

UNIVERSIDAD DE LIMA

Facultad de Derecho y Ciencias Políticas

**“DELIMITACIÓN DEL DELITO INFORMÁTICO:
BIEN JURÍDICO PROTEGIDO Y
ANÁLISIS DE LEGISLACIÓN VIGENTE”**

Tesis para obtener el Título de Abogado

**GRETTEL MARIE SOLANGE
OLIVOS LIEVEÿNS**

-Lima 2001-

Dedicatoria

A mis padres, cuyos sacrificios y esfuerzos debo mi carrera universitaria.

-
-
-
-

-
-
-
-
-
-

Agradecimientos

A la Doctora María del Carmen García Cantizano quien como profesora, consejera, pero sobre todo amiga, apoyó la realización del presente trabajo. Por su invaluable esfuerzo, por el tiempo y paciencia para las correcciones efectuadas.

Al Profesor Julio F. Mazuelos Coello, por ser el autor de esta brillante idea, con todo el sacrificio y gratitud que merecen sus afanes y estímulos para la iniciación y término del presente trabajo.

Al Doctor Julio César Núñez Ponce, profesor del curso de Derecho Informático, quien con su decidido apoyo y aporte de ideas, colaboró en el desarrollo de esta importante labor.

A Eduardo Catter Cossio, Project Manager de AT&T Latin America, por su confianza en la información brindada y,

A todas aquellas personas que de algún modo, colaboraron con información relevante para la culminación de esta tesis.

-
-

-
-

Sumario

PORTADA.....	I
DEDICATORIA	II
AGRADECIMIENTOS.....	III
SUMARIO.....	IV
ÍNDICE DE LAS ABREVIATURAS.....	V
INTRODUCCIÓN.....	VI

Primera Parte

APROXIMACIÓN AL TEMA

Capítulo I. : Análisis de la realidad. 1

Capítulo II : Algunas precisiones acerca de la criminalidad informática como nueva forma de criminalidad 29

Segunda Parte

LOS DELITOS INFORMÁTICOS: MARCO LEGAL

Capítulo I : Delimitación conceptual del delito informático 58

Capítulo II : Posición personal respecto del concepto de delito informático. 144

Capítulo III. : Los delitos informáticos en el Código penal peruano. 160

Capítulo IV : Los delitos informáticos en la legislación comparada 194

Tercera Parte

PROPUESTA DE *LEGE FERENDA*

Capítulo I : Fundamentos de la regulación administrativa 232

CONCLUSIONES..... 242

GLOSARIO DE TÉRMINOS. 246

BIBLIOGRAFÍA..... 270

BIBLIOGRAFÍA DE BOLETINES Y REVISTAS..... 276

TESIS CONSULTADAS.....	280
DICCIONARIOS CONSULTADOS.....	281
PÁGINAS WEB CONSULTADAS.....	282
ÍNDICE.....	285

Índice de las abreviaturas

art.	artículo
arts.	artículos
cap.	capítulo
caps.	capítulos
cfr.	confróntese, véase.
c.p.	Código penal.
c.p.e.	Código penal español.
c.p.p.	Código penal peruano.
c.d.p.p.	Código de procedimientos penales.
e.g.	exempli gratia: por ejemplo
ibídem.	en la misma referencia, en el mismo libro o artículo de la nota anterior
i.e.	es decir, esto es.
infra.	va más adelante, en el mismo trabajo.
loc. cit.	en el pasaje referido, en el lugar citado.
núm.	número
núms.	números
obr. cit.	obra citada en una nota anterior.
op. cit.	obra citada.
pp.	página.
ss.	páginas.
supra.	véase más arriba, en la parte anterior.
StGB.	Código penal alemán.
StPO.	Código procesal penal alemán.

c.c.	Código civil.
c.o.	Constitución política del Perú.
vid.	véase.

Introducción

En los últimos 50 años hemos sido testigos de una elevada escala de tecnología informática. El desarrollo de los sistemas informáticos produce, a su vez, el desarrollo de nuevas formas de comunicación entre los individuos.

Producto de todo el avance tecnológico, el Derecho también se ve inmerso en nuevas formas de actividades de diverso tipo, en las cuales la intervención de los sistemas informáticos para su realización es cada vez más común. Todo esto origina que surjan contratos que se celebren a través de una sistema operativo o que se realicen actos de comercio a través de la red.

Estas conductas no siempre son lícitas, por lo que es necesario su debida regulación para garantizar la participación de los usuarios en la Red y para un correcto funcionamiento de los sistemas.

Es indudable, pues, que la informática produce cada día una intensa evolución en las distintas ramas del Derecho (Derecho constitucional, Derecho civil, Derecho comercial, Derecho penal, etc.). Esta nueva realidad nos pone frente al desafío de encontrar fórmulas eficaces de aplicación del Derecho -en nuestro caso, del Derecho penal- porque constituye también parte esencial del desarrollo tecnológico y comercial del mundo entero.

Como es sabido, el uso de sistemas informáticos forma desde hace mucho tiempo una pieza clave en la vida de cada individuo, el cual se ve sujeto a la necesidad de tener una computadora, una base de datos, la red, etc., como medio para realizar diversas conductas en su vida diaria.

Mucho se habla de los grandes beneficios que los medios de comunicación y el uso de la informática han aportado a la sociedad actual, sin embargo, el desarrollo tan amplio de la tecnología informática ofrece también un aspecto negativo, ya que se han generado nuevas conductas antisociales y delictivas que se manifiestan en formas que no era posible imaginar en el siglo pasado. Los sistemas de computadoras ofrecen oportunidades nuevas y muy complejas de infringir la ley y han creado la posibilidad de cometer delitos tradicionales en formas no tan tradicionales.

Es innegable, pues, que los avanzados cambios en la tecnología de los sistemas informáticos provocan una serie de cambios en la realidad social. Estos cambios, quiérase o no, repercuten en todas las personas que utilizan estos medios informáticos, ya sea por motivos laborales, como de entretenimiento. Es así que debido a estos procesos de aceleración en la informática, surgen también nuevas formas de conductas delictuales.

La respuesta de nuestros legisladores no se ha hecho esperar, la nueva Ley N° 27309 -Ley que incorpora los delitos informáticos al Código penal-, fue promulgada el 15 de julio del año 2000 y publicada con fecha 17 de julio del mismo año. La ley que incorpora los delitos informáticos al Código penal consta de tres artículos: 207-A, 207-B y 207-C.

En definitiva, podemos afirmar que la Ley N° 27309 es la respuesta frente a las nuevas formas delictuales que se vienen originando debido al desarrollo tecnológico de los sistemas de datos, red y programas de computadoras.

Ahora bien, la sencillez con la cual ha aparecido esta nueva ley y la facilidad que aparecen estas conductas antisociales, no se asemejan en lo absoluto con la elaboración de los nuevos tipos penales en la legislación penal peruana. Es por esto que debe existir una solución adecuada a este problema que esté acorde con la realidad y con la sociedad actual. Esta pretensión es materia de análisis en la presente investigación desde una revisión de la incidencia social del uso de las computadoras y sistemas informáticos, y de aquellas conductas que resultan nocivas para los mismos, para a partir de allí confrontar los aciertos o desaciertos de la legislación penal sobre la materia.

En este orden de ideas, en el primer capítulo se explicará la incidencia social de las computadoras, se tratará, asimismo, la relación de la informática y los nuevos procesos de comunicación de las personas en la red.

Adicionalmente, se analizará la identificación de los sujetos intervinientes en la red: el anonimato de los usuarios como característica fundamental de la red, identificación de los intereses en juego en la red y de sus titulares y el significado que tiene el término "libertad" en Internet, así como el valor supremo que éste posee en la red y sus consecuencias.

Por último, se hablará del origen de Internet, los contenidos ilegales, la Free Net, las amenazas dentro de la red y la urgente y necesaria regulación de Internet.

En el segundo capítulo se desarrollarán algunas precisiones acerca de la criminalidad informática como nueva forma de criminalidad, comprendiendo aspectos generales y descripción de aquellas conductas nocivas que se cometen a través de sistemas informáticos y de Internet. Asimismo, se enunciarán las conductas nocivas e ilícitas según la Organización de las Naciones Unidas y otras conductas no previstas.

En la segunda parte de la presente investigación, capítulo primero, se explicará el concepto de delito, para a partir de allí, realizar una delimitación conceptual del delito informático y del bien jurídico protegido; en este cometido resulta necesario ocuparnos, sin ánimo exhaustivo, de la problemática actual vinculada a la delimitación del bien jurídico y la función del Derecho penal en la sociedad actual, pues entendemos imprescindible su análisis previo, para poder adoptar una posición personal sobre el delito informático. Uno de los principales objetivos de este apartado es la determinación y conceptualización de bienes jurídicos con identidad propia en el ámbito de los sistemas informáticos.

Por último, fundamentaremos nuestra posición respecto al bien jurídico protegido en los delitos informáticos.

En el capítulo segundo, explicaremos la posición adoptada respecto al concepto de delito informático, relacionando aquellas conductas desarrolladas en el punto 1.2., en el capítulo segundo, primera parte. Se enunciarán las principales clasificaciones de los delitos informáticos así como las principales manifestaciones de los delincuentes informáticos, y por último se desarrollará la tipología del delincuente informático.

En capítulo tercero, se explicarán los delitos informáticos en el Código penal Peruano. Se revisará la sistemática seguida por el legislador para su configuración, el análisis de la Ley 27309, así como los delitos de intrusismo informático, daño informático y sus formas agravadas. Por último, se analizará los aspectos problemáticos de la tipificación de los delitos informáticos en la legislación penal peruana.

En el capítulo cuarto de la presente investigación, nos ocuparemos, además, de la legislación penal adoptada sobre la materia por otros países, como Alemania, España, Estados Unidos de Norte América y Chile, con la finalidad de contrastar los diversos modelos de regulación de los delitos informáticos y evaluar aportes que sirvan de modelo para la legislación penal nacional.

La tercera parte contiene un solo capítulo, el mismo que abarca la necesidad de un ente regulador, la debida reformulación de los tipos penales del delito informático y un proyecto de ley, como propuesta de *lege ferenda*.

Cabe señalar, que la presente investigación pretende proporcionar criterios que sirvan para un análisis crítico de las disposiciones penales respecto de la nueva Ley N° 27309 y, en este sentido, no sólo aportar elementos de juicio para una futura reforma legislativa, sino evitar posibles arbitrariedades por parte de los aplicadores del Derecho, es decir, dar a los jueces los elementos de juicio que permitan una óptima aplicación de las normas penales informáticas.

Sería inadecuado concluir un trabajo de investigación advirtiendo simplemente los errores que posee la reciente ley aprobada o la urgente necesidad de regulación de las nuevas conductas delictivas que se vienen originando. Así, creemos que el objetivo de un trabajo de investigación debe ser dar una solución a un problema específico. Es por esto que hemos tratado de buscar una forma de regulación que debe de estar acorde con el Derecho penal peruano de forma óptima, concisa y entendible. Así, hemos considerado a la seguridad informática como un bien jurídico penalmente relevante. Bien jurídico que creemos que es propio de los delitos informáticos y que es urgente y necesaria su debida regulación, por lo que se elaborará un proyecto de *lege ferenda* de un modelo de regulación de los denominados delitos informáticos de acuerdo con nuestra sociedad y sistema de justicia penal. Estamos seguros que los temas aportados serán merecedores de discusión y de críticas, sin embargo, nos sentiremos satisfechos cuando el presente trabajo de investigación reciba las respectivas críticas que ayuden al legislador en la tipificación de nuevos tipos penales.

No podemos perder de vista la complejidad que este tema requiere en cuanto a la tipificación de los delitos informáticos en nuestro Código penal y la utilización de anacronismos muy de moda en estos días. Este trabajo no puede abordar a profundidad el tan amplio tema de los delitos informáticos, por eso, conductas como el hacking o cracking, son las que, por razones de tiempo y espacio, se tocarán de forma muy superficial, ya que estas conductas deben ser objeto de un estudio más profundo que excede los alcances de la presente investigación, por lo que nos vemos en la necesidad de limitar este trabajo, debido a que tiene como objetivo el análisis de los ilícitos informáticos desde un punto de vista penal y no desde una perspectiva eminentemente informática. Por tanto, de ninguna manera este trabajo constituye un examen exhaustivo de todas las conductas infractoras en la red, sino un estudio preliminar de aquellas que han sido recogidas por el legislador y tipificadas como delitos informáticos.

En cuanto a los niveles alcanzados por la criminalidad informática en la actualidad, no nos podemos alejar de la idea que la criminalidad organizada dependerá ya no sólo de un grupo de personas bien articulado, con muchos eslabones que dependen unos de otros, sino que estos eslabones, a su vez, dependerán también de un sistema de almacenamiento, de funcionamiento, que consistirá en un ordenador, entendiéndose éste como una computadora. Por ello, la presente investigación toma como criterio de análisis el desarrollo doctrinario vinculado a la globalización del fenómeno criminal y a la tendencia de internacionalizar su represión.

Preguntas como si son suficientes los bienes jurídicos ya reconocidos en el Código penal, o si se requiere de un nuevo objeto

jurídico de protección penal, o cuál será la repercusión del uso de la red en los principios generales del Derecho penal o si es correcta la legislación existente sobre los delitos informáticos respecto de la realidad peruana tratarán de ser resueltas, o se intentará hallar una respuesta, que no siempre resultará del agrado y opinión del lector, pero cuya introducción se realiza, al menos, con el deseo y la confianza de que pueda contribuir a despertar el interés y el espíritu crítico de quien se interese por este trabajo.

En la presente investigación no pretendemos crear un sistema penal óptimo para la regulación de los llamados delitos informáticos, ya que sería caer en lo irreal del Derecho penal, sin embargo, trataremos de dar, a nuestro parecer, las mejores pautas para una modificación de la ley de los delitos informáticos con el fin de una mejor regulación y, más aún, de una mejor aplicación de las normas penales informáticas por nuestros jueces.

Cabe señalar que el material bibliográfico empleado para la presente tesis comprende, principalmente, doctrina y legislación alemana, española, americana, chilena y peruana. Hemos tratado, en las medidas de nuestras posibilidades, de concentrarnos en la revisión de libros y revistas de los últimos años. Además, links y páginas web que comprenden temas acerca de los delitos informáticos que han sido de gran aporte para la culminación del presente trabajo.

Por último, es nuestro deseo que este esfuerzo intelectual pueda servir a quienes se interesen, ya sea desde el Derecho informático o desde el Derecho penal, por los problemas actuales de las nuevas formas de criminalidad vinculadas al desarrollo de la tecnología y los retos que representan para la sociedad actual; tan sólo con eso, nos sentiremos satisfechos en la tarea emprendida.

Primera Parte

APROXIMACIÓN AL TEMA

Capítulo I

Análisis de la realidad

Introducción

Comenzar el presente trabajo abordando directamente el análisis de la realidad del uso de sistemas informáticos, constituye una opción metodológica para el desarrollo de la presente tesis, la misma nos acercará a la propia actuación de las personas y sus conflictos generados en la red. Asimismo, podremos observar como el desarrollo de los sistemas informáticos ha producido grandes cambios en nuestra sociedad.

Hoy en día, nadie duda de la importancia que han adquirido en la actualidad la utilización de sistemas informáticos para el buen desarrollo de la vida en sociedad.

Concordamos con la idea de MATELLANES[1] al señalar que “es más que irrefutable la importancia que ha adquirido en nuestros días la utilización de los sistemas informáticos para el funcionamiento de la vida social en aspectos de tanta trascendencia como la Administración Pública o de Justicia, la banca[2], los operadores económicos, la seguridad pública, la sanidad y la investigación científica.”

Para explicar la importancia de estos sistemas en la vida diaria de cada individuo, empezaremos este capítulo por la explicación de la incidencia social que ha originado el uso de las computadoras en la colectividad. Seguidamente, explicaremos en qué consiste el ciberespacio y el anonimato, así como los sujetos que intervienen en la red.

Por último, nos dedicaremos a explicar la necesidad de una regulación en Internet en salvaguarda de los intereses de los individuos que ingresan a este sistema.

1.1 Incidencia Social de las Computadoras

Han pasado más de cincuenta años desde que Howard Aiken presentó en la Universidad de Harvard la primera computadora. Décadas más tarde, la evolución tecnológica ha dejado atrás los antiguos tubos electrónicos y válvulas para reemplazarlos, en la actualidad, por diminutos circuitos integrados que procesan millones de operaciones por segundo.[3]

De un tiempo a esta parte, las computadoras han evolucionado de una manera muy rápida, tan rápida que apenas la sociedad puede asimilar estos nuevos cambios. Los efectos de Internet tienen una importante incidencia sobre la estructura familiar y social. Gran parte de individuos que observaban a las computadoras como medios muy sofisticados en cuanto a su utilización, se han visto obligados al uso de las computadoras en su vida diaria.[4] No podemos dejar de mencionar el apreciable valor y los grandes aportes que ha producido Internet en los casos de las personas discapacitadas.[5]

El hombre común ensarta su comunicación e historia en los recuerdos, la memoria y la escritura. El hombre-digital no necesita estas funciones para desenvolverse y crecer, dado que puede almacenar y recuperar información con facilidad y rapidez. El *bit* [6] y la velocidad en su transmisión han adquirido el máximo protagonismo, hasta el punto de definir y caracterizar la era digital.

La realidad informática presenta, en ocasiones cada vez más numerosas, la utilización de sistemas informáticos en la sociedad actual.[7] Hoy en día nadie duda de la incidencia que han tenido las computadoras en la sociedad. Cada día más son las familias que poseen una computadora en su casa[8] y ya nadie se puede imaginar una empresa que no posea una computadora.

En la actual configuración social es necesario una complejidad de relaciones interpersonales, esta complejidad lleva implícito -muchas veces- el sistema de servicios informáticos para consolidar relaciones sociales. El hombre organiza su vida según sus conocimientos y según sus experiencias, por tanto, a mayor conocimiento de la informática, mayor hará uso de ésta.

Ahora bien, esta interiorización de los sistemas informáticos en las formas de comunicación de los sujetos se ve influenciada por los procesos de internacionalización de las economías, los mercados y por el fenómeno de la globalización. En efecto, como acertadamente señala SILVA SANCHEZ[9], “la globalización – como salto cualitativo de la internacionalización- es una de las características definitorias de los modelos sociales postindustriales, cuya principal expresión es ser un fenómeno económico orientado a la eliminación de las restricciones a las transacciones y la ampliación de los mercados.” Como consecuencia de ello se ha de agregar, sin lugar a dudas, otro fenómeno: la globalización de las comunicaciones, generado por las innovaciones técnicas.

Si bien es cierto que nuestro país no está considerado como un país postindustrial, el avance tecnológico modifica altamente el desarrollo social del Perú. Un indicador importante para evaluar la capacidad de respuesta de las sociedades a los desafíos de la nueva sociedad en despegue, es su capacidad para incorporarse a las redes que crecientemente enlazan al mundo.[10]

En este sentido, el Perú no se encuentra a la saga. En el mes abril del año 1999, la cantidad de internautas ascendía a 100,000 y se multiplicó por cuatro en los diez meses siguientes. Según datos del Instituto Nacional de Estadística e Informática, a fines del mes de mayo del año 2000, la cantidad volvió a duplicarse llegando a 820,000 personas que utilizaban Internet como medio de comunicación o para la adquisición de algún producto. Sin duda, podríamos llegar a decir que se trata de una de las tasas de crecimiento más elevadas del mundo.[11]

De las cantidades anteriormente descritas, el 26% de usuarios de Internet accede al servicio desde su centro de trabajo. Otro 50% lo hace desde cabinas públicas.[12] El resto de porcentaje, suponemos que comprendería el acceso al servicio de Internet desde cada uno los hogares de las personas que ingresan a este sistema. Por otro lado, se espera que para este año en el Perú las inversiones publicitarias en Internet alcancen un crecimiento aproximado de 300 por ciento.[13]

Como se puede observar la incidencia que tiene el desarrollo tecnológico en el Perú es elevada, por lo que es innegable argumentar que nuestra sociedad se encuentra también inmersa dentro de todo el desarrollo tecnológico evidenciado en países altamente industrializados. Sin embargo, no debemos olvidar las consecuencias negativas que el propio avance trae consigo, como, por ejemplo, la aparición de nuevos riesgos para los usuarios de sistemas informáticos en la medida que deberán adoptar nuevas formas de conductas para solventarlos.

1.2 Informática y Proceso de Comunicación de las Personas en la Red

1.2.1 Breve Reseña Histórica

Los pueblos primitivos en la antigüedad buscaron un medio para registrar el lenguaje. Para ello utilizaron signos que designaban a una tribu o pertenencia, ya que no habían desarrollado otras formas de comunicación. Posteriormente, alrededor del año 700 A.C, surge el alfabeto en Grecia, el cual determinó la infraestructura mental necesaria para una comunicación de tipo acumulativa basada en el conocimiento. Este nuevo orden permitió dentro del discurso racional, separar la comunicación escrita del sistema audiovisual de símbolos y percepciones.

A partir del desarrollo de la civilización y de las lenguas escritas, surgió también la necesidad de comunicarse a distancia de forma regular. Así es como se fueron desarrollando múltiples formas de comunicación: los servicios postales, el telégrafo, el teléfono, la telefonía celular, el fax, etc.

Las comunicaciones ocupan un lugar central y preponderante en el desarrollo de los individuos. Desde la comunicación oral hasta la virtual el hombre ha modificado su conducta y su manera de percibir la realidad.

