrets Act.

ANEXO "A": MATRIZ DE CONSISTENCIA (ESTRUCTURA ANALITICA)

TITULO DE LA INVESTIGACIÓN: LOS DELITOS INFORMATICOS EN EL CÓDIGO PENAL

PROBLEMAS	OBJETIVOS	HIPOTESIS	VARIABLES	INDICADORES
Problema General ¿En que medida los **delitos informáticos** no son denunciados e investigados en sede policial y judicial, pese a que se encuentran tipificados en el **Código Penal** vigente?.	**Objetivo General** Demostrar que el problema de los **delitos informáticos** se debe a que su tipificación en el **Código Penal** vigente, es deficiente e inoperante frente a los ilícitos que originan el avance tecnológico.	**Hipótesis General** Si se incrementa la comisión de los **delitos informáticos**, entonces el **Código Penal** vigente tiene deficiencias en su aplicación.	**Variable Independiente(VI)** Delitos Informáticos **Variable Dependiente (VD)** Código Penal	- Difícil control e investigación - Crea caos social - Atenta contra bienes jurídicos protegidos - Vacío legal - Ineficiente - No acorde con avance tecnológico
Problemas Secundarios 1. ¿Por qué se incrementa la **piratería informática**, afectando el derecho de autor, así como el **patrimonio** de personas y empresas de software, pese a que se encuentra legislado en el Código Penal?	**Objetivo Específicos** 1. Comprobar que el incremento de la **piratería informática** afecta el derecho de autor y el **patrimonio** de personas y empresas de software, debido a la inadecuada tipificación en la legislación penal.	**Hipótesis Secundarias** 1. El incremento de la **piratería informática** se debe a que la legislación penal actual es deficiente, originando el incremento y desprotección del derecho de autor y **patrimonio.**	**Variable Independiente (VII)** Piratería Informática **Variable Dependiente (VD1)** Patrimonio	- Mercado negro - Novedoso - Trata de sistemas informáticos - Tangible - Intangible - Apropiación y perdida económica
2. ¿Por qué en la actualidad se viene incrementando los delitos cometidos a través de **medios informáticos**, sabiendo que estos atentan **contra la vida el cuerpo y la salud**?	2. Demostrar que el incremento de los delitos realizados por **medios informáticos**, se debe a consecuencia del avance y desarrollo tecnológico e informático, originando ilícitos que atente **contra la vida el cuerpo y la salud** de las personas.	2. A mayor incremento de los delitos realizados por **medios informáticos**, mayor incremento de delitos que atentados contra **la vida el cuerpo y la salud**.	**Variable Independiente (V12)** Medios Informáticos **Variable Dependiente (VD2)** La vida el cuerpo y a salud	- Computarizados - Desarrollo Informáticos - Avance de tecnología - falta de prevención - Incremento - Menores
3. ¿Por qué se incrementa con tanta facilidad y rapidez la **pornografía infantil** por Internet, pese a que se encuentra sancionado en el Código Penal y sabiendo que es un delito que atenta **contra el pudor**, **honor e intimidad de los menores de edad**?	3. Demostrar que el incremento de la **pornografía infantil por Internet**, se debe a la inoperancia de la legislación penal, originando el incremento de ilícitos que atentan **contra pudor, honor e intimidad** de los menores de edad.	3 El incremento de la **pornografía infantil por Internet** se debe a la deficiente e inoperancia de la legislación penal, originando el incremento de delitos que **atentan contra el pudor, honor y la intimidad** de menores de edad**.**	**Variable Independiente (V13)** Pornografía infantil por Internet **Variable Dependiente (VD3)** Pudor, Honor y la intimidad	- Pobreza - Descuido familiar - Extranjeros - se viene incrementando - Poco denunciado - Legislación inadecuada