1.2.2 Nuevas Formas de Comunicación

1.2.2.1 Internet Relay Chat

La comunicación mediada por computadoras ha generado nuevas formas de comunicación entre las personas como por ejemplo el fenómeno del IRC[14]. IRC es el acrónimo de *Internet Relay Chat*, y es un protocolo que permite intercambiar mensajes en forma directa a un gran número de usuarios conectados simultáneamente a la red por medio de servidores de IRC diseminados por todo el mundo. Con frecuencia se lo utiliza para charlas simples o juegos intrascendentes, aunque otras veces se lo ha empleado para cosas más serias; por ejemplo, durante la Guerra del Golfo y en otras situaciones catastróficas, sirvió para obtener noticias en directo. Dicha comunicación es en tiempo real y sus implicancias y sus efectos sobre los sujetos que participan en dichas conversaciones podría llegar a ser adictivo.[15]

1.2.2.2 El Correo Electrónico

Otra forma de comunicación virtual entre las personas es el uso del correo electrónico. Años atrás, los individuos debían de conformarse con el uso del correo postal, en donde una carta podía demorar meses en ser leída por su destinatario, sin embargo, hoy en día el uso del correo electrónico ha favorecido muchísimo no sólo las relaciones personales, sino también los negocios, la economía y la industria.[16]

En tanto la realidad social ofrece un sin número de posibilidades de formas de comunicación, estas posibilidades proveen que a través de la red un individuo pueda optar por la personalidad que quiera. “La máscara que facilita la red, la facultad de simulación, permite a algunos de sus navegantes ganarse el respeto de otros usuarios, a los que no podrían acercarse en la sociedad real.”[17]

Podríamos atrevernos a decir que la comunicación social no podría conseguirse de una manera eficiente sin el empleo del uso del correo electrónico, cámaras virtuales, etc., ya que hoy en día el ser humano no puede desarrollarse de forma óptima (en tiempo y espacio) sólo con el uso de medios de comunicación tradicionales, tales como el correo postal o los videos comunes. Por estas razones, cada vez más los contactos sociales son producto de nuevas formas de avanzada tecnología.

Como es sabido, el desarrollo de esta tecnología no sólo se encuadra en los cambios sociales que produce el uso de los sistemas informáticos. La industria, la economía, la educación, la administración pública, los sistemas financieros etc., son testigos de los cambios que se han producido en estos últimos cincuenta años. El Derecho no es la excepción.

Si bien es cierto que el presente trabajo no pretende enunciar de manera amplia todos los cambios que se han originado desde la creación de los medios informáticos, ya que de esto, se ocupa el Derecho Informático, nos parece necesario destacar la relación existente entre la informática y las diversas ramas del Derecho, las mismas que han tenido en muchos casos que cambiar su normativa vigente y/o adaptar su derecho positivo a las necesidades que la informática obliga. Así, tenemos en el Derecho contractual la mutación de los contratos tradicionales escritos por los llamados contratos virtuales o contratos

electrónicos[18], incluyendo la firma digital[19], innovación dada mediante la Ley de Firmas Digitales y Certificados Digitales (LFCD), ley aprobada y en revisión su reglamento.

De igual manera, en cuanto al Derecho comercial, mediante el uso del Internet es posible adquirir todo tipo de productos en la red, desde un libro hasta semillas de marihuana para fines agroindustriales.

Asimismo, el Derecho tributario se ha visto obligado a implementar y modernizar nuevamente -exactamente desde enero del presente año-, su página web (versión 2.0) en donde se encuentra el formulario N° 688 para ser llenado por los deudores tributarios. Un cambio importante es también la violación de Derechos bancarios[20] por dominios relacionados con el derecho de competencia.

No es nuestro objetivo relacionar los avances tecnológicos con todas las ramas del Derecho, ya que escapa a las pretensiones de la investigación por ello la evolución tecnológica es tomada en cuenta sólo cuando incide en nuevas formas de conductas que pudieran tener incidencia sobre el Derecho penal.

En efecto, si bien es cierto que todos estos avances tecnológicos son bien recibidos por la sociedad; este desarrollo sumado a los fenómenos económicos de la globalización y de la integración económica dan lugar a la conformación de nuevas modalidades de delitos clásicos, así como a la aparición de nuevas formas delictivas. [21]

1.3 Principales Características en la Red

1.3.1. El Ciberespacio

“El desarrollo alcanzado por los elementos electrónicos, unión con las redes de telecomunicaciones determinan la creación de una zona donde las personas pueden interactuar sin estar físicamente presentes”[22]. Esta zona, es denominada “ciberespacio”.

Por ciberespacio se puede entender el lugar en el cual ocurren determinadas conductas, desde conversaciones telefónicas, comunicación por chat, envío de mensajes electrónicos, compra de artículos de diversas clases, etc.

“El concepto de ciberespacio, expresa la directa incidencia de la nueva tecnología sobre la efectividad de los límites territoriales de los Estados y sobre las políticas que, sin integrar este concepto operativo puedan diseñar y pretendan hacer valer.”[23] Así, el ciberespacio origina una nueva cultura, la denominada “cultura tecnológica”.

Bien hace STERLING[24] al señalar que el ciberespacio no es real, sin embargo, es serio y muy importante.

En el ciberespacio la gente se conoce, muchos se enamoran[25], y hasta algunos se casan[26], existen comunidades enteras viviendo en el ciberespacio, charlando, consultándose y enviándose correo de voz y correo electrónico y hasta cometiendo conductas antisociales tanto en forma individual como grupal.

“El ciberespacio es hoy en día una red, una matriz de alcance internacional y que crece rápida y constantemente. Crece en tamaño, en riqueza y en importancia política.”[27]

El desarrollo del ciberespacio es cada vez tan exorbitante, que Internet cuenta ya con más de 150 millones de usuarios en el planeta. Cada hora aparecen 6,500 nuevas páginas en la Red, cada día se conectan 15,000 nuevos usuarios y para el presente año 2001 se espera que superen los 350 millones.[\[28\]](#)

-
Por último, “podemos inferir que el ciberespacio es una realidad nueva que va adquiriendo día a día mayor importancia estratégica desde el punto de vista: empresarial, cultural, político y social; que para su funcionamiento necesita de un medio físico adecuado, el mismo que se encuentra en Internet”.[\[29\]](#)

1.3.2. El Anonimato

Ahora bien, “las nuevas formas de comunicación electrónica horadan el ámbito de la subjetividad. El anonimato de la red promueve igualmente actitudes críticas abiertas, puntos de vista excéntricos e impopulares, estimulando la promiscuidad del yo. El género, la orientación sexual, la edad, todo puede cambiar al instante y a voluntad, en la creación de una nueva y efímera identidad.”[\[30\]](#) Por tanto, las personas en la red pueden poseer cualquier nacionalidad, cualquier inclinación religiosa, cualquier tipo de vida y ser identificados bajo una personalidad virtualmente construida.[\[31\]](#) No en vano se dice que Internet es la reina del anonimato.

Este hecho es de enorme importancia, toda vez que la sociedad está construida sobre las bases de una comunicación personalizada, en la cual los contactos directos e individualizados son su característica principal; sin embargo, se expande hoy en día en la sociedad la idea del anonimato en las relaciones sociales, es decir, la despersonalización de los contactos como, por ejemplo, cada vez sabemos menos quien es nuestra contraparte en una operación bancaria debido a los cajeros automáticos. En la comunicación que se origina por medio del chateo en Internet, la mayoría de personas no se conocen físicamente sino sólo a través del medio de comunicación virtual.[\[32\]](#)

Así, aparecen hoy día nuevas formas de criminalidad que son difíciles de comprobar.[\[33\]](#)

“En primer lugar, porque las nuevas técnicas han supuesto la incorporación al mundo jurídico de un nuevo ámbito de regulación (los derechos u obligaciones consecuentes a la creación, distribución, uso del hardware y el software, a las bases de datos, a la contratación de servicios informáticos o a la transferencia electrónica de datos); y porque tales aparatos y tales técnicas han supuesto cambios revolucionarios en la manera de entender las relaciones jurídicas tradicionales.”[\[34\]](#)

1.4 Los Sujetos en la Red

1.4.1 Cinco Categorías

Concordamos con DE MIGUEL[\[35\]](#) cuando establece cinco categorías para diferenciar a los sujetos en la Red, las mismas que se detallan a continuación.

- a. Los Operadores de telecomunicaciones, quienes disponen de la infraestructura que permite la transmisión de datos.[\[36\]](#)
- b. Los proveedores de acceso a Internet. Quienes proporcionan el servicio de conexión a la Red.[\[37\]](#)

- c. Los proveedores de servicios de Internet. Servicios que son ofrecidos como el buzón de correo electrónico, elaboración de páginas web[38], etc.
- d. Los suministradores de servicios en línea y suministradores de contenido. Los primeros proporcionan información a los abonados a sus sistemas, mientras que los segundos son los titulares de la información y los datos que constituyen los contenidos, normalmente de las páginas web.
- e. Los usuarios, que en un primer momento consistían en un grupo de personas homogéneas -personas que poseían alto cocimiento informático- sin embargo, la heterogeneidad es la principal característica hoy en día entre los usuarios.

Como se puede apreciar de la clasificación descrita, existe una relación de dependencia entre los sujetos que intervienen en la red, los mismos que forman parte de un gran engranaje que hace posible la comunicación y la obtención de información entre los usuarios. Afirmamos esto debido a que la falta de alguno de los sujetos descritos haría imposible la configuración de la red.

Podemos advertir que en estas cinco categorías se ha configurado el mercado en la red, sin embargo, debemos señalar que no se trata de un numerus clausus, ya que la constante y vertiginosa evolución de los sistemas informáticos harán que en un breve plazo sean integrados nuevos sujetos en la red.

Por otra parte, la precisión de los sujetos en la red no sólo es una cuestión de identificación, porque, además, permite atribuir determinadas competencias a los autores en la red y así atribuir responsabilidades, inclusive penales.

1.5 Necesidad de Regulación de Internet

1.5.1 Origen de Internet

Es preciso señalar la diferencia existente entre la Red y la Web. La primera, es una red de redes, básicamente hecho de PC's y cables que envían paquetes de datos a cualquier parte del mundo. El WWW. (world wide web) cuya traducción literaria es "mundo ancho telaraña" es abstracto (imaginario) un espacio de información, en donde las conexiones son uniones entre hipertextos. En la Web se encuentran documentos, sonidos, videos, información. La Web no podría existir sin la red y hace la red útil, ambos conceptos web y red definen al Internet.

Internet se inició en 1967 a raíz del diseño de la Red ARPANET -Agencia para el Desarrollo de Proyectos de Investigación Avanzada- del Departamento de Defensa de los EE.UU. Dicha red unía universidades y redes de ordenadores de titularidad militar, contratistas de defensa y laboratorios universitarios que realizaban investigaciones militares. Esta red permitió, posteriormente, a los investigadores de todo Estados Unidos acceder directamente a los ordenadores de gran potencia que se localizaban únicamente en algunas universidades y laboratorios. [39]

Para LLANEZA GONZÁLEZ[40], "Internet es un sistema, que no un medio, de comunicación transnacional que, gracias a unos estándares comunes y usando tecnologías y redes de telecomunicación, permite el intercambio y la obtención de información mediante el uso de diversas modalidades de comunicación en línea (listas de correo, grupos de discusión de Usenet, FTP, WWW, chats, etc.). Internet es información, tecnología y una red física de telecomunicación." Para los efectos de una eficaz comunicación, cada computadora debe estar comunicada a Internet. Esta red universal debe tener una identificación única.[41]

Internet se muestra como un medio universal de comunicación y búsqueda de información a muy bajo costo. “Se compone por un conjunto de redes interconectadas que permiten la comunicación entre millones de usuarios de todo el mundo, generando un inmenso grupo de recursos de información, en forma de imágenes, texto, gráficos y sonido”.[\[42\]](#) Sin duda, Internet ha sido creada para el libre acceso a la información global.

Internet es identificada por la mayor parte de usuarios como la gran autopista de la información.[\[43\]](#) Así, la eficaz intermediación de Internet posibilita reconducir los incontenibles flujos de información y contribuye a que la “sociedad de la información”[\[44\]](#) pueda efectivamente transformarse en “sociedad del conocimiento”, como consecuencia de la posibilidad de extraer conocimientos útiles de la sobreabundancia de información.[\[45\]](#)

Sin embargo, a partir de 1990, por la afluencia comercial de Internet, comienza la preocupación principal por la seguridad[\[46\]](#) y es que hay que recordar que ninguna entidad académica, empresarial, gubernamental o de cualquier otro tipo administra Internet. [\[47\]](#)

1.5.2 Contenidos Ilegales en Internet

Los contenidos ilegales en la Red son el problema más difícil de atacar por parte de los países. El acceso libre a contenidos ilícitos en Internet se ha convertido en uno de los problemas fundamentales de los estados a la hora de regular su uso. Todos los países coinciden con la necesidad de fomentar el desarrollo de Internet y las nuevas tecnologías, y generalizar su uso para el comercio y las comunicaciones. Pero una de las primeras alarmas que surgen en este proceso es cómo hacer compatible ese desarrollo con el aumento exorbitante de los contenidos de pornografía, armas, racismo o drogas ilegales.[\[48\]](#) No es tan cierto que Internet sea un territorio no regulado. Por un lado, “existen normas sencillas de carácter formalista, expresadas para un uso más rápido y eficaz en la red.” [\[49\]](#)

Se tratan de normas de cortesía[\[50\]](#), relativas, por ejemplo, a cómo debe emplearse el lenguaje en la red, a la extensión y número que deben tener los mensajes de correo electrónico, etc. Para cierta doctrina, llegan a ejercer una verdadera coerción social en el ámbito de la red. Sin querer abordar con profundidad el ámbito de las normas de cortesía conocidas también como las “*netiquettes*”[\[51\]](#), se considera que éstas, devienen en pautas de comportamiento eficaces y generalmente respetadas.

Sin embargo, la otra cara de la moneda nos muestra que son muy pocas las personas que consideran este tipo de normas, máxime cuando en la red –como hemos visto- prevalece el anonimato de los individuos, por lo que se podría llegar a decir que la educación cibernética aún se encuentra en forma incipiente; se cuestiona, precisamente, que dadas las características de Internet, estas normas ejerzan una real y verdadera coerción entre los usuarios en la Red.

Los usos asociados a Internet requieren de instituciones jurídicas tradicionales que se adecuen para dar solución a aquellas conductas antisociales[\[52\]](#) que se producen en la red, así como la creación de nuevas instituciones jurídicas que tutelén estos casos. Sin embargo, para este planteamiento es necesario considerar el principio de “universalidad” que rige en Internet, considerando así una regulación internacional. Ahora bien, el explosivo crecimiento de Internet como medio comercial impone nuevos desafíos en el Derecho penal, por ello resulta necesaria la determinación de las conductas atentatorias a la red que puedan y deban ser comprendidas en una regulación jurídico penal.

En nuestra opinión, respecto de si se deben controlar o no los contenidos que proporciona Internet, pensamos que desde el momento en que se comprueba que se están cometiendo conductas antisociales a través de la red, es innegable la necesidad de una debida regulación. Sin embargo, esta regulación no debe perder de vista el objetivo por el que se creó Internet, compartir

información, conocimientos, ideas, etc.

Así, somos de la opinión que se debe crear una instancia previa a la penal, en donde se regule las actividades ilícitas en la red y en los sistemas informáticos y se establezca qué conductas están permitidas y cuáles constituyen un daño tanto para los individuos como para los sistemas informáticos, como por ejemplo, el envío de publicidad no deseada, más conocido como el spamming y aquellas conductas atentatorias a la red, pero que no llegan a constituir la comisión de un delito. De esta manera, se crearía una Institución con leyes y normas propias que regulen las actividades en la red, todo ello con la finalidad de poder distinguir cuantitativa y cualitativamente las actividades ilícitas con significación jurídico penal de aquellas que seguirán sólo una regulación administrativa.

1.5.3 La Free Net

A pesar de lo señalado en los apartados precedentes, pareciera ser que cualquier intento de regulación y limitación de determinadas actividades antisociales en la red se verá –en un futuro- truncado, ya que se encuentra en proyecto la “Free Net”. La aplicación “Free Net” ha sido diseñada precisamente con la intención de impedir cualquier control para los mensajes o informaciones que se expiden desde cualquier punto que aplique tal tecnología.

El uso de la multipolaridad de Internet consigue que los mensajes se copien y multipliquen instantáneamente al salir del servidor, de modo que quedan automáticamente a disposición de todos los ordenadores conectados a la red. Mediante este proyecto, se puede acceder a una red muy similar a Internet, sin embargo, los puntos que diferencian a “Free Net” constituyen una bomba de tiempo para el Derecho penal. Mediante este sistema, la información es almacenada en los ordenadores de las personas conectadas. [\[53\]](#)

Así, no sólo se estaría compartiendo información como en el modelo tradicional, sino que sería imposible el censurar o eliminar publicaciones, ya que se desconocería dónde está almacenada dicha información debido a que las conexiones se harían de forma anónima siendo mucho más sencillo acceder a la información más demandada, ya que ésta se duplica a medida que se va desplegando por la red. [\[54\]](#)

Esperamos que el mencionado proyecto no llegue a su realización, ya que de lo contrario, podría existir una red privada internacional de delincuentes de todos los niveles, delincuentes que serían inubicables como autores de diversos delitos informáticos, los mismos que gozarían de impunidad bajo la protección de la red privada “Free Net”.

1.5.4 Amenazas en Internet

Mientras uno navega por Internet, existen todo tipo de amenazas que se pueden originar por malos usuarios. Las amenazas en Internet están latentes para el individuo que ingresa diariamente a este amplio mundo de información como es Internet.

En el lenguaje informático se denomina “amenaza” a la violación de la seguridad (confidencialidad, integridad, disponibilidad o uso legítimo) que podría efectuar una persona, máquina, suceso o idea, dada una oportunidad. Un ataque no es más que la realización de una amenaza. [\[55\]](#)

Según el Instituto Nacional de Estadística e Informática, existen cuatro categorías generales de amenazas o ataques, son las siguientes:

- a. Interrupción: Es un ataque contra un recurso del sistema que es destruido o deshabilitado temporalmente. [\[56\]](#)
- b. Interceptación: Este es un ataque de una entidad que consigue acceso a un recurso no autorizado. Dicha entidad podría ser una persona, un programa o una computadora. [\[57\]](#)
- c. Modificación: Este es un ataque de una entidad no autorizada que consigue acceder a un recurso y es capaz de modificarlo. [\[58\]](#)
- d. Fabricación: Este es un ataque de una entidad no autorizada que añade mensajes, archivos u otros objetos extraños en el sistema. [\[59\]](#)

Asimismo, existe diferencias entre ataques pasivos y ataques activos en Internet. En los ataques pasivos el atacante no altera la comunicación, sino que únicamente la observa, con el fin de obtener la información que está siendo transmitida. Sus objetivos son la interceptación de datos y el análisis de tráfico, una técnica más sutil para obtener información de la comunicación puede consistir en:

- a. Obtención del origen y destinatario de la comunicación, leyendo las cabeceras de los mensajes interceptados.
- b. Control del volumen de tráfico intercambiado entre las entidades interceptadas, obteniendo así información acerca de actividad o la inactividad inusuales.
- c. Control de las horas habituales de intercambio de datos entre las entidades de comunicación, para extraer información acerca de los períodos de actividad.

Cabe señalar, que al igual que los sujetos en la red, los ataques tanto activos como pasivos, no constituyen de ninguna manera numerus clausus para la configuración de las amenazas, ya que cada día se originan nuevos tipos de ataques y/o amenazas para los sujetos que ingresan a Internet.

Los ataques pasivos son muy difíciles de detectar, ya que no provocan ninguna alteración de los datos. Sin embargo, es posible evitar su éxito mediante el cifrado de la información y otros mecanismos de seguridad de la información.

Los ataques activos implican algún tipo de modificación en el proceso de transmisión de información a través de la red o a creación de un falso proceso de transmisión, pudiendo subdividirse en cuatro categorías:

- a. Suplantación de identidad: el intruso se hace pasar por una entidad diferente. Normalmente incluye alguna de las otras formas de ataque activo. [\[60\]](#)
- b. Reactuación: uno o varios mensajes legítimos son capturados y repetidos para producir un efecto no deseado. [\[61\]](#)

c. Modificación de mensajes: una porción del mensaje legítimo es alterada, o los mensajes son retardados o reordenados, para producir un efecto no autorizado. [62]

d. Degradación Fraudulenta del servicio: impide o inhibe el uso normal o la gestión de recursos informáticos y de comunicaciones. [63]

Pareciera ser, como se ha podido apreciar de las conductas descritas, que Internet no ha sido diseñado para ser seguro, la inexistencia de fronteras presenta ciertos riesgos tanto para los usuarios como para los servidores.

“La pretendida sustitución de los límites territoriales (y materiales) por nuevas fronteras propias de Internet, junto con la independencia atribuida a las redes en su funcionamiento y su supuesta transformación en comunidades con poder para imponer sus propias reglas, son elementos que se encuentran en el origen de uno de los planteamientos básicos en lo que respecta al régimen jurídico en Internet.” [64]

Por lo expuesto, concluimos el presente punto señalando que la necesidad de una regulación de Internet es urgente no sólo por el hecho que las normas de cortesía no producen un efecto coercitivo o por las amenazas latentes tanto pasivas como activas que se pueden generar en la red, sino especialmente por el hecho que es necesaria la creación de una institución que regule las conductas que no están permitidas en la red para que de esta manera, se lleve a cabo un buen funcionamiento entre los sujetos que utilizan este amplio campo de la información.

Sólo a través de la regulación de la red en una instancia previa a la penal, podrá orientarse a los usuarios sobre el correcto uso y funcionamiento de la misma, podrá delimitarse las conductas que son permitidas de aquellas que son prohibidas y, luego, definirse aquellas que requieren de una regulación jurídico-penal.

Por último, debemos advertir que para la definición de las formas de intervención sobre aquellas conductas nocivas en la red, resulta necesario la previa determinación del objeto jurídico de protección, de ello nos ocuparemos en el primer capítulo de la segunda parte de la presente investigación.

Capitulo II

Algunas precisiones acerca de la criminalidad informática como nueva forma de criminalidad

LA CRIMINALIDAD INFORMÁTICA

1.1. Aspectos generales de la criminalidad informática

Las líneas de este subcapítulo obedecen a la preocupación constante por las recientes formas de criminalidad que han sido tratadas por la dogmática penal tanto en artículos en revistas, como en diversos congresos sobre la novedosa forma de criminalidad, denominada “criminalidad informática”.

Mucho se habla de los grandes beneficios que los medios de comunicación y el uso de la informática han aportado a la sociedad actual, sin embargo, el desarrollo tan amplio de la tecnología informática ofrece también un aspecto negativo, ya que se han generado nuevas conductas antisociales que se manifiestan en formas que no era posible imaginar en el siglo pasado. Los sistemas de computadoras ofrecen oportunidades nuevas y muy complicadas de infringir la ley y han creado la posibilidad de cometer delitos tradicionales en formas no tan tradicionales.[\[65\]](#)

El comercio en la Red es un lugar muy apetecible para que personas sin escrúpulos o criminales con acceso a nuevas tecnologías, puedan acceder a sistemas remotos y cometer robos electrónicos al detectar puertas traseras en los sistemas de las empresas[\[66\]](#). Por este motivo es importante que las naciones tomen medidas más concretas en esta materia para evitar llegar a un caos legalmente reconocido.

La enorme evolución de la informática ha transformado al mundo en una gran tecnología, la cual nos facilita el quehacer diario y la eficacia de nuestro trabajo, sin embargo, así como ha transformado al mundo, la tecnología también ha transformado las antiguas conductas delictuales en los ahora llamados “delitos informáticos”. A modo de ejemplo[\[67\]](#), las empresas que sufrieron de ataques cibernéticos (últimamente) fueron, entre otras, el portal de Internet Yahoo, la tienda minorista Amazon.com, el lugar de subastas Ebay, la tienda de descuentos Buy.com, la cadena CNN interactive [\[68\]](#) y ZDNet, la piratería informática[\[69\]](#) provoca en Europa unas pérdidas de 3,705 millones de dólares, la progresiva implantación de las nuevas tecnologías en todos los ámbitos de la denominada sociedad de la información ha disparado el uso ilegal de aplicaciones de software en todo el mundo[\[70\]](#), en 1999 se hicieron famosos los virus[\[71\]](#) Melissa[\[72\]](#), Chernovyl, Explore Zip, Babylonia y Bubleboy; en el año 2000 el virus ILOVEYOU conmovió al mundo entero causando daños, en algunos casos, irreparables[\[73\]](#), los fraudes en Internet aumentaron significativamente en el año 2000 y representaron dos tercios del total de casos presentados en el Servicio de Crímenes Comerciales de la Cámara de Comercio Internacional (ICC). Según el informe, 2 mil 776 de los 4 mil 139 casos referidos por sus miembros estuvieron directamente relacionados al crimen, fraude y falsificación a través de sitios web que ofrecen mercancía o servicios falsos, dicha encuesta mostró que en el año 2000, esta oficina salvó a sus miembros de pérdidas de alrededor de 2 millones 300 mil dólares, advirtiéndoles acerca de las negociaciones con esta nueva generación de criminales que habían sido previamente investigados"[\[74\]](#). Noticias como éstas son temas tratados todos los días en los medios de comunicación.

Es innegable, que el uso de las nuevas tecnologías conduce a la ampliación y creación de nuevos delitos en todas las partes del mundo.

Es por conductas que son producto del desarrollo tecnológico que se dice que el moderno Derecho penal necesita asumir y afrontar los nuevos conceptos y estrategias de la criminalidad, sobre todo en conexión con nuevos fenómenos o formas delictivas.[\[75\]](#)

Por “criminalidad informática” se pueden señalar conductas tales como la burla a los sistemas de dispositivos de seguridad, tanto en cajeros automáticos, como en máquinas tragamonedas, manipulaciones técnicas en el sistema de televisión pagado, invasiones a computadoras, correos o sistemas mediante una clave de acceso, revelación de secretos por parte del personal de la institución bancaria, fraudes en la telefonía celular móvil, conductas antisociales de personas que ingresan a sistemas no autorizados, sustracción de información, envío de mensajes falsos, hasta la alteración de datos que provocan cada vez más pérdidas de miles de millones de dólares cada año.

BAÓN RAMÍREZ[\[76\]](#) define a la criminalidad informática como la realización de un tipo de actividades que, reuniendo los requisitos que delimitan el concepto de delito, sean llevados a cabo utilizando un elemento informático (mero instrumento del crimen) o vulnerando los derechos del titular de un elemento informático, ya sea hardware o software.

Para TIEDEMANN[77] la expresión "criminalidad mediante computadoras" alude a todos los actos antijurídicos, según la ley penal vigente, realizados con el empleo de un equipo automático de procesamiento de datos.

Como se puede desprender de lo anteriormente dicho, la utilización de computadoras en la economía, industria y, sobre todo, en el sector de bancos y seguros, genera también la aparición de nuevas formas de conductas delictivas[78] que pronostican[79] desde ya, el origen de una criminalidad informática transnacional.[80] En consecuencia, la interconexión global posibilitada por el Internet trae consigo, una nueva calidad de criminalidad que afecta numerosos ámbitos de la vida y la economía.

Es preciso señalar que el concepto de "criminalidad informática transnacional" no se deberá de confundir con el término "criminalidad organizada." [81] [82] Como hemos explicado, la criminalidad informática será transnacional cuando las conductas delictuales traspasen las fronteras de los países.

Por "criminalidad organizada", nos unimos a la definición que establece la UNION EUROPEA[83] que la define según 11 requisitos, de los cuales como mínimo han de concurrir 6, en los siguientes términos:

1. Más de dos personas.
2. Distribución entre más de dos personas.
3. Permanencia.
4. Control interno.
5. Sospechosas de la comisión de un delito grave.
6. Actividad internacional.
7. Violencia.
8. Uso de estructuras comerciales o de negocios.
9. Blanqueo de dinero.
10. Presión sobre el poder público.
11. Ánimo de lucro.

Por otro lado, como observa TIEDEMANN[84], es difícil para el criminólogo obtener un panorama confiable sobre las manipulaciones informáticas reales y potenciales en Alemania y en el extranjero, porque son raros los procesos penales debido a las razones conocidas de la "limpieza" interna de abusos y en vista a la pérdida de imagen temida especialmente por las víctimas con carácter de Institución.[85]

En una sociedad caracterizada por el ansia de poder, éste se consigue precisamente a través de la información. Por tanto, los sistemas informáticos no sólo acrecientan el poder de quien posee más información, sino que contribuyen a la batalla por el dominio de esta información. Los sistemas para la prevención del crimen, sus métodos de detección, procesamientos, etc., varían mucho en función del país y así, acciones que en un país se consideran legales, pueden ser consideradas ilegales en otro.

Por este motivo, el crecimiento del comercio en la Red introduce dos retos para tratar el crimen cibernético:

- a. Determinar exactamente en qué lugar se está realizando el delito.
- b. El problema de localizar al sospechoso.

Actualmente hay escasos acuerdos internacionales que permiten a las diferentes policías y diferentes países compartir información, más allá de los tratados de extradición para criminales detenidos en terceros países.

Ahora bien, así como vemos la necesidad de regulación de las conductas que se originan por el avance tecnológico, no debemos perder de vista que al ser reguladas, también debemos de recordar el principio de ultima ratio que le asiste al Derecho Penal. [\[86\]](#)

1.2 Conductas nocivas que se cometen a través de sistemas informáticos y de Internet

Existen dos posiciones respecto de las conductas que originan el “delito informático”. La primera comprende conductas cuya única característica especial radica en el empleo de una computadora.[\[87\]](#) La segunda posición consiste en toda conducta ilegal que requiere del conocimiento de la tecnología informática para su perpetración, investigación y prosecución, de tal forma que el empleo mismo del medio informático le permita su diferenciación respecto de un delito común que utilice como medio de comisión la computadora. Sin embargo, ha de tenerse en cuenta que las nuevas técnicas informáticas no son simplemente el instrumento para la comisión de un delito, sino que en muchas ocasiones son el mismo objeto de la conducta delictiva.[\[88\]](#)

Nos parece necesario señalar algunas de las conductas más comunes que se cometen a través de los sistemas informáticos y de Internet[\[89\]](#), sin embargo esta clasificación es una simple enumeración de las conductas cometidas por los delincuentes informáticos en los últimos años, por lo que no se deberá pensar que constituyen la totalidad de conductas nocivas e ilícitas existentes.

1.2.1 Introducción de datos falsos o “Data Diddling”

Consiste en manipular las transacciones de entrada al computador con el fin de ingresar movimientos falsos total o parcialmente, o eliminar transacciones verdaderas que deberían haberse introducido.

Es un método al alcance de muchas personas que desarrollan tareas en los servicios informáticos para lo cual no es necesario poseer conocimientos técnicos especiales sino tan sólo haber percibido las deficiencias de control que muestre un determinado sistema.[\[90\]](#)

Se trata de una manipulación de los sistemas o programas informáticos, cuya alteración genera información distorsionada que puede tener incidencia económica y causar un perjuicio patrimonial, de ahí que pueda ser considerada como una conducta fraudulenta.

1.2.2 El Caballo de Troya o “Trojan Horse”[\[91\]](#)

Atendiendo a su denominación, podemos precisar que este método consiste en la inclusión de instrucciones dentro del programa de uso habitual de una rutina para que realice un conjunto de funciones, desde luego no autorizadas, para que dicho programa ejecute en ciertos casos de una forma distinta a como estaba previsto. Puede tratarse en determinados casos de la ejecución de cálculos erróneos, por ejemplo, aumentando el importe de la lista de un empleado, desviando ingresos hacia cuentas ficticias, etc. También puede presentarse cuando se imprimen documentos no autorizados o inclusive no imprimir

documentos reales, por ejemplo, emitir cheques a proveedores reales cuando previamente se les ha cancelado su deuda, ya que se ha alterado la forma de pago transfiriendo los fondos a una cuenta que pertenece al defraudador.[\[92\]](#)

Por sus características es necesario que el agente posea una capacidad técnica suficiente, al menos saber programar y, además, tener acceso al programa para poder manipularlo. Es importante agregar que en todo este tipo de ilícitos el programa manipulado ha estado en funcionamiento habitual desde hace un buen tiempo y casi nunca se trataba de un programa de nueva creación.

El motivo es muy simple, los programas nuevos suelen ser sometidos a procesos de revisión y chequeo para detectar cualquier anomalía que puedan afectarlos.

Sin embargo, un programa que ha estado en funcionamiento correctamente durante un prolongado tiempo no es cuestionado, y salvo casos absolutamente excepcionales, jamás sus resultados son sometidos a comprobación. Debido a ello la modalidad del Caballo de Troya es una de las más peligrosas formas delictivas y al mismo tiempo difícil de detectar.[\[93\]](#)

Al igual que la conducta anterior, se trata de una manipulación fraudulenta de los sistemas o programas informáticos generalmente practicados con fines económicos.

1.2.3 El Salame, Redondeo de Cuentas o “Rounding Down”

Es tal vez la técnica más sencilla de realizar y la que menos probabilidades tiene de ser descubierta.

La modalidad consiste en introducir o modificar unas pocas instrucciones de los programas para reducir sistemáticamente una cantidad de dinero transfiriéndola a una cuenta distinta o proveedor ficticio que se abre con nombre supuesto y que obviamente la controla el defraudador.

Por ejemplo, puede darse el caso de disminuir constantemente en unos céntimos las cuentas corrientes de un cliente bancario, pequeños saldos de proveedores, reducir los talones de impresión para el pago a acreedores, transfiriendo luego estas pequeñas cantidades a la cuenta particular del autor.

También se suele aplicar esta modalidad cuando se calculan los intereses de cuentas corrientes bancarias, de libretas de ahorro, de depósitos a plazo o bien cuando se elabora el cálculo de la planilla de los trabajadores de una empresa, procediéndose a eliminar el criterio generalizado de redondeo de céntimos a la alza o a la baja de dinero en montos exactos y a cambiarlo por la eliminación total de dichos céntimos que son transferidos a una determinada cuenta o a nombre de un empleado real o ficticio.

La razón principal por la que es tan difícil descubrir este tipo de hechos es porque las cuentas o el importe total del listado, siguen estando “cuadrados” o contablemente equilibrados en el arqueo de caja por lo que no se deduce ninguna señal de alarma que pueda indicar lo que está sucediendo. Por ejemplo, se da el caso al redondear cuentas bancarias y acreditar los montos resultantes a una cuenta determinada repitiendo automáticamente la operación sin intervención posterior del autor.[\[94\]](#)

La finalidad económica de la conducta fraudulenta se torna evidente en el presente caso, de ahí que se trate de otra de las formas de manipulación informática con incidencia patrimonial.

1.2.4 Uso Indebido de Programas o “Superzapping”

Es el uso no autorizado de un programa de utilidad para alterar, borrar, copiar, insertar o utilizar cualquier forma no permitida, los datos almacenados en el computador o en los soportes magnéticos.

El nombre proviene de un programa llamado “*Superzap*” y es una especie de llave que permite abrir cualquier rincón de una computadora por más protegida que pueda estar. Estos programas pertenecen al grupo de los llamados “Programas de Acceso Universal” de uso imprescindible en cualquier instalación de ciertas dimensiones cuando fallan los procedimientos normales para recuperar o reiniciar “el sistema”.

Efectivamente, cuando un sistema informático almacena gran cantidad de información se hace necesario disponer de un mecanismo de emergencia que permita entrar a cualquier punto del sistema en caso que se produzca alguna avería o lo que normalmente se ha denominado “caída del sistema”.

Es por esta razón que se justifica la existencia de los llamados “Programas de Acceso Universal” (PAU); herramientas imprescindibles en cualquier instalación de ciertas proporciones cuando fallan los procedimientos normales para “recuperar” o “reiniciar” el sistema.

Los programas de utilidad son una herramienta valiosa y muchas veces imprescindible en los casos de caída del sistema pero igualmente un arma peligrosísima cuando se encuentra al alcance de personas que lo utilizarán con otras intenciones.

No obstante, suelen estar archivados en las librerías de producción junto con el resto de programas de uso común y generalizado, con lo cual cualquier técnica podría tener la posibilidad de utilizarlo indebidamente.

Con la modalidad de “*superzapping*” es posible alterar los registros de un fichero sin que quede constancia de tal modificación, lo cual hace sumamente difícil descubrir y detectar al autor de tales eventos. Aparentemente se suelen registrar los ingresos a un sistema y las transacciones que se han procesado en una determinada operación actualizando los registros con un dato específico como, por ejemplo, la hora de ingreso.

Sin embargo, los programas de acceso universal permiten modificar directamente la información sin activar los programas de actualización ni introducir ninguna operación al computador. Aún más, sin dejar rastro si la persona que lo está usando sabe como realizarlo. Bastaría con hacer coincidir el monto de la modificación no autorizada con el comienzo o el final de la ejecución del programa verdadero de actualización y algún error intencionado en el sistema que requiera la utilización del programa de acceso universal. En ese preciso momento tendremos cargado en el sistema el fichero que queremos modificar y el programa que nos permite modificar, no registrándose por lo tanto su utilización no justificada ni del fichero, ni del programa de utilidad. Cuando se descubran las alteraciones de los datos se pensará que ha sido un funcionamiento erróneo del programa de actualización, un funcionamiento inadecuado del computador o una transacción errónea y en esas direcciones se encaminará la investigación, las cuales seguramente no abordarán a ningún puerto. En el mejor de los casos, si se descubre como se realizó la alteración de datos, será muy difícil probarlo. [\[95\]](#)

En definitiva, la técnica del “superzapping” representa una forma de acceso a sistemas o programas informáticos que puede o no estar autorizado por un titular, lo cual incide en la licitud o no de la conducta, dicho acceso puede orientarse a cuestiones económicas o al conocimiento de información o datos reservados, por lo que puede tener una incidencia patrimonial como también para la intimidad.

1.2.5 Puertas falsas o “Traps Doors”

Es una costumbre en el desarrollo de aplicaciones complejas que los programas permitan introducir interrupciones en la lógica de los desarrollos del mismo, con el objeto de chequear por medio de los procesos informáticos si los resultados intermedios son correctos, producir salidas de emergencia y de control a fin de guardar resultados parciales en ciertas áreas del sistema para comprobarlos después. Inclusive algunas veces este procedimiento se enlaza con rutinas del sistema operativo para facilitar una “puerta entrada al programa” que no estaba prevista, pero de esta manera facilitan la labor de desarrollo y prueba de programas.

El problema radica en tener la seguridad de que cuando los programas entran en proceso de producción normal, todas esas “puertas falsas” hayan desaparecido.

Y aunque parezca mentira, las puertas creadas no se eliminan, permitiendo a su paso puertas de acceso al programa con el agravante que por ser elementos temporales creados por la computadora no constan en la documentación del sistema.

Es de uso frecuente para posibles recuperaciones en caso de “caída del sistema” a mitad de un proceso, ir grabando en cinta resultados intermedios o copia de las transacciones procesadas, o incluso ciertas áreas de memoria para la recuperación más rápida y sencilla. Las puertas falsas son: por personas que no las crearon, pero que una vez descubiertas se aprovechan de ella sin necesidad de poseer una formación informática profunda.[\[96\]](#)

Estas técnicas inciden en la forma de acceso a los sistemas o programas informáticos, por lo que tendrá relación en cuanto se trata de un ingreso no autorizado. En tal virtud, es una conducta antesala a aquellas vinculadas a fraudes o sabotajes informáticos.

1.2.6 Bombas Lógicas o “Logic Bombs”

Previamente debe señalarse que este tipo de delito se ejecuta para producir daños sin otro beneficio que el placer de perjudicar.

El método consiste en introducir en un programa un conjunto de instrucciones no autorizadas para que en una fecha o circunstancia predeterminada se ejecuten automáticamente desencadenando el borrado o la destrucción de información almacenada en el computador, distorsionando el funcionamiento del sistema o produciendo paralizaciones intermitentes.[\[97\]](#)

Esta modalidad es una forma bastante extendida, utilizada por muchos fabricantes de paquetes de software con el fin de asegurar el importe de los mismos[\[98\]](#).

Consiste en programar una instrucción que revisa la fecha del día, lo que permite una fecha de caducidad oculta que ha introducido el fabricante del software al instalarlo en el computador del cliente y que no será eliminada o prorrogada hasta que el cliente pague los nuevos derechos.

Esto constituye una verdadera forma de coacción ilegal, pero que es utilizada por una falta de protección adecuada de los derechos de autor y los derechos del consumidor o usuario. Esta conducta es denominada comúnmente como daños o sabotaje informático.

1.2.7 Ataques Asincrónicos o “Asynchronous Attacks”

Los sistemas informáticos en la mayoría de los casos funcionan ejecutando más de dos comandos u órdenes a la vez o en otras circunstancias una instrucción sucesiva de la otra en forma secuencial. Cabe recordar que el sistema operativo es el conjunto de programas que controlan el funcionamiento del computador y todos sus dispositivos periféricos (discos, cintas, impresoras), la entrada de los datos procesados por el programa, la ejecución de los programas de las diferentes aplicaciones y la salida de la información elaborada hacia los dispositivos exteriores.

El sistema operativo es imprescindible para el funcionamiento del equipo y su desarrollo es responsabilidad del fabricante. Una de las principales funciones del sistema operativo de las computadoras es controlar la ejecución simultánea de varios programas a la vez. Otra función fundamental del sistema operativo es optimizar la ocupación de memoria central reasignando áreas en función de las necesidades de cada uno en los programas que están ejecutando en cada momento.

De otro lado el sistema operativo asigna a los programas otras funciones de clasificación, intercambio, etc. Por lo tanto, el sistema operativo es quien controla y maneja todos los errores que pueden producirse tanto en la computadora como en los programas que se están ejecutando, avisando al operador por medio de mensajes de cualquier situación anormal que se produzca.

Pues bien, los programas funcionan en forma sincrónica, es decir, ejecutando sus instrucciones en un orden fijo predeterminado de nivel en nivel, en tanto que el sistema operativo funciona en forma asincrónica, es decir, ejecutando sus órdenes de manera independiente, en función de una gran cantidad de factores ajenos a él.

Como consecuencia, se produce rigurosidad en los programas en ejecución conformando las llamadas “colas de espera” que se van a ir desbloqueando en función de la disponibilidad de los datos o comandos que estaban esperando.

Uno de los típicos casos es el que puede producirse en los llamados puntos de recuperación del sistema. Cuando se procesan programas complejos y de larga duración se establecen puntos de recuperación cada cinco o diez minutos, por ejemplo, gravando en soporte magnético externo (diskettes) el estado del programa, lo que implica que si el sistema “se cae”, es decir, que se interrumpa el proceso por una situación de error no recuperable, por ejemplo, falta de energía eléctrica, no es necesario retroceder desde el principio del programa sino bastará hacerlo desde el último punto de recuperación ya que todo se encuentra gravado, reiniciando de esta manera el proceso.

Pues bien, si entre dos puntos de recuperación se provoca voluntariamente una “caída del sistema” y en el intermedio se manipula los parámetros en que se va a apoyar el sistema operativo, para reiniciar resulta obvio que las condiciones en que se ejecuten serán distintas a las originales por lo que sus resultados serán por lo menos diferentes, fraudulentos o erróneos.

Se trata de una conducta de sabotaje informático que puede orientarse hacia la obtención de un provecho económico para el agente o un tercero, o hacia la causación de daños de los sistemas o programas informáticos.

1.2.8 Recojo de Información Residual o “Scavenging”

Este procedimiento se basa en aprovechar los descuidos de los usuarios ya que la información ha sido abandonada sin ninguna protección como residuo de un trabajo real efectuado con la debida autorización.

La denominación proviene del anglicismo “*to scavenge*” que significa recoger la basura. Simplemente se va aprovechando las finalizaciones de los trabajos reales en el computador para obtener la información residual que ha quedado en la memoria.

La modalidad más frecuente es la “impresión diferida”, la cual prepara la unidad para que posteriormente imprima sin ningún tipo de protección siendo fácilmente recuperable sin necesidad de utilizar ninguna clave de acceso.

Tiene dos formas bien definidas: *scavenging* físico y *scavenging* electrónico.

- a. **El Scavenging Físico:** Consiste en recoger el material de desecho que se abandona en las papeleras, encima de las mesas, en el suelo, etc., y que frecuentemente incluye listados de pruebas de programas, documentos conteniendo información de entrada a un programa a la computadora, a copias de apoyo que no han sido repartidas, etc.
- b. **El Scavenging Electrónico:** Consiste en aprovechar las finalizaciones de las ejecuciones de los programas realizados en el computador para obtener la información residual que ha quedado en la memoria o en los soportes magnéticos.

Una de las formas más simples del *scavenging* electrónico es cuando se ordena la impresión diferida, ya que en la computadora queda preparada la información que posteriormente se imprimirá sin ningún tipo de protección, siendo sumamente fácil recuperar la información sin la necesidad de utilizar ningún tipo de clave o cualquier procedimiento de seguridad. [99]

Se trata de una técnica para obtener información sin autorización. Por tanto, lo importante en estos casos será el contenido de la información.

1.2.9 Divulgación No Autorizada de Datos o “Data Leakage”

Consiste en sustraer información confidencial almacenada en un computador central desde un punto remoto, accediendo a ella, recuperándola y finalmente enviándola a una unidad de computador personal, copiándola simultáneamente. La sustracción de información confidencial es quizás uno de los cánceres que con mayor peligro acechan a los grandes sistemas informáticos.

Se ha empleado también bajo la denominación de espionaje industrial, pues sería particularmente débiles al sustraerse aspectos claves de su actividad empresarial, como, por ejemplo, estrategias de mercado, nuevos productos, fórmulas de producción, etc. Inclusive hay cierto tipo de empresas que dependen de la privacidad de su información como las empresas de publicidad directa en donde tiene ficheros completos de su público objetivo.

1.2.10 Acceso a Áreas No Autorizadas o “Piggyn Baking”

Pese a no tener una traducción específica consiste en acceder a áreas restringidas dentro de la computadora o de sus dispositivos periféricos como consecuencias de puertas abiertas o dispositivos desconectados.

Se da también cuando el usuario que está trabajando en una terminal en un nivel autorizado que le permite realizar ciertas funciones reservadas deja el terminal conectado, con lo que cualquier otra persona puede continuar trabajando sin necesidad de identificarse pudiendo efectuar operaciones que en condiciones normales no le estarían permitidas.

1.2.11 Suplantación de la Personalidad o “Impersonation”

Puede ser entendida como la suplantación de personalidad, fingiendo ser una persona que no es imitándola e inclusive remedándola. Algunos sistemas requieren la identificación con una clave para acceder al sistema. Más adelante se ha requerido la posesión de algo pudiendo ser una llave o tarjeta magnética. Y aún podríamos complicarlo más si adicionamos dispositivos

de reconocimiento biométrico como identificación con la palma de la mano o dactilográfica, scanners de retina o del iris, reconocimiento de voz, etc.

Un caso muy frecuente de *impersonation* o suplantación de personalidad se da en el robo de las tarjetas de crédito y de cajeros automáticos. Los autores del delito se hacen pasar por empleados de la central de tarjetas de crédito, llamando telefónicamente al titular para solicitarle que con el objeto de anular la posibilidad de utilización fraudulenta de la tarjeta robada le revele su clave secreta o personal.

Como es fácil advertir, una vez descubierta la clave a la persona desconocida que las ha llamado utilizan la tarjeta para sacar el dinero de los cajeros automáticos hasta su límite máximo de crédito.[\[100\]](#)

1.2.12 Interferencia de Líneas Telefónicas o “Wiretapping”

Se trata de interferir líneas de transmisión de datos y recuperar la información que circula en ellas, generalmente se produce en el mismo origen de la transmisión. No es necesario tener equipo sofisticado, sólo se requerirá un pequeño cassette, una grabadora, una radio portátil AM-FM, un Módem para demodular las señales telefónicas analógicas y convertirlas en digitales, y una pequeña impresora para listar la información que se hubiera captado. La forma de realizarlo depende del sujeto que lo ejecuta.

1.2.13 Hurto de Tiempo

Se da cuando los empleados utilizan sin autorización las horas de la máquina del empleador por empleo para realizar trabajos particulares hurtando el tiempo del computador o del servicio de procesamiento de datos y por tanto incrimina un uso no autorizado. Esta conducta es usada mayormente en aquellas empresas que cancelan a sus empleados por las horas trabajadas.

1.2.14 Simulación e Imitación de Modelos o “Simulation and Modeling”

Se trata del uso de la computadora para simular y planificar la comisión de un delito antes de realizarlo. La utilización de la computadora se realiza de forma mediata para conseguir un fin ilícito, como ejemplos podemos señalar desde la simulación del robo de una bóveda de un banco hasta el contador que contrató los servicios contables de una empresa para estudiar detenidamente las repercusiones de los asientos fraudulentos que pensaba realizar para sustraer una cantidad importante de dinero. Aquí se difiere de los anteriores tipos de infracciones informáticas, pues el computador que puede ser usado para simular situaciones previsible o efectuar modelos que representen el comportamiento previsible de una empresa, una fábrica, una inversión, es utilizado equivocadamente con fines delictivos.

1.3 Conductas nocivas e ilícitas según la Organización de las Naciones Unidas

Existen distintas categorías reconocidas por la Organización de las Naciones Unidas -ONU- las mismas que se detallan a continuación:

- a. Fraudes: Cometidos mediante manipulación de computadoras, por ejemplo, colocando datos falsos en un sistema y manipulación de programas.[\[101\]](#)
- b. Falsificación: Por medio de la Informática, de dinero, ticket, etc.
- c. Daños a Datos: Por medio de virus, accesos no autorizados por *hacker* o *cracker*.

Para la Organización de las Naciones Unidas, estas son las conductas más frecuentes que se cometen a través de sistemas informáticos.

1.4 Otras conductas no previstas

Asimismo, existe nuevas conductas delictuales no previstas por las leyes vigentes en algunos países, como:

- a. *Hacking*: Es la conducta de entrar a un sistema sin autorización. Pero la finalidad no es considerada no ilícita.
- b. *Cracking*: Es la conducta de entrar sin autorización a un sistema con el objetivo de destruir la información.
- c. *Phreaking*: Es la actividad de obtener ventajas de las líneas telefónicas a los efectos de no pagar los costos del servicios.
- d. *Carding*: es la actividad de cometer fraude o estafa con los números de las tarjetas de crédito, obtenidas ilegalmente de sitios seguros de las Website, ya sea creándola de la nada o real de un titular. [\[102\]](#)

Desde una apreciación global de las conductas anteriormente descritas, podemos advertir que pueden ser agrupadas en tres grandes rubros: conductas vinculadas al ingreso no autorizado a sistemas informáticos, conductas de manipulación fraudulenta de sistemas informáticos y conductas de sabotaje o daño informático.

Creemos que para poder tipificar los comportamientos descritos anteriormente se debe buscar una normativa internacional homogénea para lograr la persecución de estas conductas, porque el criterio territorialista de nuestro Derecho penal es ineficaz por el problema de la competencia y jurisdicción aplicables.

Segunda Parte

LOS DELITOS INFORMÁTICOS:

MARCO LEGAL

Delimitación conceptual del delito informático

1.1 Concepto de Delito

Para empezar a hablar de delitos informáticos es necesario primero señalar qué entendemos por el término "delito". Etimológicamente la palabra delito procede del latín "*delictum*", que significa abandonar el camino prescrito por la ley. Originariamente significaba la omisión de lo que se debe hacer, en contraposición al acto culpable positivo, la acción, para cuya designación se reservaba el término "*facinus*".[\[103\]](#)

"Ya a finales del siglo XIX, VON LISZT, en su Tratado de Derecho Penal, definía el delito como acto contrario a Derecho, culpable y sancionado con una pena"[\[104\]](#)

A lo largo de la evolución del Derecho penal, ha sido la teoría general del delito la que ha venido ocupándose de las características que debe poseer un hecho para ser considerado delito.

Existen características comunes y diferentes en cuanto a los tipos delictivos. Por eso, la Parte General del Derecho penal, especialmente la teoría general del delito, estudia los tipos delictivos, sus diferencias, etc., con la finalidad de sistematizar los elementos del delito.

Para BRAMONT-ARIAS[\[105\]](#), la teoría general del delito reúne en un sistema los elementos que, en base al Derecho positivo, pueden considerarse comunes a todo delito o grupos de delitos; constituyéndose así la característica central de la dogmática del Derecho penal.

Para MUÑOZ CONDE y GARCÍA ARÁN[\[106\]](#), por "delito" se puede entender como toda conducta que el legislador sanciona con una pena. En nuestro Código penal el concepto de delito está comprendido en el artículo 11 que establece que "Son delitos y faltas las acciones y omisiones dolosas o culposas penadas por la ley."

Las dos formas de conducta (acción u omisión) están colocadas en un plano de igualdad en el Código penal, pero, naturalmente, la ley penal está construida sobre la acción, pues los delitos de omisión son la excepción.

Sin embargo, creemos que no debemos explicar el concepto del delito respecto al Derecho penal positivo, esto es, desde la definición que le otorga nuestro Código penal, sino a partir de la elaboración alcanzada por la dogmática penal en la actualidad. Así, se tiene que el delito posee fundamentalmente tres elementos, la tipicidad, la antijuricidad y la culpabilidad.[\[107\]](#) Los mismos que serán brevemente explicadas.

La tipicidad es entendida como la adecuación de un hecho delictuoso cometido a la descripción que del mismo se recoge en la ley penal. Ésta presenta dos aspectos, por un lado la tipicidad objetiva que comprende estados y procesos que se hallan fuera del dominio interno del autor y que son requeridos por el tipo y la tipicidad subjetiva que comprende estados internos del autor. De ahí que se distinga en la tipicidad un aspecto objetivo referido a los elementos descriptivos y normativos, de un aspecto subjetivo caracterizado por la concurrencia del dolo o la culpa y determinados elementos subjetivos adicionales.

Otro elemento del delito es la antijuricidad, conocida por la doctrina española como “injusto”, a través del cual se afirma que la acción típica no está justificada debido a la valoración que se hace de la contravención de la norma con todo el ordenamiento jurídico en su conjunto. Es decir, la desaprobación del acto realizado por el autor. Las conductas típicas son antijurídicas, empero, si concurren algunas de las causas de justificación [\[108\]](#) de nuestro ordenamiento penal, la conducta típica no será antijurídica y, por lo tanto, no constituirá delito.

Como último elemento encontramos a la culpabilidad. La culpabilidad también conocida como la responsabilidad del autor del hecho delictuoso, es la atribución de la conducta antijurídica a su autor para hacerlo responsable del hecho.

Por tanto, la tipicidad, la antijuricidad y la culpabilidad son características comunes a todo delito. [\[109\]](#) Y van en ese orden, ya que si no existiera la tipicidad, no habrían las bases para determinar la antijuricidad y la culpabilidad [\[110\]](#), por tanto, si concurren todos estos elementos hay delito. [\[111\]](#) Ante la falta de uno de estos requisitos, no habría la comisión de un delito.

En definitiva, delito es el comportamiento típico, antijurídico y culpable. Adicionalmente, se ha de tener en cuenta que atendiendo a los principios de lesividad y proporcionalidad, la configuración de una conducta como delito sólo está justificada cuando se persiga la protección de un bien jurídico con significación para el Derecho penal.

1.2 El Concepto de Delito Informático

Se debe partir de la idea que todos los programas de informática pueden ser vulnerados; asimismo, de que todos los sistemas de seguridad basados en el software son vulnerables. [\[112\]](#)

De esta manera, las conductas delincuenciales respecto a sistemas informáticos son inimaginables, es por esto que es necesario una delimitación terminológica y conceptual de los llamados delitos informáticos.

Sin embargo, esta delimitación no es nada sencilla y, por el contrario, como señala ROMEO CASABONA [\[113\]](#), las nuevas tecnologías informáticas deben ser reducidas a sus justos términos. En efecto, no se debe entender que por el mero hecho de que en una conducta intervenga un elemento del ámbito de atención de la informática ésta sea un delito informático.

De mantenerse esta postura acabaría por considerarse a cualquier conducta delictiva en la que se vea implicada una computadora como delito informático.

En primer lugar, debemos entender qué conductas están referidas a los llamados “delitos informáticos”. Creemos que la falta de una definición general sobre las conductas que comprenden el llamado “delito informático” se debe a la inexistencia de una tipificación generalizada. Así, si existiera una definición sobre que es en realidad un “delito informático” para todos los países, sería mucho más fácil comprender el concepto de esta conducta.

Así, encontramos términos como delitos informáticos, delitos electrónicos, delitos relacionados con las computadoras,

crímenes por computadoras, delincuencia relacionada con los sistemas informáticos, etc.; son denominaciones que se han creado a fin de señalar conductas ilícitas en las que se emplean sistemas informáticos.

Muchos han sido los esfuerzos de expertos, tanto de juristas como de ingenieros de sistemas, sobre una definición única de delito informático. Pese a tales esfuerzos, aún no se ha conseguido dar una definición unánime sobre que es un “delito informático”.

Según el material revisado para el presente trabajo, podemos llegar a decir que no existe una definición propia, tanto a nivel nacional como internacional, de “delito informático”, ni existe un concepto uniforme sobre su significado.

Por ejemplo, para BRAMONT-ARIAS[114] no existe un concepto único sobre delito informático; “ello, debido que la delincuencia informática[115] se basa en una cantidad de conductas que son difíciles de agrupar en un solo significado.”

Un sector de la doctrina considera que se debe recurrir a las características de los sistemas informáticos. Así, en opinión de MATELLANES[116], el significado de delito informático comprende aquellas conductas que constituyen agresiones a las funciones de procesamiento, transmisión y ejecución de programas propios de sistemas informáticos, de esta manera, el significado de delito informático se verá considerablemente reducido y excluirá a aquellos delitos tradicionales que utilizan los medios informáticos para la comisión de algún ilícito penal.[117] Así, serán excluidos del ámbito de delito informático, por ejemplo, el robo de una computadora o de un diskette, o agresiones a un sistema de ordenador, etc.

Para DAVARA RODRÍGUEZ[118] no parece adecuado hablar de delito informático ya que, como tal, no existe, si atendemos a la necesidad de una tipificación en la legislación penal para que pueda existir un delito. Por ejemplo, el Código penal español de 1995 no introduce el delito informático, ni admite que exista como tal un delito informático, si bien admite la expresión por conveniencia, para referirse a determinadas acciones y omisiones dolosas o imprudentes, penadas por la Ley, en las que ha tenido algún tipo de relación en su comisión, directa o indirecta, un bien o servicio informático.

Para SIEBER[119] los Delitos Informáticos comprenden todas las acciones dolosas e ilícitas del patrimonio relacionadas con datos procesados automáticamente.

LA ORGANIZACIÓN PARA LA COOPERACIÓN ECONÓMICA DEL DESARROLLO[120] (OCDE) ha definido al delito informático como cualquier conducta ilegal, no ética, o no autorizada que involucra el procesamiento de datos y/o la transmisión de datos.

TIEDEMANN[121], por su parte, define al delito informático como aquel acto antijurídico que para su comisión se emplea un sistema automático de procesamiento de datos o de transmisión de datos.

Por su parte JIJENA LEIVA[122], define a los delitos informáticos 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.

Como se puede apreciar de la mayoría de autores citados, el concepto de delito informático involucra en el medio comisivo de

la conducta delictuosa un sistema informático o base de datos.

Cabe agregar que la ausencia de una identificación homogénea del delito informático es también consecuencia del hecho que la mayoría de empresas no sólo no denuncia estos hechos, sino que los niega rotundamente, dado el temor al desprestigio que pudiera provocar estas denuncias.^[123] Por ejemplo, si A ha transferido sumas de dinero a una cuenta por medio de los sistemas de cómputo del Banco X, éste no denunciará el hecho, debido a que pudiera crear un pánico colectivo a distintos ahorristas que confían en el prestigio y seguridad del Banco X.^[124]

Ello también pone en evidencia la existencia de una gran dificultad en cuanto a la elaboración de estadísticas sobre los delitos informáticos. La *cifra negra*^[125] es muy alta, existen grandes dificultades para descubrir estas conductas ilícitas y más aún para sancionarlas.^[126] Así, las víctimas optan por sufrir las consecuencias e intentar prevenir estas conductas en un futuro, conciliar con los delincuentes informáticos y no iniciar un procedimiento judicial.

En definitiva, podemos advertir que la doctrina mayoritaria define al delito informático como aquella conducta en la cual el medio comisivo es la utilización propia de un sistema informático. Sin embargo, pensamos que esta idea es demasiado genérica, pues el empleo en sí mismo de un sistema informático no es determinante para poder hablar de la existencia de un “delito informático”, toda vez que se ampliaría el concepto de éste y se incurriría en el error de definir como delito informático a todas aquellas conductas en donde intervenga un sistema informático, como pudiera ser el caso del médico que prescribe una medicina mediante correos electrónicos a un paciente y le altera la receta, cometería, entonces, un homicidio “informático”. O, por ejemplo, el daño que se genere por un delito de lesiones en donde el objeto fue una computadora, también constituirían un delito informático o un delito de estafa a una empresa virtual que se pudiera cometer mediante un sistema informático. Así, todos los delitos, en un futuro no muy lejano, constituirían un delito informático por el creciente uso de la red o sistemas informáticos.

Por tanto, en nuestra opinión, creemos que para poder dar una definición propia sobre las conductas que configuran el "delito informático" es prioritario y necesario identificar qué bienes jurídicos se protege y si estos bienes jurídicos deben ser objeto de protección penal. Pues, entendemos que la creación de un delito atendiendo a los principios de lesividad y proporcionalidad, sólo está justificada cuando exista un objeto jurídico digno de protección penal.

Desde esta perspectiva, la determinación del objeto de protección nos brindará, precisamente, los índices necesarios de tipificación o no de un delito informático con autonomía.

En tal virtud, antes de asumir una posición acerca de si las conductas nocivas que se cometen a través de sistemas informáticos y de Internet anteriormente descritas configuran un delito informático, resulta necesario revisar previamente el objeto de protección al que se pretende otorgar protección penal.

1.3 Delimitación del Bien Jurídico de los Delitos Informáticos

1.3.1 Función del Derecho Penal

Antes de ocuparnos acerca de la problemática del bien jurídico protegido en el delito informático, creemos conveniente precisar nuestra opinión acerca de la función que tiene el Derecho penal en nuestra sociedad actual.

A partir de las décadas de los años 60' y 70', el Derecho penal se encontraba en una discusión jurídico penal referente al

principio de protección exclusiva de bienes jurídicos.[\[127\]](#)

Como vemos, muchas décadas han pasado, sin embargo, hasta el momento la discusión se ha visto acrecentada aún más debido a la aparición de nuevas teorías –especialmente en Alemania- que pretenden encontrar la verdadera función del Derecho penal.

Es conveniente señalar que los últimos desarrollos de la ciencia jurídico penal muestran posiciones doctrinales que atribuyen una función al Derecho penal, por ello, a todas estas posturas se les denomina “funcionalistas” debido a que se refieren única y exclusivamente a la “función” que el Derecho penal cumple. Por lo que al hacer referencia a la corriente funcionalista del Derecho penal no se ha de identificar sólo a aquella concepción funcionalista-normativista de JAKOBS.[\[128\]](#)

Muchos han sido los intentos por explicar la finalidad del Derecho penal, sin embargo, existen básicamente dos teorías acerca de las funciones que cumple el Derecho penal actual. Ambas teorías, al no constituir tema central del presente trabajo de investigación, serán brevemente explicadas con la finalidad de adoptar, al final de este apartado, aquella que se adecue con nuestra legislación y con nuestra realidad social, y que permita, a su vez, una mejor comprensión de los delitos informáticos.

1.3.2 La Función de Tutela de Bienes Jurídicos

Podemos señalar que el término “bien jurídico” se atribuye a BIRNBAUM, a mediados del siglo XIX.[\[129\]](#) El origen de este concepto es propio de la dogmática del objeto de protección elegido por la ley. Posteriormente, VON LISZT afirmó que el origen del bien jurídico era en realidad un interés de la vida previo al Derecho, que surgía de las relaciones sociales; sin embargo, admitió que el interés vital no se convierte en bien jurídico hasta que es protegido por el Derecho. Por su parte, los Neo-kantianos situaron el origen del referido bien en el mundo espiritual subjetivo de los valores culturales.[\[130\]](#)

Con el finalismo se vincula la idea del bien jurídico con el orden social; sin embargo, la teoría del bien jurídico pasa a un segundo plano, en la medida que WELZEL, desde su teoría final de la acción, pone el acento en los deberes ético-sociales que sirven de base a los mandatos y prohibiciones.[\[131\]](#)

Con posterioridad al finalismo han prevalecido las orientaciones político-criminales que vinculan la teoría del bien jurídico con los fines del ordenamiento jurídico penal.

La discusión se centra entre aquellas posiciones que formalizan los fines del ordenamiento jurídico recurriendo a la Constitución, ya sea identificando bienes jurídicos con derechos fundamentales o bien con los fines del Estado y la sociedad trazados en el texto constitucional, y las posiciones que van más allá y pretenden identificar los bienes jurídicos en la realidad social.

Uno de los principales exponentes de la tesis constitucionalista es ROXIN[\[132\]](#), quien sostiene que "El punto de partida concreto consiste en reconocer que la única restricción previamente dada para el legislador se encuentra en los principios de la Constitución. Por tanto, un concepto de bien jurídico vinculante político-criminalmente sólo se puede derivar de los cometidos plasmados en la Ley Fundamental de nuestro Estado de Derecho basado en la libertad del individuo, a través de los cuales se le marcan sus límites a la potestad punitiva del Estado." En tal medida, para este autor el concepto de bien jurídico le viene previamente dado al legislador penal, pero no es previo a la Constitución.

Dentro de las concepciones que vinculan la teoría del bien jurídico con la realidad social misma, se ha de destacar la obra de BUSTOS RAMÍREZ[133], cuya posición acerca de la teoría del delito toma, precisamente, al bien jurídico como piedra angular del sistema.

Para este autor, la característica de toda sociedad democrática es la concepción de la persona humana como ente social, cuya forma de expresión son las relaciones sociales (comunicativa y participativamente) en una sociedad determinada; luego, el bien jurídico es una síntesis normativa determinada de una relación social concreta y dialéctica.

Los desarrollos de la doctrina respecto del bien jurídico se han dado, en la mayoría de los casos, debido a la búsqueda de tesis conciliadoras de las dos posiciones anteriores; así, por ejemplo, para MUÑOZ CONDE Y GARCÍA ARÁN[134], "a la norma penal, igual que a las demás normas jurídicas, le incumbe una función eminentemente protectora. La diferencia entre la norma penal y las demás normas jurídicas en esta materia radica en la especial gravedad de los medios empleados por la norma penal para cumplir esta misión y en que sólo interviene o debe intervenir en los casos de ataques muy graves a la convivencia pacífica."

Como bien señala MIR PUIG[135], "el Derecho penal de un Estado social ha de justificarse como sistema de protección de la sociedad". Los intereses sociales que por su importancia pueden merecer la protección del Derecho se denominan "bienes jurídicos".

"Por el término "bienes jurídicos" se entiende aquellos presupuestos que la persona necesita para su autorrealización y el desarrollo de su personalidad en la vida social." [136] Así, la autorrealización humana necesita de unos presupuestos existenciales que, en tanto son de utilidad para el hombre, se denominan "bienes" y mientras sean objeto de protección por el Derecho, serán "bienes jurídicos"

Ahora bien, es necesario señalar la diferencia entre "bienes jurídicos" (a secas) y los "bienes jurídicos objeto de protección penal", ya que la absoluta autonomía del Derecho penal en la configuración de sus efectos no quiere decir que éstos pueden ser empleados de cualquier modo, en su calidad y cantidad, para proteger bienes jurídicos cualesquiera. Acertadamente señala MUÑOZ CONDE[137] que si para el restablecimiento del orden jurídico violado es suficiente con las medidas civiles o administrativas, son éstas las que deben emplearse y no las penales.

Sabemos que no todos los bienes jurídicos deben y pueden ser tutelados por el Derecho penal[138], ya que ello contravendría los principios de subsidiariedad y carácter fragmentario del Derecho penal.[139] Esta diferencia debe tomarse en cuenta para determinar qué bienes jurídicos deberán ser o no tutelados por el Derecho penal y cual deberá de ser el criterio para limitar al "*ius puniendi*". [140]

En definitiva, entendemos que la presente teoría establece que la verdadera función del Derecho penal se basa en la protección de bienes jurídicos[141], determinando estos bienes jurídicos como penales, debido a una finalidad de protección de las condiciones fundamentales de la vida en común[142], es decir, porque son condiciones fundamentales de toda sociedad moderna. Este hecho es conocido también como el principio de proporcionalidad.

1.3.3 La Función de Tutela de la Vigencia de las Normas.

Por otro lado, tenemos la tesis contraria que cuestiona la protección de bienes jurídicos como función primordial del Derecho penal. Esta tesis funcionalista-normativista fue creada por JAKOBS, quien asegura que "el Derecho penal no repara bienes,

sino que confirma la identidad normativa de la sociedad.”[\[143\]](#)

Esta teoría establece que el Derecho penal no puede reaccionar frente a un hecho en cuanto lesión de un bien jurídico, sino solamente frente a un hecho en cuanto contraviene la norma.[\[144\]](#) Explica así, que el quebrantamiento de la norma no se trata de un suceso natural entre seres humanos, sino de un proceso de comunicación, de expresión de sentido entre personas.

Dicha teoría se concibe como “aquella teoría según la cual el Derecho penal está orientado a garantizar la identidad normativa, la constitución y la sociedad.”[\[145\]](#)

Asimismo, el modelo de imputación de JAKOBS parte por reconocer que al igual que lo que sucede en el mundo de la naturaleza en el que las expectativas cognitivas tienen su aprendizaje en el trato mismo con la naturaleza respecto de los fenómenos que suceden, y que a partir de ello se puede confiar en determinadas regularidades; por ejemplo, nadie camina pensando todo el día en que puede ocurrir un terremoto. En el marco de las relaciones sociales también el hombre ha de recurrir a tales expectativas cognitivas cuando se trata del contacto con otros hombres, de tal suerte que al entrar en contacto social con los demás, el sujeto no espera un output totalmente indeterminado del otro, pues se confía en determinadas regularidades, luego nadie está pensando en que el compañero de clase le va a hurtar la billetera.[\[146\]](#) De lo contrario, cada contacto social se convertiría en un riesgo impredecible.[\[147\]](#)

Desde este orden de ideas, la tesis funcionalista-normativista pretende demostrar que la sociedad está configurada a través del establecimiento entre sus miembros de determinadas expectativas, las mismas que orientan, precisamente, los comportamientos de los miembros de la sociedad.

En opinión de JAKOBS, sucede que a veces las expectativas de la naturaleza se ven defraudadas, puede darse un terremoto, luego, el hombre aprende a tomar más cuidado, a comportarse de otra manera ante estos fenómenos naturales, se llega a ser juicioso por medio de la experiencia.[\[148\]](#)

Respecto de las relaciones sociales no puede predicarse lo mismo, ante

la defraudación de una expectativa garantizada jurídicamente no hay que adaptarse a esa defraudación, no hay que encontrar la solución del conflicto volviendo a aprender algo, por ejemplo, usando en el futuro un casco, esto es, asociando el conflicto con un comportamiento propio, sino que hay que asociar el conflicto con el comportamiento incorrecto del autor, de tal suerte que la víctima se mantiene contrafácticamente en su expectativa.

Por último, esta tesis impone la idea de que el Derecho penal se ocupa de garantizar la configuración de la identidad de la sociedad, al igual que una persona rechaza una propuesta que no encaja en su forma de ser, ratificando de ese modo su forma de ser, así también la sociedad rechaza la propuesta de abandonar la expectativa defraudada, ratificando así su identidad.[\[149\]](#)

En definitiva, la tesis funcionalista-normativista se encuadra dentro de la pugna entre naturalismo y normativismo, y rechaza como función del Derecho penal la protección de bienes jurídicos, en la medida que ésta se apoya en una perspectiva naturalista que busca los objetos materiales para dotar de contenido a la intervención penal; mientras que, desde su punto de análisis, lo importante es que el Derecho penal persiga la función de mantener aquellas expectativas normativas de conducta que en un momento histórico la sociedad considera fundamentales para el desarrollo de los sujetos.[\[150\]](#)

1.3.4 Posición personal respecto a la función del Derecho Penal

Debemos señalar que nuestra intención no es explicar a profundidad las razones por las cuales nos adherimos a la tesis de la protección de los bienes jurídicos, sin embargo, debemos indicar que nos unimos a la mayoría de la doctrina que piensa que la verdadera función del Derecho penal se encuentra en la protección de bienes jurídicos.

Brevemente, explicaremos las razones de esta adhesión a la referida teoría. Básicamente, son tres puntos:

- a. Creemos que la teoría funcionalista-normativista de JAKOBS se expone a tres objeciones; i) la falta de un punto de partida crítico hacia el sistema social; ii) la falta de la estructura lógico-material y iii) la falta del sujeto. Asimismo, de un estudio superficial de la teoría funcionalista-normativista de JAKOBS y pese a la funcionalidad del sistema, consideramos que el Derecho penal ha de conservar la misión de proteger bienes jurídicos, ya que constituye una de las garantías fundamentales del Derecho penal en la medida en que la protección se basará necesariamente en las relaciones sociales de los individuos.
- b. Somos de la opinión que la tesis funcionalista-normativista de JAKOBS no es uniforme, sino que se basa en determinados tipos de sociedad, no existiendo unidad de criterios. Como acertadamente señala SILVA SANCHEZ, la adopción de una perspectiva exclusivamente funcionalista puede anular de hecho la eficacia limitadora del concepto, pues, ciertamente, la protección de valores morales o (incluso, como sucede en nuestros días, de determinadas estrategias políticas) puede ser estimada “funcional” en una determinada sociedad.
- c. Por último, la asunción de la tesis que considera la función del Derecho penal como protección de bienes jurídicos tiene un apoyo de carácter legislativo, ya que el Principio de Lesividad establecido en el artículo IV del Título Preliminar del Código penal peruano, señala que la pena, necesariamente, precisa de la lesión o puesta en peligro de bienes jurídicos tutelados por la ley. Al respecto, nos parece acertada la diferencia que anotan BRAMONT-ARIAS y GARCÍA CANTIZANO[151] en cuanto señalan que la extensión que debe darse a este elemento del delito depende de cómo se concibe la función del Derecho penal dentro de la sociedad.
- d. “El criterio dominante, y el que ha seguido nuestro legislador al momento de elaborar el Código penal peruano, ha sido el de clasificar los delitos de acuerdo al bien jurídico protegido”[152], por tanto, “se debe considerar que al Derecho penal sólo le importan las infracciones de una norma si con ella se lesiona o pone en peligro bienes jurídicos tutelados por la ley”. [153]

Por lo tanto, apoyamos firmemente la tesis en la cual la función del Derecho penal es la de proteger bienes jurídicos, debido a que se basa técnicamente en que el Derecho penal debe proteger valores e intereses que deban tener relevancia constitucional[154], sin que ello signifique la identificación de bienes jurídicos y derechos fundamentales, sino que la configuración de los bienes jurídicos ha de estar en armonía con los lineamientos trazados en el texto constitucional respecto de la sociedad, el Estado y el orden jurídico.

1.4 El contenido del bien jurídico protegido en los Delitos Informáticos

Como se ha podido apreciar en la primera parte del presente trabajo, las diferentes conductas nocivas que se cometen a través de sistemas informáticos y en Internet pueden ocasionar diversas lesiones a diferentes bienes jurídicos protegidos, tales como la intimidad, el patrimonio y nuevos objetos jurídicos de protección que adquieren autonomía e identidad propias en la red, los cuales serán tratados en los apartados siguientes.

Es innegable que el bien jurídico protegido es un punto de referencia obligado para la determinación del tipo penal del delito

informático, pues determina el marco dentro del cual pueden realizarse las conductas delictivas. [155] Ahora bien, luego de haber optado por la tesis que recoge la función del Derecho penal como la exclusiva protección de bienes jurídicos, nos dedicaremos a determinar el bien jurídico protegido en los delitos informáticos.

Al igual que sucede respecto del concepto de delito informático, sobre el cual, como hemos visto, no existe un consenso unánime en cuanto a su significado, creemos que ocurre lo mismo en cuanto al contenido del bien jurídico protegido. Algunos autores sostienen que en los delitos informáticos el bien jurídico protegido es el patrimonio y la intimidad de la persona.

Sin embargo, creemos que si bien estos bienes jurídicos pueden verse afectados mediante el uso de sistemas informáticos, principalmente debido a la expansión de la tecnología, no constituyen bienes jurídicos propios de los delitos informáticos, ya que se trata de objetos de protección penal que están más allá del uso de los sistemas informáticos y que, en consecuencia, no se han originado producto de la tecnología.

De su viabilidad como objetos de protección en estos delitos nos ocuparemos a continuación; sin perjuicio de identificar aquellos otros objetos de protección que resulten autónomos y propios de la red, los cuales serán tratados más adelante.

1.4.1 La Intimidad como bien jurídico protegido

Se puede decir que la elaboración doctrinal que sirve de precedente a la constitucionalidad del derecho a la intimidad, fue concebida como “*the right to be let alone*”, es decir, el derecho a ser dejado en paz o a ser dejado solo, término que se originó en el año 1,890 cuando WARREN y BRANDEIS publicaron un artículo sobre “*The Right to Privacy*”. [156]

Para empezar a desarrollar la intimidad [157] como bien jurídico protegido por el Derecho penal, nos vemos en la obligación de señalar las diferencias entre el significado del vocablo intimidad y privacidad.

Para HERRÁN ORTIZ, “por el vocablo intimidad se alude tanto al carácter oculto o secreto de aquellas circunstancias que rodean la existencia de un individuo, como a las circunstancias internas, esenciales del hombre y que éste mantiene como núcleo de su personalidad”. [158]

La palabra privacidad sigue siendo un anglicismo en nuestro entorno. El Diccionario de la Real Academia de la Lengua Española aún no ha recogido dicho concepto. [159]

Sin embargo, DAVARA RODRIGUEZ [160] define la privacidad como el “término al que le podemos hacer referencia bajo la óptica de la pertenencia de los datos a una persona –su titular- y que en ellos se puedan analizar aspectos que individualmente no tienen mayor trascendencia, pero que al unirlos a otros pueden configurar un perfil determinado sobre una o varias características del individuo que éste tiene derecho a exigir que permanezcan en su esfera interna, en su ámbito de privacidad.”

En el plano jurídico, concordamos con MUÑOZ CONDE [161] cuando señala que el “derecho a la intimidad trata de tutelar la voluntad de una persona física o jurídica de que no sean conocidos determinados hechos que tan sólo ella o un número limitado de personas conoce.”

Ahora, si bien es cierto que tan sólo la persona natural queda comprendida dentro del concepto “intimidad”, los alcances de dicho término deben abarcar también a la persona jurídica, ya que, como se sabe, toda persona jurídica va a poseer información reservada y valiosa que nadie tiene derecho a conocer o revelar. Sin embargo, el Código penal peruano

comprende como sujeto pasivo de los delitos contra la intimidad tan sólo a la persona natural y no a la persona jurídica.[\[162\]](#)

Por tanto, es necesario seguir el ejemplo del Código penal español, en donde se establece que el Título X “Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio” abarca también a la persona jurídica. Así, es importante señalar la opinión de PÉREZ LUÑO[\[163\]](#) respecto del artículo 200 del Código penal español [\[164\]](#). El referido autor entiende que la tutela penal de la intimidad se extiende a las personas jurídicas, cuando se descubren o revelan datos reservados de personas jurídicas sin el consentimiento de sus representantes legales.

De esta manera, el nuevo Código penal español corrige uno de los aspectos más insatisfactorios de la LORTAD (actualmente LOPD), ya que a medida que el proceso de datos se proyecta a las empresas, a las instituciones y asociaciones, se hace cada vez más evidente la conveniencia de no excluir a las personas jurídicas del régimen de protección que impida o repare los daños causados por la utilización indebida de informaciones que les conciernen.

En efecto, la defensa de la intimidad y los demás derechos fundamentales no es privativa de los individuos, sino que debe proyectarse a las formaciones sociales en las que los seres humanos desarrollan plenamente su personalidad.

Ello se aprecia, fundamentalmente, en cuanto a la participación de las personas jurídicas en el sistema económico, dentro del cual adquiere el rol de agente económico y es socialmente individualizada en la unidad empresarial.[\[165\]](#) De ahí que, las personas jurídicas ostentan una identidad y significación social propias y distintas de las personas naturales que la integran y/o representan.

En el plano internacional, el derecho a la intimidad ha sido reconocido en el artículo 12 de la Declaración Universal de Derechos Humanos de las Naciones Unidas de 1948, en el artículo 8.1 de la Convención Europea para la protección de los Derechos Humanos y de las Libertades Fundamentales de 1950 y en el artículo 17.1 del Pacto Internacional de Derecho Civiles y Políticos de 1966.[\[166\]](#)

Es ya conocida la violación constante a los derechos de la intimidad de individuos por información que se encuentra latente en Internet. Todo parece ser que el derecho a la intimidad relacionado con el aspecto informático juega un papel importante en la red. Así, aparece el término “intimidad informática”, el cual podemos entender como la información personal que puede ser manejada en la red y/o almacenada en el disco duro de una computadora.[\[167\]](#) Si bien es cierto que la definición de intimidad informática ha sido producto del desarrollo de la tecnología, podemos argumentar que se trata de la misma intimidad y del mismo concepto que se ha venido desarrollando años atrás, variando, únicamente, la forma de almacenamiento de los datos de carácter personal.

De otro lado, cabe indicar que la página web es considerada como medio de difusión general, por lo tanto Internet es un espacio difícil para preservar derechos fundamentales como la intimidad.[\[168\]](#) En efecto, Internet es un territorio incómodo para preservar derechos fundamentales, como, por ejemplo, el derecho a la intimidad[\[169\]](#), el dominio reservado de cada uno que no se desea abrir al conocimiento de los demás. Al parecer con la denominada sociedad de la información ha sido cuando más se ha invadido la intimidad de las personas, hasta el punto que en la actualidad el individuo reclama la adopción de instrumentos jurídicos de respuesta a las sucesivas y frecuentes intromisiones que debe padecer en su intimidad.[\[170\]](#)

El gran riesgo de la privacidad frente a la informática es inimaginable. "El empleo de computadoras hace factible recopilar una amplia información sobre cada persona, reuniendo un conjunto de datos que aisladamente nada dicen, pero que al ser presentados en forma sistematizada, pueden dar lugar a una información que el afectado no se imagina ni le agradaría ver en

poder de otros.

Tengamos presente que un computador puede clasificar y relacionar rápidamente, por ejemplo, nuestros datos económicos, legales, laborales y de salud, construyendo un detallado perfil de cada individuo." [\[171\]](#)

La facilidad para hacer acopio, tratar, transmitir y almacenar información pone en riesgo uno de los bienes más preciados del ser humano: su derecho a la intimidad, a no permitir que los demás conozcan de uno aquello que no deseamos que se conozca y, en último caso, si esto llega a ocurrir que podamos saber quién tiene nuestros datos, qué datos tiene, cómo los ha obtenido y para qué los quiere. [\[172\]](#)

De la misma manera deben considerarse las conductas que ponen a disposición de menores de edad imágenes de contenido altamente sexual

explícito y que ponen en riesgo su formación integral ocasionando trastornos en el normal desenvolvimiento de su personalidad.

Se debería controlar esta situación mediante el acceso a estas páginas web con doble clave. Asimismo, evitar casos de prostitución infantil por esta vía.

De otra parte, los contenidos nocivos en Internet están amparados bajo la libertad de expresión, sin embargo, no debe olvidarse la preservación del derecho de las personas, en cuanto a que alguna información nociva existente en Internet pueda afectar a algún individuo.

“Gran notoriedad ha alcanzado la polémica acerca del control en Internet de contenidos tales como “la pornografía infantil o aquellos que inciten al odio por motivos de raza, sexo, religión, nacionalidad u origen étnico. La gravedad de estos comportamientos, las peculiares exigencias que impone la supervisión de los contenidos disponibles por Internet y la paulatina extensión de este medio a sectores de la población necesitados de especial protección, como los menores, justifican la importancia del debate que se ve condicionado por la existencia de estándares diferentes según los países al concretar los límites de lo tolerable.” [\[173\]](#)

Una manera de solucionar este problema podría ser prohibir la utilización de la tecnología que permite estas formas de agresión, como el *spam* o los *cookies*, sin embargo, parece que es imposible hacerlo -otra cosa es limitar su empleo- sin acabar con técnicas imprescindibles para el funcionamiento del sistema.

Pero creemos que es necesario regular el uso que se puede dar a los datos que tan fácilmente se obtienen de cualquiera que se asoma a la red, aunque sólo sea para curiosear lo que hay en ella. [\[174\]](#)

Pareciera ser entonces que las cuestiones a decidir son las limitaciones al desarrollo de la libre comunicación en la red y cómo puede preservarse la intimidad y los datos personales [\[175\]](#) frente a su utilización abusiva o no consentida; y para esto la libre comunicación en la red y la preservación de la intimidad y los datos personales tienen que ser normas universales.

Uno de los avances legislativos en materia de protección de datos se dio en España, a través de la Ley Orgánica 5/92 de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal, más conocida como la LORTAD, posteriormente modificada por la Ley Orgánica 15/99 “Ley de Protección de Datos de Carácter Personal” (LOPD), publicada

el 14 de diciembre de 1999, mediante la cual se establecen principios que fijan las obligaciones en relación con el procesamiento y utilización de datos; así tenemos el **principio de calidad de los datos personales**, que prevé que sólo podrán recogerse datos de carácter personal para su tratamiento automatizado, cuando tales datos sean adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades legítimas para las que se haya obtenido[176]; el **principio de transparencia y publicidad del tratamiento**, vinculado a brindar informaciones precisas a los interesados para que puedan contrastar y evaluar la incidencia y alcance que en sus derechos y libertades fundamentales va a tener el tratamiento automatizado de sus datos personales[177]; el **principio de seguridad de los datos de carácter personal**, que establece la obligación del responsable del fichero de adoptar las medidas de índole técnica y organizativas necesarias para garantizar la seguridad de los datos personales y evitar su alteración, pérdida, tratamiento o acceso no autorizado[178]; el **principio del consentimiento**, que exige que en todo tratamiento automatizado de datos de carácter personal se deberá requerir la autorización del afectado.[179]

De igual modo, Alemania posee, según cada estado federal, leyes de protección de carácter personal. Así, tenemos la Bundesdatenschutzgesetz (BDSG)[180]. La Ley Federal sobre Protección de Datos dictada en la Ley para el Desarrollo de Elaboración y Protección de Datos de fecha 20 de diciembre de 1990, modificada por la Ley sobre el Nuevo Ordenamiento de Sistema de Correo y de las Telecomunicaciones de 14 de setiembre de 1994. La finalidad de esta ley es la protección de los datos personales y los perjuicios para los derechos de la personalidad.

Asimismo, en Alemania algunos estados han adoptado leyes sobre protección de datos dentro de su jurisdicción, así tenemos el caso de la Bayerische Datenschutzgesetz (BayDSG) de 23 de julio de 1993, modificada el 25 de octubre del año 2000.

Por su parte, en el Perú no existe hasta el momento una ley similar que regule los derechos y obligaciones con relación a la utilización de datos, por lo que nos tendremos que limitar a lo establecido por el artículo 2 inciso 6 de la Constitución en donde se señala que toda persona tiene derecho a que los servicios informáticos computarizados o no, públicos o privados, no suministren informaciones que afecten la intimidad personal y familiar. Es decir, se protege el derecho a la intimidad de cada persona al evitar que los datos no sean mal empleados y no perjudiquen así a su titular y a su entorno familiar.

Asimismo, la Ley de Habeas Data, Ley N° 26470, constituye una de las garantías constitucionales más modernas, a través de la cual todo individuo tiene derecho a accionar contra el hecho u omisión, por parte de cualquier autoridad, funcionario o persona, que vulnera o amenaza los derechos a que se refiere el artículo 2, inciso 5 y 6 de la Constitución.[181] Es importante señalar que para el Perú es necesario la creación de una ley que regule la protección de datos de carácter personal (en donde no se excluya a la persona jurídica), tarea que deberá ser dejada para los legisladores.

Por otro lado, el Código penal en el Capítulo II del Título IV “Delitos contra la Intimidad”, artículo 154, establece que la pena no será mayor de dos años cuando la violación de la intimidad personal o familiar, sea mediante procesos técnicos u otros medios.

Así, el legislador ha tratado de abarcar aquellas conductas producto del avance tecnológico al establecer el término “u otros medios” para que de esta manera queden comprendidas aquellas conductas atentatorias a la intimidad por medio del uso de sistemas informáticos.

De la misma opinión son BRAMONT-ARIAS y GARCÍA CANTIZANO[182], quienes señalan que mediante el empleo del término “por otros medios” el legislador deja una cláusula abierta, donde tendría cabida el avance de las nuevas tecnologías, sobre todo de la informática.

Por tanto, las conductas que configuren los tipos penales de los delitos contra la intimidad (artículos 154 a 157) mediante el uso de redes o sistemas informáticos, se encuentran, todas ellas, con la debida protección penal.

En definitiva, la intimidad resulta ser un bien jurídico de posible afectación a través de la red; no obstante ello, la conducta atentatoria por sí misma no representaría la configuración de un delito informático, en la medida que lo único que variaría respecto del tipo básico del delito contra la intimidad es la modalidad empleada, es decir, el uso del medio informático, lo cual no le brinda autonomía ni identidad para dejar de ser un delito propio contra la intimidad.

En igual sentido, CARBONELL Y GONZÁLEZ[183] objetan la denominación de estas conductas como “delitos informáticos”, ya que, en puridad, se deberían llamar “delitos contra la intimidad de las personas mediante el uso de la informática y de las comunicaciones” debido a que el bien jurídico protegido sigue siendo la intimidad.

Por último, del análisis expuesto, podemos concluir que los delitos contra la intimidad en donde los medios de ejecución sean sistemas informáticos, el bien jurídico protegido seguirá siendo la intimidad y, por lo tanto, no podemos hablar de delitos informáticos, ya que somos de la opinión que el derecho a la intimidad no es característica exclusiva de los sistemas informáticos, ya que sólo está en relación a ellos en cuanto al tipo de información almacenada, lo cual nos permite sostener que la intimidad constituye un valor a ser preservado en la red y sistemas informáticos, sin llegar a sostener que constituye el bien jurídico protegido en los delitos informáticos.

1.4.2 El Patrimonio como bien jurídico protegido

Existen principalmente cuatro tesis planteadas en torno al concepto de “patrimonio”. La concepción jurídica del patrimonio, la concepción económica estricta del patrimonio, la concepción patrimonial personal y, por último, la concepción mixta o jurídico-económica del patrimonio. No siendo nuestra intención explicar las referidas teorías, nos limitaremos a comentar brevemente la posición que actualmente asume la doctrina mayoritaria.

Desde esta concepción el patrimonio está constituido por la suma de los valores económicos puestos a disposición de una persona, bajo la protección del ordenamiento jurídico.[184]

Como acertadamente señalan BRAMONT-ARIAS Y GARCÍA CANTIZANO[185], “un aspecto digno de ser resaltado es el grado de reconocimiento jurídico requerido en los bienes de contenido económico para constituir el patrimonio.

En base a esto, los bienes ilícitos forman también parte del concepto de patrimonio, dado que, al adquirirse un bien ilícito, éste pasa a formar parte del patrimonio de su adquirente; esto es, se daría una relación fáctica que entraña un valor económico, siempre y cuando no sea frente al propietario.”

Ahora, debido al desarrollo que ha tenido el comercio electrónico, el patrimonio se ha convertido en un derecho importante para todo individuo que ingresa a la red. “El traslado creciente de las decisiones a sistemas informáticos presenta sobre todo el problema penal de cuando y por qué la protección del patrimonio, la cual es clásicamente otorgada sólo contra las formas de ataque de engaño (astucia), amenaza y violencia, como también de abuso de confianza, es ampliada a la burla de los dispositivos de seguridad que ofrece o puede ofrecer el sistema informático.” [186]

El patrimonio se evidencia como uno de los principales objetos de protección en la red debido a la expansión del comercio electrónico como nueva forma de contratación, de allí que su protección adquiere enorme relevancia dentro de la criminalidad informática.

Como hemos visto respecto del derecho a la intimidad, en los cuales los delitos contra la intimidad por medio de sistemas informáticos se les denomina delitos informáticos, con el derecho al patrimonio sucede lo mismo. Así, el derecho a la intimidad y al patrimonio, han sido –hace mucho tiempo- erróneamente considerados como bienes jurídicos penales en los denominados delitos informáticos.

En efecto, entendemos 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 informáticos. Las nuevas formas de lesión del patrimonio mediante el empleo de sistemas informáticos deberían ser comprendidas como nuevas modalidades de los delitos patrimoniales y no como delitos informáticos autónomos. Así, por ejemplo, se puede advertir del artículo 186 inciso 3 que sanciona como modalidad de hurto agravado la sustracción de un bien mueble cometida mediante la utilización de sistemas de transferencia electrónica de fondos, de la telemática en general, o la violación del empleo de claves secretas, dicha conducta no constituirá un delito informático *per se* en la medida en que recoge para su configuración típica todos los elementos propios del tipo básico previsto en el delito de hurto del artículo 185, lo cual limita el objeto jurídico de la acción a bienes muebles, entre ellos el dinero, sin que pueda abarcar las funciones propias de los sistemas informáticos, constituyendo por tanto una modalidad de delito patrimonial.

En definitiva, si bien el patrimonio se erige como un valor a ser preservado y salvaguardado en la red, no constituye el bien jurídico protegido en los delitos informáticos, ya que no responde a la propia naturaleza de la red que está en función del acceso y transmisión de información.

Por tanto, concluimos que aquellas conductas que sean realizadas mediante sistemas informáticos o redes, en donde el bien jurídico afectado sea el patrimonio, no se les deberá dar la definición de delitos informáticos, ya que en un futuro caeríamos en el error de comprender a todos los delitos contra el patrimonio como delitos informáticos.

1.4.3 El Honor como bien jurídico protegido

“Jurídicamente, el derecho al honor 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 méritos y cualidades que ha ido adquiriendo como fruto de su desarrollo personal y social.” [\[187\]](#)

El honor como objeto de protección penal ha sido concebido desde muy diversas perspectivas, sin embargo, para una concepción estrictamente jurídica, la dignidad de la persona, como sujeto de derecho, constituye la esencia misma del honor y determina su contenido. [\[188\]](#)

“Los servicios y aplicaciones de Internet pueden ser instrumentos para la realización de actividades que suponen intromisiones ilegítimas en el derecho al honor, a la intimidad personal y familiar y a la propia imagen.” [\[189\]](#)

Al igual que otros bienes jurídicos tutelados por el Derecho penal, el derecho al honor puede verse afectado; ya sea por algún envío masivo a un determinado grupo de personas de mensajes difamatorios, como publicaciones en páginas web con información que atente contra el honor de una determinada persona.

Conviene resaltar la aparente cercanía que existiría entre los bienes jurídicos honor e intimidad; sin embargo, concordamos con HERRÁN ORTIZ [\[190\]](#), al establecer que “jurídicamente el honor y la intimidad representan diferentes bienes de la persona, lo

cual no significa que mediante una misma acción no puedan ser lesionados ambos, ya que el derecho a la intimidad se caracteriza por el derecho del individuo a preservar su vida privada de cualquier injerencia ajena, mientras que el derecho al honor se define por el derecho al respeto que merece toda persona en su dignidad humana”.

Desde este orden de ideas, partimos por reconocer que tanto el honor como la intimidad pueden verse afectados, conjunta o indistintamente, a través del empleo de medios informáticos.

Sin duda, el debate se ha desarrollado debido a las numerosas reclamaciones interpuestas por usuarios contra proveedores de servicios de Internet, típicamente operadores de foros de discusión, por mensajes difamatorios publicados en esos foros. Entre la inicial jurisprudencia de EE.UU. dos decisiones se han convertido en referencia obligada. En el asunto *Cuvi vs Compuserver* no se consideró responsable por las afirmaciones difamatorias de terceros, a un proveedor de servicios en uno de cuyos foros de discusión habían aparecido esas afirmaciones, con base en que el proveedor de servicio actuaba como un mero distribuidor de información. Por su parte, en el asunto *Stratton Oakmont vs. Prodigy* el proveedor de servicios demandado fue considerado responsable por comentarios difamatorios de terceros aparecidos en un foro de discusión que ofrecía, con base en que decía ejercer un control efectivo sobre los contenidos públicos y había implantado ciertos mecanismos de control.[\[191\]](#)

Ahora bien, el alcance del control que se ejerce varía significativamente según los instrumentos tecnológicos empleados. En concreto, la simple aplicación de programas de filtro que detectan el empleo de expresiones que pueden ser indicio de la existencia de contenidos ilícitos, no es un medio determinante del efectivo control de la presencia de contenidos difamatorios. Por lo tanto, la mera contraposición entre la ausencia de todo control, de una parte, y el efectivo control de los contenidos en los términos tradicionales de la supervisión editorial de los medios de información tradicionales, de otra, es una simplificación que margina la realidad del alcance de las tecnologías de filtrado más difundidas.

En esta línea, la tradicional distinción entre los grupos de noticias moderados y aquellos en los que no está presente un moderador, a los efectos de atribuir responsabilidad al proveedor en la medida en que su foro es moderado, no impide apreciar que si bien la función del moderador es controlar qué mensajes son difundidos, su selección – en un contexto, caracterizado por la multiplicidad de mensajes, la participación de diversos servidores en la difusión de los foros, la heterogeneidad de los participantes en la red y la velocidad a la que se sucede la publicación de mensajes- se ciñe en muchas ocasiones a comprobar que el mensaje se corresponde con la materia a la que se refiere ese foro, sin analizar su contenido y en particular que éste puede generar responsabilidad civil.[\[192\]](#)

“Ante la incertidumbre generada, diversos ordenamientos jurídicos han reaccionado fijando legislativamente el alcance de la responsabilidad de los proveedores de servicios de Internet en supuestos de intromisión en el derecho al honor o a la propia imagen.”[\[193\]](#)

Ahora bien, la posible afectación del honor mediante el empleo de sistemas informáticos tampoco configura un delito informático, en la medida en que el medio informático representa sólo una característica de la conducta llevada a cabo que por sí misma no varía su naturaleza de delito contra el honor.

En efecto, conductas que afecten el honor mediante publicaciones en páginas web, el envío de correo masivo, u otros medios, no constituyen *per se* un delito informático. Por lo que deberá ser de aplicación lo establecido en los artículos 130 y siguientes del Código penal, no siendo necesario ninguna modificación al respecto. Cabe destacar que según la doctrina nacional, la persona jurídica podrá ser sujeto pasivo en los delitos de injuria y difamación, más no del delito de calumnia, en donde el sujeto pasivo no podrá ser una persona jurídica, debido a que la conducta típica es la de atribuir un delito y éste sólo puede ser cometido por una persona natural y no por una persona jurídica.[\[194\]](#)

Respecto a la doctrina extranjera, específicamente la doctrina española, ha ido asimilando la idea que una persona jurídica puede tener derecho al honor. Así, FRÍGOLA y ESCUDERO[195] establecen que “referente al derecho al honor de las personas jurídicas, la doctrina del Tribunal Constitucional ha ido evolucionando desde una inicial posición negadora de que dichas personas tuvieran honor, alegando para ello el significado personalista del derecho al honor exclusivo de las personas físicas, a una progresiva aceptación, de tal forma que en la actualidad se reconoce que las personas jurídicas puedan ver menoscabado su honor.”[196]

Por tanto, la actual doctrina del Tribunal Constitucional Español es clara al respecto, reconociendo que las personas jurídicas pueden ver menoscabado su honor, tras la entrada en vigor del nuevo Código penal (español), que ha mantenido a las personas jurídicas dentro del ámbito de protección del derecho al honor.[197]

No obstante, se ha de advertir que la atribución a una persona jurídica de la realización de conductas delictivas puede quedar comprendida dentro de los alcances del artículo 240 del Código penal peruano, en cuanto se atente contra la reputación comercial de la empresa, siempre que se refiera a las actividades, servicios o productos de las personas jurídicas.[198]

Es importante destacar la sentencia de la Sala Penal de la Corte Suprema de la República (R.N. N°953-2000), de fecha 18 de diciembre del 2000, la misma que generó discrepancias en los magistrados acerca del uso de los medios informáticos para la configuración típica de los delitos contra el honor y sobre el procedimiento especial que siguen las querellas tratándose de la aplicación del artículo 314° del Código de Procedimientos Penales[199] respecto de dicho uso.

Los hechos se refieren a la incriminación que se efectúa contra el querellado Harry Hans Venegas Berastain al haber emitido un correo electrónico a todas las oficinas en el extranjero de la empresa Inspectore Griffith, en cuya sucursal Inspectorate Griffith del Perú SAC labora el querellante, dando a entender a todos los funcionarios de dicha empresa en el mundo que el querellante Douglas José Ruiz Díaz es un delincuente por cuanto la empresa RANSA Comercial Sociedad Anónima lo ha denunciado penalmente por los delitos de estafa y contra la fe pública, lesionando de esta manera la imagen y reputación del querellante.

Los autos se refieren a dos situaciones concretas:

- a. Si el envío de un correo electrónico o e-mail cuyo contenido es difamatorio, constituye un medio idóneo para la realización del delito de difamación, previsto en el artículo 132° del Código penal.
- b. La excepción de naturaleza de juicio promovida en virtud a establecerse si como consecuencia de utilizar un correo electrónico cuando se dirige a numerosas empresas corporativas con acceso al personal de cada una de ellas, constituye el medio de comunicación masiva que hace referencia el artículo 314° del Código de Procedimientos Penales, cuando señala “u otro medio análogo de publicidad”, esto es, si se puede asimilar al delito cometido por medio de impresos, publicaciones, prensa u otro medio de publicidad, y, en consecuencia, tramitarse la causa de acuerdo al procedimiento especial de investigación sumaria.

La discrepancia suscitada al interior de la Sala Penal oscila entre la consideración del envío de un correo electrónico a varias personas como la realización de la conducta típica de atribuir a una persona un hecho, una cualidad o una conducta que pueda perjudicar su honor o reputación, de manera que pueda difundirse la noticia. Esto es, si el e-mail constituye un medio de difusión idóneo para la difamación ante varias personas reunidas o separadas. Y, por otro lado, si de considerarse un medio

idóneo para la realización del tipo penal del artículo 132° del C.P., es posible su comprensión dentro de los alcances de la fórmula “otro medio análogo de publicidad” prevista en el artículo 314° del Código de Procedimientos Penales.

La solución dada por mayoría en la Sala Penal es que sí ha de considerarse al correo electrónico como medio idóneo para la realización del delito de difamación por medio de comunicación social, en virtud de que es asimilable al delito cometido por medio de impresos, publicaciones, prensa u otro medio de publicidad y atendiendo, sobre todo, a que cuando el correo electrónico es dirigido a varias personas, estas a su vez pueden comentar con otras personas, por lo que constituye un medio de comunicación masiva.

Existe, no obstante, el voto singular del Vocal Supremo Dr. Hugo Sivina Hurtado, quien considera que no puede ser considerado el envío de un correo electrónico como idóneo para la realización del delito de difamación a través de un medio de comunicación social, en atención a que viene a ser un medio de intercomunicación personal a través de un sistema informático o red de comunicación electrónica de datos y, de otro lado, en el presente caso fueron remitidos en forma separada e individual a los ficheros informáticos privados de los distintos representantes de la empresa involucrada, cuyos códigos de acceso eran conocidos por el querellado. Sobre esta polémica debemos efectuar algunas notas que sirvan a la aclaración de lo discutido en la sentencia.

En cuanto a determinar si el envío de un correo electrónico con información difamatoria a diversas personas configura el tipo básico del delito de difamación en los términos de la tipicidad contenida en el artículo 132° del Código penal, debemos señalar que sí, ya que las exigencias típicas del delito de difamación se caracterizan por la atribución a una persona de un hecho, cualidad o conducta que pueda perjudicar su honor o reputación, ante varias personas reunidas o separadas, de manera que pueda difundirse la noticia; para ello el envío de un correo electrónico se muestra como un medio idóneo para su realización, no siendo necesario que se lleve a cabo mediante el envío de un correo masivo, esto es, un solo e-mail a distintas personas, ya que la propia norma señala que puede darse este delito respecto de personas que se encuentran separadas a través del envío de varios e-mails. A ello, se ha de agregar que concurrirían todos los elementos necesarios para que pueda difundirse la noticia, ya que el envío de un correo puede generar, a su vez, su reenvío a una infinidad de usuarios de la red.

Entendemos, por otra parte, que si bien el envío de varios correos electrónicos a distintas personas puede considerarse como un medio idóneo para la realización de la conducta típica del delito de difamación, difícilmente puede ser considerado dentro de los alcances de la expresión “otro medio análogo de publicidad” contenida en el artículo 314° del Código de Procedimientos Penales, pues la analogía en este caso está en función de una exposición al público y del uso de medios de difusión masiva, como sucede a través de la radio o la televisión; de ahí que coincidamos con el voto singular emitido en la sentencia en análisis en el sentido que el correo electrónico o e-mail resulta un medio de intercomunicación personal a través de un sistema informático o red de comunicación electrónica de datos, sin que represente un medio de comunicación social, y, en consecuencia, no cabe la posibilidad de sustanciarse la causa conforme al procedimiento especial de investigación sumaria.

Por último, es necesario advertir -como ha sido explicado líneas arriba- que sí debería ser considerado como medio de publicidad análogo la edición y publicación de una página web con información difamatoria, ya que no sólo resulta un medio idóneo para la realización de la conducta típica del delito de difamación, sino que, además, no se trata de una comunicación interpersonal, sino que está dirigida a la comunidad de la red y pueden acceder a ella todos los usuarios del sistema sin limitación alguna, resultando un medio de comunicación social masivo.

En definitiva, observamos que la jurisprudencia nacional todavía no ha recogido la verdadera dimensión del uso de los sistemas informáticos ni su operatividad en la realización de determinadas conductas típicas, ello ha de responder a un progresivo desarrollo de los conocimientos informáticos dentro de los magistrados y a la elaboración de una casuística que permita una jurisprudencia vinculante. En definitiva, el honor no es ni puede ser el bien jurídico protegido en los delitos informáticos.

1.4.4 La libertad Informática

Según el Diccionario de la Real Academia de la Lengua Española, la libertad es la facultad natural que tiene el hombre de obrar de una manera o de otra, y de no obrar, por lo que es responsable de sus actos. [\[200\]](#)

Según el mismo diccionario, por el término "informática" se entiende el conjunto de conocimientos científicos y técnicas que hacen posible el tratamiento automático de la información por medio de ordenadores. [\[201\]](#)

Hoy por hoy, debido al avance tecnológico y como respuesta a la necesidad de tutela de los derechos humanos, surge para ser frente a las necesidades de los individuos propias de la denominada "era tecnológica", la "Tercera Generación de Derechos". [\[202\]](#)

Entre los derechos de la "Tercera Generación" destaca la libertad informática o autodeterminación informativa [\[203\]](#), en donde se pretende tutelar los derechos frente a la creciente utilización de la informática. Como señala ÁLVAREZ-CIENFUEGOS [\[204\]](#), la libertad informática, como bien jurídico objeto de consumo en las sociedades avanzadas, no puede concebirse sin el contrapunto de la salvaguarda o defensa de los datos personales que afecten la intimidad personal y familiar. Por tanto, por "libertad informática" se puede entender el derecho del individuo a controlar el uso de sus datos personales tratados o insertos en un programa informático.

La libertad informática ha sido denominada 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 bancos de datos -lo que se denomina habeas data por su función análoga en el ámbito de la libertad de información a 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". [\[205\]](#)

Ahora bien, creemos que el derecho a la autodeterminación informativa o libertad informática se encuentra estrechamente vinculado al concepto de intimidad, ya que se trata de ofrecer al individuo la seguridad de sus datos de carácter personal ante el posible uso mediante la informática u otro sistema automatizado; sin embargo, no es necesario que los datos utilizados sean íntimos o pertenezcan 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. [\[206\]](#)

Con respecto al término "autodeterminación informativa" existen básicamente dos opiniones encontradas, la de PÉREZ-LUÑO [\[207\]](#), quien considera la autodeterminación informativa como la respuesta del presente al fenómeno de contaminación de las libertades que amenaza con invalidar los logros del progreso tecnológico en los Estados de Derecho con mayor desarrollo económico. Sin embargo, para SÁNCHEZ DE DIEGO el término "derecho a la autodeterminación" tiene en la actualidad, tanto en el Derecho internacional como constitucional, una significación muy precisa –referida a la capacidad de los pueblos a determinar su destino político y totalmente diferente a la que se quiere dar. [\[208\]](#)

Concordamos con SÁNCHEZ DE DIEGO, ya que el término "autodeterminación" puede confundirse con los derechos que protege el Derecho internacional. Creemos, pues, que para los derechos que se defienden es más claro y preciso el término "libertad informática". Ahora, no solamente existe un debate entre el concepto de autodeterminación informativa, sino que existe la discusión acerca de si la definición de la libertad informática es equiparable a la autodeterminación informativa. Después de un largo debate entre cada posición, la mayoría de autores estudiosos del tema, equiparan el término libertad informática con la autodeterminación informativa. [\[209\]](#)

Por último, surge también la interrogante de si las personas jurídicas gozan del derecho a la libertad informática. La LORTAD (ahora LOPD), luego de un incesante debate, excluye a las personas jurídicas, las cuales no ostentan la condición de beneficiarios de las garantías propias del derecho a la libertad informática en la legislación española.

Así como se discute la responsabilidad penal por parte de una persona jurídica, en donde, la mayoría de la doctrina española, especialmente MUÑOZ CONDE^[210], sugiere un tipo de responsabilidad penal para las empresas, creemos que es necesario la adopción o modificación de la LORTAD (ahora la LOPD) para que las personas jurídicas gocen también de la denominada

“libertad informática” y de esta manera pueda orientarse en ese camino la legislación de diversos países.^[211]

Por su parte, el Perú garantiza la libertad informática en el artículo 2 incisos 4, inciso 6, 7 y 10 de nuestra Constitución Política. Según el artículo 2° de nuestra Carta Magna toda persona tiene derecho: a las libertades de información, opinión, expresión y difusión del pensamiento mediante la palabra oral o escrita o la imagen, por cualquier medio de comunicación social, sin previa autorización ni censura ni impedimento algunos, bajo las responsabilidades de ley (inciso 4), a que los servicios informáticos, computarizados o no, públicos o privados, no suministren informaciones que afecten la intimidad personal y familiar (inciso 6), al honor y a la buena reputación, a la intimidad personal y familiar así como a la voz y a la imagen propias (inciso 7) y al secreto y a la inviolabilidad de sus comunicaciones y documentos privados (inciso 10).

Somos de la opinión, que si bien el artículo segundo hace referencia a la persona en términos generales sin hacer distinción alguna entre persona natural y persona jurídica, no todos los derechos consagrados en dicha norma resultan de aplicación para la persona jurídica, pues los casos de intimidad personal y familiar hacen referencia al individuo y no a un ente colectivo, así como al honor; sin embargo, sí creemos que comprendería o debería comprender, en todo caso, a la persona jurídica en cuanto ésta debe gozar de libertad de información, opinión, expresión, así como el derecho de una buena reputación, al secreto e inviolabilidad de sus comunicaciones y documentos privados.

En definitiva, la libertad informática se erige como un objeto de protección dentro de la red, caracterizado por el derecho que tiene el individuo a decidir que información personal se podrá difundir y el destino de esta información, derechos comprendidos en los denominados derechos de “Tercera Generación”. Se trata de un bien jurídico de naturaleza individual y personal.

Por tanto, creemos que debido a la relación que existe entre la libertad informática y el derecho a la intimidad, ambos bienes jurídicos se encuentran vinculados en la medida en que el ejercicio de la capacidad de decidir sobre los datos protegidos por el derecho a la intimidad, constituye precisamente el ejercicio de la libertad informática cuando tales datos se encuentren almacenados en un sistema informático; por lo que no se debe considerar la libertad informática como un bien jurídico que requiere de protección penal en forma autónoma de la intimidad, ya que quien disponga de datos que se encuentren almacenados en sistemas informáticos y los utilice en perjuicio del titular, estará afectado el derecho a la intimidad o al honor, según sea el caso.

Por último, llegamos a la conclusión que la libertad informática si bien se erige como un valor a ser reconocido en la red, no podrá ser considerada como bien jurídico en los delitos informáticos, debido a que consiste en la facultad de decidir sobre los datos de carácter personal y, precisamente, el ejercicio de dicha libertad se verifica a través de los límites establecidos por el derecho a la intimidad y al honor, bienes jurídicos que cuentan con protección penal.

1.4.4.1 La Libertad Informática en el Derecho Comparado

A continuación se presenta una breve relación sobre las disposiciones fundamentales sobre la libertad informática y los derechos a la intimidad personal y familiar y a la privacidad en las Constituciones de América Latina. [\[212\]](#)

En Argentina, mediante el artículo 43 dispone: Toda persona puede interponer acción expedita y rápida de amparo, siempre que no exista otro medio judicial más idóneo, contra todo acto u omisión de autoridades públicas o de particulares, que en forma actual o inminente lesione, restrinja, altere o amenace, con arbitrariedad o ilegalidad manifiesta, derechos y garantías reconocidos por esta Constitución, un tratado o una ley.

En el caso, el juez podrá declarar la inconstitucionalidad de la norma en que se funde el acto u omisión lesiva.

Podrán interponer esta acción contra cualquier forma de discriminación y en lo relativo a los derechos que protegen al ambiente, a la competencia, al usuario y al consumidor, así como a los derechos de incidencia colectiva en general, el afectado, el defensor del pueblo y las asociaciones que propendan a esos fines, registradas conforme a la ley, la que determinará los requisitos y formas de su organización.

Toda persona podrá interponer esta acción para tomar conocimiento de los datos a ella referidos y de su finalidad, que consten en registros o bancos de datos públicos, o privados destinados a proveer informes, y en caso de falsedad o discriminación, para exigir la supresión, rectificación, confidencialidad o actualización de aquellos. No podrá afectarse el secreto de las fuentes de información periodística.

Cuando el derecho lesionado, restringido, alterado o amenazado fuera la libertad física, o, en caso de agravamiento ilegítimo en la forma o condiciones de detención, o en el de desaparición forzada de personas, la acción de habeas corpus podrá ser interpuesta por el afectado o por cualquiera en su favor y el juez resolverá de inmediato, aun durante la vigencia del estado de sitio.

Por su parte, Brasil consagra el derecho a la libertad informática en los Art. 5/10 – 22/IV – 102/d.-

Artículo 5.- Todos son iguales ante la ley, sin distinción de cualquier naturaleza, garantizándose a los brasileños y a los extranjeros residentes en el País la inviolabilidad del derecho a la vida, a la libertad, a la igualdad, a la seguridad y a la propiedad, en los siguientes términos: ...10: . son inviolables la intimidad, la vida privada, el honor y la imagen de las personas, asegurándose el derecho a indemnización por el daño material o moral derivado de su violación....

Artículo 22.- Compete privativamente a la Unión legislar sobre:...IV: aguas, energía, informática, telecomunicaciones y radiodifusión;...

Artículo 102.- Es competencia del Supremo Tribunal Federal, principalmente, la garantía de la Constitución, correspondiéndole:

I. procesar y juzgar, originariamente:

“...d) los habeas corpus, siendo sujeto pasivo cualquiera de las personas señaladas en las líneas anteriores; los mandados de seguridad y los habeas data contra actos del Presidente de la República, de las Mesas de la Cámara de los Diputados y del

Senado Federal, del Tribunal de Cuentas de la Unión, del Procurador General de la República y del propio Supremo Tribunal Federal;...”

En Chile el artículo 19 inciso 4 señala lo siguiente:

Artículo 19.- La Constitución asegura a todas las personas:.... 4° El respeto y protección a la vida privada y pública y a la honra de la persona y de su familia.

La infracción de este precepto, cometida a través de un medio de comunicación social, y que consistiere en la imputación de un hecho o acto falso, o que cause injustificadamente daño o descrédito a una persona o a su familia, será constitutiva de delito y tendrá la sanción que determine la ley. Con todo, el medio de comunicación social podrá excepcionarse probando ante el tribunal correspondiente la verdad de la imputación, a menos que ella constituya por sí misma el delito de injuria a particulares. Además, los propietarios, editores, directores y administradores del medio de comunicación social respectivo serán solidariamente responsables de las indemnizaciones que procedan;

De otro lado, Colombia establece en el artículo 15, lo siguiente: Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas.

En la recolección, tratamiento y circulación de datos se respetarán la libertad y demás garantías consagradas en la Constitución.

La correspondencia y demás formas de comunicación privada son inviolables. Sólo pueden ser interceptadas o registradas mediante orden judicial, en los casos y con las formalidades que establezca la ley.

Para efectos tributarios o judiciales y para los casos de inspección, vigilancia e intervención del Estado podrá exigirse la presentación de libros de contabilidad y demás documentos privados, en los términos que señale la ley.

Por último, en Ecuador los artículos 23 inciso 8, 23 inciso 12 y 23 inciso 13 se señala lo siguiente:

Artículo 23.- Sin perjuicio de los derechos establecidos en esta Constitución y en los instrumentos internacionales vigentes, el Estado reconocerá y garantizará a las personas los siguientes:

Inc. 8.- El derecho a la honra, a la buena reputación y a la intimidad personal y familiar. La ley protegerá el nombre, la imagen y la voz de la persona.

Inc. 12.- La inviolabilidad de domicilio. Nadie podrá ingresar en él ni realizar inspecciones o registros sin la autorización de la persona que lo habita o sin orden judicial, en los casos y forma que establece la ley.

Inc. 13.- La inviolabilidad y el secreto de la correspondencia. Esta sólo podrá ser retenida, abierta y examinada en los casos previstos en la ley. Se guardará el secreto de los asuntos ajenos al hecho que motive su examen. El mismo principio se observará con respecto a cualquier otro tipo o forma de comunicación.

1.4.5 La Seguridad Informática

Según el Diccionario de la Real Academia de la Lengua Española, la seguridad se encuentra definida -respecto a los temas tratados- como el término que se aplica también a ciertos mecanismos que aseguran algún buen funcionamiento, previniendo que éste falle, se frustre o se viole. [\[213\]](#)

La informática es concebida por el autor ALTMARK [\[214\]](#) en términos amplios, como “la ciencia que estudia y tiene como objeto el tratamiento automatizado o electrónico de la información”.

Como se sabe, Internet es una red abierta donde la información es susceptible de ser inspeccionada, manipulada o intervenida por terceras personas. De hecho, el nacimiento de Internet se produce por la interconexión espontánea de redes y ordenadores a través de los cuales se formaliza la transmisión de información. Por lo tanto, la comunicación en Internet se produce de manera más sensible y menos segura, y la intrusión y alteración de cualquier comunicación es más frecuente.

Como señala MARTÍNEZ NADAL [\[215\]](#) “los riesgos más importantes derivados de un intercambio de información a través de redes abiertas son que el autor y fuente del mensaje hayan sido suplantados; que el mensaje se haya alterado, de forma accidental o de forma maliciosa, durante la transmisión; que el emisor del mensaje niegue haberlo transmitido o el destinatario niegue haberlo recibido; y que el contenido del mensaje sea leído por una persona no autorizada. A estas preocupaciones en materia de seguridad informática se corresponden los conceptos jurídicos de autenticación, integridad, no rechazo o no repudio y confidencialidad. Estos cuatro tipos de servicio de seguridad son ofrecidos por la técnica para conseguir una cierta certidumbre en los contenidos transmitidos por Internet. Así, la autenticación es el servicio que asegura la identidad del remitente del mensaje y que el mensaje procede de quien se dice que lo envía.

La integridad es el servicio que garantiza que el mensaje no ha sido alterado en el tránsito. El no rechazo o no repudio, es el servicio que garantiza que una parte interviniente en una transacción no puede negar su actuación. El no rechazo implica la autenticación y la integridad de un mensaje y, en este caso, se consiguen los efectos de la firma digital, pero no a la inversa, es decir, la autenticación y la integridad de un mensaje no implican, necesariamente, el no rechazo.

Las dos formas más importantes son el no rechazo en origen, que tiene por finalidad que el originador del mensaje no pueda negar un mensaje con un determinado contenido, y el rechazo en destino, que tiene como fin que el destinatario del mensaje no pueda negar haber recibido un mensaje con un determinado contenido. Por último, la confidencialidad es el servicio que protege los datos de revelaciones y accesos de personas no autorizadas”. [\[216\]](#)

Conforme hemos avanzado nuestra investigación, encontramos mayores elementos de juicio para sustentar la importancia que adquiere el uso de medidas técnicas y jurídicas en seguridad informática. [\[217\]](#)

La seguridad es uno de los aspectos más importantes en el uso de Internet. La falta de una [política de seguridad](#) global está frenando el desarrollo de Internet en áreas tan interesantes y prometedoras como el comercio electrónico o la interacción con las administraciones públicas. Nadie duda ya que es importante crear [un entorno seguro](#). [\[218\]](#)

Las tecnologías seguras están disponibles para organizaciones comerciales, tales como vendedores on-lines, instituciones financieras, bancos, operadores de tarjetas de crédito, etc. Estas tecnologías incluyen protección de contraseñas, vías de protección o cortafuegos, sistemas para prevenir el acceso no autorizado o simuladores de asaltos que verifican la integridad de un sistema de protección cortafuegos. Una vez que la información está en tránsito, se puede proteger mediante técnicas de

encriptación y software de autenticación que identifican al remitente y previenen el acceso no autorizado a esta información.

Una cuestión fundamental es la seguridad en la red que uno puede y debe poseer. Así, la seguridad en la red se puede centrar en dos áreas principales.

- . Acceso, asegurando el no acceso a observadores no autorizados
- b. Tránsito, certificando que la información viaje segura.

a. ACCESO

Es algo frecuente encontrar en la prensa que un sistema ha sido asaltado por un *hacker* o pirata informático, trabajando de modo independiente o como miembro de un grupo internacional. Los piratas cibernéticos se han introducido con éxito en numerosas instituciones financieras bloqueando sus sistemas o en algunos casos realizando daños severos. Pero estas actuaciones no han impedido el crecimiento vertiginoso de Internet y los bancos, que siempre han estado alerta con los ataques de criminales, cuentan con que estos cada día utilicen métodos más ingeniosos para realizar sus actos.

Por otro lado, las empresas comerciales de la red no han denunciado todavía ninguna fechoría en sus sistemas de seguridad, debido a varios hechos:

- a. El posible desprestigio comercial ante la colectividad.
- b. La gran incidencia que tiene la denominada cifra negra respecto a la denuncia de estos hechos.

Como consumidores estamos acostumbrados a utilizar tarjetas de crédito en restaurantes o tiendas que utilizan sistemas de transacción telefónica, con una mínima incidencia de fraude con este método. Es más, los sistemas electrónicos permiten un control automático que alertaría frente a un posible fraude, tanto del comprador, vendedor, intermediario o agente.

Ahora, el acceso no sólo está en función de la información almacenada, sino también en tránsito.

El acceso se torna como la primera función de los sistemas informáticos y ha de ser considerado dentro de la seguridad informática, ya que a partir del acceso a un sistema informático, el agente toma contacto con la información del titular del sistema lo que representa la llave de otras puertas que pueden conducir a atentados contra la intimidad, el patrimonio o el honor.

Así, para evitar accesos indebidos, la propia red ha configurado una serie de dispositivos como passwords, códigos secretos, claves, etc. que representan los mecanismos de seguridad que han de asumir los usuarios para preservar sus sistemas.

b. TRÁNSITO

Una vez que la información está en movimiento, los protocolos de seguridad de la Red y las aplicaciones de encriptación

proporcionan seguridad en las transacciones. Las firmas digitales autenticadas ofrecen una posibilidad a los sistemas de comprobar la genuinidad, del mismo modo que un código de barras o un número de tarjeta de crédito verifican la identidad de la persona.

Es cierto que no existe un único mecanismo de seguridad, sin embargo, la mayoría de ellos hace uso de técnicas criptográficas basadas en el cifrado de la información.[\[219\]](#)

Se ha de tener en cuenta que no sólo el almacenamiento de información es propiedad de la red, sino también el tránsito de la misma, por lo que la configuración de los sistemas informáticos está en función de establecer los mecanismos de seguridad respectivos.

Por otro lado, desde una perspectiva subjetiva, se ha de advertir que existe la denominada sensación social de inseguridad, propia de una sociedad enmarcada en un desarrollo tecnológico, con la consecuente aparición de nuevos riesgos, pluralidad de opciones y complejidad social.[\[220\]](#)

Las principales características que evidencian este fenómeno constituyen la revolución de las comunicaciones y las dificultades de adaptación de la población a sociedades en continua aceleración, situaciones que generan en la colectividad una falta de dominio del curso de los acontecimientos que se traduce en términos de inseguridad.[\[221\]](#) Las comunicaciones en la red no son ajenas a estos fenómenos y debido a su novedad y constante evolución, introducen permanentemente nuevos riesgos y, sin lugar a dudas, nuevas inseguridades, por lo que en esta materia también la seguridad se torna como un valor en sí misma, exigida por los usuarios de la red.[\[222\]](#)

La seguridad se erige en una pretensión social a la que se supone que el Estado y, particularmente, el Derecho penal deben dar respuesta.[\[223\]](#) La seguridad, a diferencia de la libertad informática, no está en función de la persona individualmente considerada, sino de la sociedad en su conjunto.

Desde este orden de ideas, la seguridad informática se erige como un objeto digno de protección en la regulación de la red y de los sistemas informáticos, sin embargo, la discusión se centra en si la seguridad informática posee los niveles exigidos para una protección jurídico penal.

Dar respuesta a esta interrogante no es fácil. Creemos que delimitar el interés social de si la seguridad informática se encuentra en la necesidad de ser protegida penalmente es una cuestión delicada. Sin embargo, trataremos de fundamentar esta posición al amparo del Derecho penal y de nuestros escasos conocimientos en informática.

Somos de la opinión, que la seguridad informática debe ser considerada como un bien jurídico protegido con relevancia penal, desde el momento en que tanto la vía administrativa como la vía civil no otorguen la debida protección a la seguridad en la red o en un sistema informático. Como hemos visto, debido a que la seguridad informática está en función del acceso por parte de los usuarios y del tránsito de información, resulta de suma importancia para el funcionamiento de la red y de los sistemas informáticos, ya que se trata de un bien jurídico anterior al derecho a la intimidad, al honor y al patrimonio. En consecuencia, el Derecho penal al proteger un bien jurídico como la seguridad informática de naturaleza supraindividual, está preservando, a la vez y en forma antelada, determinados bienes jurídicos individuales.

Por otro lado, la seguridad informática se verá lesionada en cuanto se atente al uso y funcionamiento de redes o sistemas

informáticos, como, por ejemplo, el acceso indebido a un computador, ya sea para realizar o no conductas ilícitas. Asimismo, como hemos visto en la primera parte del presente trabajo, existe un gran número de conductas que se cometen a través de la red en donde el inicio de estos medios de ejecución de posteriores delitos se basa específicamente en el acceso o ingreso indebidos a un determinado sistema informático.

En consecuencia, concluimos que la seguridad informática se erige como un bien jurídico que debe primar como objeto de protección en los delitos informáticos por su autonomía y característica principal del uso de los medios informáticos, esta fundamentación la desarrollaremos al exponer nuestra posición personal respecto del bien jurídico en los delitos informáticos.

1.4.6 La Información

Hemos dejado para el final de este apartado el tema de la información no precisamente por ser el elemento menos importante. La opción ha sido únicamente para poder comprender como la información se encuentra en una relación de dependencia –en nuestra opinión- tanto de la libertad como de la seguridad informáticas. Así, el derecho a que los datos de una persona se protejan, no es sino porque esa información es valiosa e importante para el individuo que impide el conocimiento de dicha información por otros sujetos. Al titular de la información le asiste la capacidad de decidir respecto de su divulgación hacia terceras personas, luego se trata del ejercicio de su libertad.

De igual manera sucede respecto de la seguridad. Tantos medios de seguridad en sistemas, hoy desarrollados, es porque anhelan la protección de la información de una pérdida o la protección frente al conocimiento de individuos. Ambas premisas suceden tanto a nivel personal como empresarial. La relación de la información con la seguridad se verifica materialmente en dos fases, su almacenamiento y transmisión, de ahí, precisamente, que afirmamos la relación de dependencia aquí planteada.

El término “información”, según la definición de la Real Academia de la Lengua Española significa: “enterar, dar noticia de algo”, sin embargo, dicho concepto se ha ampliado debido a que hoy en día se puede considerar como un interés social valioso.[\[224\]](#)

Ahora bien, como hemos visto en el primer capítulo, se hizo una breve reseña acerca de la “sociedad de la información” que se ha desarrollado producto de los avances tecnológicos, específicamente en Internet, por ser ésta la gran autopista de la información, pues bien, en este punto, debemos considerar a la información que es almacenada, tratada y/o transmitida a través de los sistemas informáticos. Ello nos permite distinguirla de aquella información referida al conocimiento de una persona, la misma que se desarrolla en la mente del sujeto y se vincula a sus subjetividades.

Como acertadamente establece MAZUELOS COELLO[\[225\]](#), la información codificada se erige en un valor cuantificable y fundamental para el desarrollo de las actividades de las empresas en el marco de la globalización económica. Así, el autor señala que en el futuro, la criminalidad no operará mediante asaltos a las bóvedas de los bancos, sino que recaerá sobre las bases de datos de las empresas, como pueden ser su cartera de clientes, sistemas de cobranza, contabilidad, balances, estrategia de mercado, desarrollo de tecnología, etc. No cabe duda que hoy en día la información constituye un bien de capital. [\[226\]](#)

Pues bien, no ha pasado mucho tiempo para que se halla configurado este tipo de criminalidad. Así, la información no sólo es importantísima a nivel empresarial, sino también en el ámbito personal. “La información, de la índole que sea, se ha convertido en un bien jurídico de extraordinario valor”.[\[227\]](#)

En la actualidad, empresas públicas, privadas y administraciones públicas invierten cuantiosas sumas en desarrollar sistemas de información automatizados que les permitan producir información para atender a sus requerimientos organizacionales y, en

consecuencia, intercambian y manipulan la más amplia variedad de datos, de diversa índole y con diferentes finalidades.[\[228\]](#) Por tanto, si la información es nominativa o relacionada con las personas se atentaría contra la intimidad, de ser económica o representar valores se atentaría contra la propiedad o contra el patrimonio. [\[229\]](#)

Si bien es cierto que la información almacenada en cuanto a su contenido puede determinarse de un modo muy subjetivo, ya que la información de un individuo o una empresa puede ser poco útil o importante para otro, no debe dejar de ser determinada a un valor económico[\[230\]](#). Este valor se lo dará, desde un plano individual, el titular de la información, de ahí que se trataría de un bien jurídico individual, personal; sin embargo, el sustento de la valoración de la información no puede estar apoyada en subjetividades individuales, por lo que debemos tomar en cuenta el valor que la información posee para la sociedad en su conjunto, por lo que deberá de apreciarse los indicadores del mercado, como pueden ser la bolsa de valores, el cambio del dólar, la tasa de intereses bancarios, etc., tratándose fundamentalmente de la información de la empresa.

Consideramos que respecto de una persona natural sigue siendo válido en cuanto a los datos personales, familiares, etc., seguir hablando de intimidad, mientras que respecto de la persona jurídica, respecto a datos vinculados a su actuación en el mercado, se debe hablar de información en cuanto tal, es decir, como valor económico de la empresa.

Esta concepción superaría las limitaciones que ostenta la persona jurídica para ser considerada como titular del derecho a la intimidad.

Como hemos visto en los apartados anteriores, la información almacenada puede lesionarse de diversas maneras, como, por ejemplo, por medios de sabotaje o espionaje informático, conductas realizadas por un *cracker*, un *phreaker* o hasta por un malicioso *hacker*.

En el ámbito administrativo, las normas encargadas de regular el uso de la información resultan muy limitadas. A modo de ejemplo, la propiedad intelectual se orienta a la salvaguarda de los programas contra la llamada “piratería de software”. La Ley sobre Represión de la Competencia resulta sólo aplicable a los supuestos de contenido de información, banco de datos informatizados etc., que constituyan de por sí una obra o creación. De esta forma en el marco del derecho administrativo sancionador se protege el programa en sí mismo pero no la información con él trabajada y archivada, razón por la cual podemos afirmar que existe un vacío legal sobre esta materia a nivel administrativo[\[231\]](#), tema que se deberá tener en cuenta por los legisladores con relación a las competencias del Derecho Administrativo.

Sucede lo mismo en materia penal. El desarrollo legislativo en materia de protección penal de la información, pese al avance producido en sistemas de

criptografía y codificación de información, es todavía muy incipiente en relación con los avances de la informática. “Así, se rechaza la equiparación de los atentados contra la información con aquellos delitos de apoderamiento material de bienes, ya que en el presente caso no estamos frente a “cosas muebles”, corporales y tangibles, sino que la acción recae sobre elementos inmateriales, intangibles, no susceptibles de apoderamiento material. Debido a ello, los ilícitos penales patrimoniales tradicionales como el hurto, la apropiación ilícita, etc., resultan inapropiados para una efectiva protección de la información como valor económico.”[\[232\]](#) “La revolución informática ha incidido en forma insospechada en el viejo concepto de la información, revitalizándolo espectacularmente e incrementando de forma extraordinaria su valor. Las nuevas técnicas posibilitan una potenciación indefinida de las acumulaciones de datos en poco espacio, de fácil acceso y recuperación, a través de una clave o código único, en cuestión de escasos segundos y de también muy simple interrelación, tratamiento y transmisión.”[\[233\]](#)

Como se puede apreciar, consideramos que la información en sistemas informáticos es un elemento importantísimo en la red,

en donde la información no sólo comprende a individuos, sino también a Estados, Instituciones, Organismos Internacionales, Empresas, etc.

En opinión de RIQUERT[234], el manipuleo y tratamiento que hoy se hace de la información, puede llegar a poner en serio peligro intereses y bienes de todo orden, tanto en el sector de la economía, la defensa nacional, la administración pública, etc., como en el más pequeño pero no menos importante espacio de la intimidad personal. Sin embargo, estimamos que la información al igual que otros bienes que concurren en la red o sistemas informáticos, requiere de una protección adelantada, para la cual, como hemos visto, se muestra idónea la seguridad informática. Otra de las razones por las cuales no consideramos a la información como bien jurídico penalmente relevante en los delitos informáticos, es porque la información puede ser manipulada, ya sea por un medio informático o no. Actualmente, en el Perú existen muchos lugares en donde la tecnología aún se encuentra incipiente y en donde el almacenamiento de información se encuentra no en archivos o sistemas informáticos sino físicamente en papel.

En sentido contrario parece abogar MAZUELOS COELLO[235], en cuanto a la información como valor económico de la empresa. Sin embargo, entendemos que al igual que la intimidad, la protección de la información se encontraría garantizada desde la protección penal de la seguridad informática, de ahí que no consideramos su configuración como bien jurídico penal.

En igual sentido REYNA ALFARO[236], quien propugna como propuesta de *lege ferenda*, la protección de la información “con valor económico de empresa” como bien jurídico penalmente relevante. Es decir, sólo cuando la información tenga un valor económico empresarial, deberá ser protegida por el Derecho penal, sin embargo, cabe preguntarse que si esto fuera así, que sucedería con los derechos de aquellas personas que posean información “sin un valor económico de empresa? Se verían desprotegidas por el Derecho penal por no encuadrarse en el tipo penal? Consideramos que si bien la información constituye un valor a ser salvaguardada en la red o sistemas informáticos, la intimidad sigue siendo el bien jurídico que tutelaría los datos personales, mientras que la tendencia a no considerar como titular de intimidad a la persona jurídica podrá verse superada desde la perspectiva de una protección adelantada a través de la seguridad informática.

De otra parte, si, como se ha seguido aquí, de lo que se trata es de salvaguardar la información en cuanto se encuentra almacenada, podrá resultar de aplicación la sustracción de la misma teniendo como objeto material de la conducta el soporte o base de datos, lo cual permitirá su comprensión dentro de los alcances del delito de hurto del artículo 185 del Código penal.

Por otro lado, pese a la cobertura de protección penal que se le podría dar a la información -con valor económico- como bien jurídico protegido, respecto de algunas conductas delictuales que se generan en la red o en sistemas informáticos que atenten contra el patrimonio o contra el orden socioeconómico, según sea el caso, se observa que existe otros intereses en juego no precisamente coincidentes con la noción de orden socioeconómico, como sucede con la seguridad informática frente al acceso indebido a un sistema informático.

1.5 Posición personal respecto del bien jurídico en los Delitos Informáticos

En nuestra opinión, la seguridad informática constituye una condición primordial de la existencia de los sistemas informáticos y de la red, por ello necesita de regulación y protección por parte del Derecho penal.

Creemos que debido al desarrollo tecnológico que se viene dando, la lesión de la seguridad informática se hace merecedora de una pena, ya que constituye un bien jurídico con relevancia penal a ser protegido en la red, debido a que es un bien jurídico autónomo, propio de la red y de los sistemas informáticos, y anterior a determinados bienes jurídicos individuales que están en juego en la red y los sistemas informáticos. Mientras que bienes jurídicos como el derecho a la intimidad, al patrimonio y al honor, si bien pueden verse afectados por medios informáticos, no son propios de la naturaleza de la red y sistemas

informáticos lo cual no nos dificulta pensar que son objeto de protección del delito informático.

Como hemos visto en la primera parte del presente trabajo, las conductas que atentan contra la red y contra sistemas informáticos ponen en peligro las relaciones sociales producidas en la red, dentro de las cuales la intimidad, el patrimonio y el honor resultan bienes jurídicos que sintetizan normativamente tales relaciones, relegadas a un segundo plano, pues protegiéndose la seguridad informática se protege anteladamente tales bienes jurídicos de naturaleza individual.

A continuación nos ocuparemos de la fundamentación de la seguridad informática como bien jurídico protegido en los delitos informáticos.

1.5.1 Fundamentación Constitucional

Se ha de precisar que los alcances del bien jurídico no deben provenir exclusivamente del texto constitucional, en forma que se identifique bienes jurídicos con derechos fundamentales, pues ello significaría atrofiar el sistema penal de protección de bienes jurídicos y supeditar al texto expreso de la Constitución. De ahí que se haya de partir de una interpretación y desarrollo del texto constitucional sin perder de vista aquellos criterios empíricos y prejurídicos que provienen de la realidad social y muestran, precisamente, la necesidad preventiva de la intervención penal.

Desde este orden de ideas, observamos que la Constitución Política de 1993 no reconoce expresamente la protección de la seguridad informática, por lo que su verificación constitucional ha de ser derivada de otros principios, derechos y libertades de las personas contenidos en el texto constitucional. En efecto, la omisión constitucional no impide la conceptualización de la seguridad informática como bien jurídico penal ni que el legislador esté debidamente legitimado para expedir normas que protejan este bien jurídico.

Así, se ha de recurrir a la construcción de la seguridad informática a partir de otros derechos fundamentales que están en juego en la red y sistemas informáticos, a saber: intimidad, honor, patrimonio, libertad de información, secreto e inviolabilidad de las comunicaciones y documentos privados. Al respecto la Constitución Política señala como derechos de la persona:

“Artículo 2º.- Toda persona tiene derecho:

4) A las libertades de información, opinión, expresión y difusión del pensamiento mediante la palabra oral o escrita o la imagen, por cualquier medio de comunicación social, sin previa autorización ni censura ni impedimento algunos, bajo las responsabilidades de ley. (...)

5) A solicitar sin expresión de causa la información que requiera y a recibirla de cualquier entidad pública, en el plazo legal, con el costo que suponga el pedido. Se exceptúan las informaciones que afectan la intimidad personal y las que expresamente se excluyan por ley o por razones de seguridad nacional. (...)

6) A que los servicios informáticos, computarizados o no, públicos o privados, no suministren informaciones que afecten la intimidad personal y familiar.

7) Al honor y a la buena reputación, a la intimidad personal y familiar así como a la voz y a la imagen propias.

Toda persona afectada por afirmaciones inexactas o agravada en cualquier medio de comunicación social, tiene derecho a que éste se rectifique en forma gratuita, inmediata y proporcional, sin perjuicio de las responsabilidades de ley.

10) Al secreto y a la inviolabilidad de sus comunicaciones y documentos privados.

Las comunicaciones, telecomunicaciones o sus instrumentos sólo pueden ser abiertos, incautados, interceptados o intervenidos por mandamiento motivado del juez, con las garantías previstas en la ley. Se guarda secreto de los asuntos ajenos al hecho que motiva su examen. (...)

16) A la propiedad y a la herencia.”

La seguridad informática en cuanto bien jurídico colectivo está en relación de complementariedad con los derechos y libertades anteriormente descritos y constituye un desarrollo de la protección (anticipada) de los mismos en cuanto a que al dotársele de protección penal se prohíbe la realización de conductas que generan riesgos para determinados bienes jurídicos personales como la libertad de información, intimidad, patrimonio, honor, inviolabilidad de las comunicaciones.

Como hemos visto en la primera parte de esta investigación, los riesgos y peligros propios de la red y los sistemas informáticos debido al proceso de aceleración que vive la sociedad a través de la ampliación y generalización del uso de medios informáticos, ponen en peligro no sólo el funcionamiento de la red y los sistemas y el conjunto de actividades en ellos desarrollados, sino, y principalmente, este proceso viene generando riesgos para los mencionados bienes jurídicos personales. Sin embargo, se ha de advertir que en el reconocimiento de esta situación y la necesidad de control de tales riesgos, la respuesta penal podría, en principio, asumir dos enfoques normativos diferentes. Uno de ellos es la creación de delitos adicionales que se estiman ponen en peligro al público en general, haciendo referencia a los objetos de protección individuales tradicionales, como el patrimonio, la intimidad, el honor, la inviolabilidad de las comunicaciones, etc. (orientación seguida por el legislador nacional en la promulgación de la ley de delitos informáticos); otro enfoque esgrime la posibilidad de construir delitos especiales contra la seguridad informática que abarquen, en forma independiente, aquellas entidades propias al uso y funcionamiento de los sistemas informáticos.

Nuestro planteamiento es la orientación hacia la segunda opción, pues partimos de la idea que el recurso a la exclusiva protección de bienes personalísimos dentro de la red, si bien permitiría superar las deficiencias actuales en cuanto a la tipicidad de las conductas y el respeto al principio de legalidad, conllevaría el desconocimiento de la relevancia social que ha adquirido la red como tal en cuanto forma de comunicación de los sujetos, con identidad y autonomía propias. A ello se ha de agregar que un sistema de protección que desconozca una protección antelada de la seguridad informática como bien autónomo, sería poco idóneo para proteger los bienes jurídicos individuales, ya que la norma penal tendría una influencia demasiado lejana en el control de los atentados a estos bienes debido a que sería preciso probar la motivación y la intención subjetiva del autor respecto del patrimonio, honor, intimidad, etc., lo que en la mayoría de los casos no es posible, pues el ataque no se dirige contra estos bienes.

Por otra parte, la protección penal de la seguridad informática busca propiciar una función simbólica positiva, en cuanto estimula la conciencia social sobre la necesidad de protección de la seguridad en la red y la gravedad del uso y funcionamiento indebidos de la misma.

En consecuencia, una protección desde los bienes individuales sería deficiente porque no respondería a las actuales expectativas sociales que exigen una protección directa y más eficaz.

La protección de la seguridad informática es indispensable para el correcto uso y funcionamiento de las redes y sistemas informáticos. Ahora bien, la titularidad colectiva de este bien jurídico viene dada por su propia naturaleza, ya que la red es una sola e interrelacionada en diversos sub - sistemas informáticos y, en consecuencia, no es fraccionable o divisible en sí misma considerada, lo cual

nos permite afirmar la indisponibilidad de este bien. En efecto, las agresiones a la seguridad informática van a crear riesgos frente a todos los integrantes de la colectividad y no respecto de un sujeto en concreto, de ahí que todos y cada uno de los sujetos de la colectividad tengan un interés particular en la protección del bien jurídico colectivo.

1.5.2 Fundamentación Jurídico – Penal

En cuanto a la seguridad informática y a las garantías jurídico-penales, debemos afirmar que desde el punto de vista de la intervención punitiva, surge la necesidad de una concreción y delimitación del concepto en orden a dos consideraciones:

Respecto al principio de legalidad que reclama que la ley describa el hecho típico de forma inequívoca (mandato de determinación, mandato de certeza) y trata de evitar la desformalización del control penal mediante el empleo de fórmulas generales, términos vagos o imprecisiones que no ofrecen suficientes y razonables criterios de determinación para establecer los límites de la intervención punitiva.[\[237\]](#)

Debemos señalar que el bien jurídico seguridad informática se encuentra en armonía con el referido aspecto material del principio de legalidad, en cuanto tiene como referente material las características propias de la seguridad informática, como son la autenticación que está vinculada a la identidad del usuario de la red y a la certeza que un usuario determinado ha llevado a cabo la operación informática de que se trate, la integridad que está en función a que la información o datos transmitidos o almacenados no han sido alterados, la confidencialidad referida a la protección de los datos respecto de accesos no autorizados.

Desde esta perspectiva, la construcción de los tipos penales del delito informático, podrá delimitar con precisión el ámbito de la intervención penal sin generar fricciones con el principio de legalidad.

Otro de los límites esenciales de la intervención punitiva se concreta en el carácter de ultima ratio de la sanción penal, en la medida que el Derecho penal debe desempeñar un papel limitado y excepcional en una política de protección, de ahí que se ha de tener en cuenta que no todo bien jurídico requiere tutela penal, ni todos los aspectos de un mismo bien jurídico requieren protección penal.

Tratándose la seguridad informática de un bien jurídico colectivo, se debe precisar que este tipo de bienes responde a relaciones sociales basadas en la satisfacción de necesidades de cada miembro de la sociedad o un ente colectivo y en conformidad al funcionamiento del sistema social.[\[238\]](#)

En este caso estamos frente a un bien jurídico referido al funcionamiento del sistema que tiende a asegurar materialmente las bases y condiciones del sistema, es decir, las relaciones macrosociales.

A su vez, cabe distinguir dentro de estos bienes aquellos bienes jurídicos institucionales que tienden a establecer mecanismos y procedimientos organizativos-conceptuales para asegurar los bienes jurídicos personales.[\[239\]](#) Ello no significa, sin embargo, que no son bienes autónomos, pues configuran una institución jurídica diferente de los distintos bienes individuales, de ahí que su titularidad esté referida a la colectividad.

Al respecto, debemos señalar que la seguridad informática está directamente en función de dos formas de “relación social” que se dan en la red y en los sistemas informáticos: el acceso a los mismos y el tránsito de la información. Ambos constituyen mecanismos organizativos de la actuación de los sujetos en la red y los sistemas informáticos.

Ahora bien, en cuanto al carácter de complementariedad que es propio de todos los bienes jurídicos colectivos, debemos afirmar que tras la seguridad informática deben ser claramente identificables los bienes individuales a los que sirve de tutela anticipada, la cual debe permitir graduar la intensidad de la protección penal de la seguridad informática, esto es, debe graduarse de acuerdo con los intereses personales a los cuales sirve de tutela anticipada.

Los bienes jurídicos individuales con los que está en relación de complementariedad la seguridad informática son el patrimonio, la intimidad, el honor, esto no debe significar que al momento de definirse la conducta de protección del delito informático se defina el resultado típico respecto de los bienes jurídicos individuales, pues la seguridad informática muestra un resultado material claramente reconocible necesitado de protección.

La configuración de la protección penal de la seguridad informática ha de estar en armonía con una concreta aplicación del principio de proporcionalidad y, en tal virtud, la gravedad de la sanción penal debe ser comparada con el contenido de desvalor típico del hecho ilícito; de ahí que sólo cuando entre los dos términos de la relación subsiste proporción, estaría justificada la conminación de la sanción penal, en caso contrario habría que acudir a instrumentos sancionatorios menos incisivos.

En el presente caso, tratándose de un bien jurídico colectivo estaría justificada la anticipación de la tutela a nivel del peligro cuando estén en juego bienes jurídicos fundamentales. La importancia social que ostentan actualmente la intimidad, patrimonio, honor, libertad de información resulta, a todas luces, suficiente para fundamentar su protección anticipada desde la seguridad informática.

Asimismo, no debemos dejar de lado que la intervención del Derecho penal en la protección de bienes jurídicos depende, además, del criterio de merecimiento de pena, esto es, del juicio de si un comportamiento concreto que afecta a un determinado bien jurídico debe, por la gravedad del ataque, por la propia importancia del bien jurídico ser sancionado penalmente, para lo cual el legislador ha de guiarse no sólo por criterios de justicia, sino también de oportunidad y utilidad social.[\[240\]](#)

Por último, la justificación de que la seguridad informática resulta un bien jurídico merecedor de protección se apoya en la trascendencia social que la red y los sistemas informáticos han adquirido en los últimos años, generándose una sensibilización de la opinión pública sobre esta materia y la necesidad de su protección.

Con respecto a la ley de delitos informáticos N° 27309 creemos que el legislador no ha determinado con claridad el bien jurídico protegido en los delitos informáticos, ya que parte de la confusión de lo que es la regulación misma de la red cuya competencia debe ser exclusiva del Derecho administrativo y termina por considerar como objetos jurídicos de protección bienes que son ajenos a las características propias de la red como es la intimidad y el patrimonio. Somos de la opinión que la aparición de nuevas leyes penales sin una adecuada regulación, puede originar la confusión y el peligro de arbitrariedades frente a una posible expansión de la jurisdicción penal para irregularidades que no son de su competencia.

Por nuestra parte, somos de la opinión que debido a los principios de Subsidiariedad, Lesividad y Última Ratio, el derecho a la seguridad informática debe ser considerado como bien jurídico penalmente relevante en la medida que su tutela y protección no son competencia del Derecho administrativo, pues éste se ocuparía sólo de una debida regulación de la red en cuanto a la

participación de los sujetos en la misma, como, por ejemplo, la regulación del envío indeseado de publicidad y el contenido mismo de la información almacenada, transmitida o puesta a disposición de los usuarios.

En definitiva, creemos que existe un bien jurídico penal respecto de las conductas definidas como delito informático, bien jurídico constituido por la seguridad informática, propia del funcionamiento de los sistemas y redes informáticas.

De esta manera podemos demostrar que la realidad exige una actitud diferente en cuanto a la percepción del bien jurídico protegido en los delitos informáticos, lo que conduciría a prevenir conductas ilícitas posteriores. Así, la realidad exige la creación de un nuevo bien jurídico propio de la red y sistemas informáticos diferente a la hasta hora ofrecida por los distintos órdenes jurídicos. Esto es, la seguridad informática.

Capítulo II

Posición personal respecto del concepto de delito informático

-
-
-
-

1.1 Posición personal respecto del concepto de Delito Informático

Luego del análisis realizado y como hemos podido ver, los denominados delitos informáticos constituyen una nueva categoría delictiva. Por tanto, el concepto de delito informático será el siguiente: “el acceso, utilización e interferencia indebidos a un sistema informático, base de datos, sistema, red de computadoras o a cualquier parte de la misma”.

Así, se excluyen todas aquellas conductas que a partir del uso de un sistema informático o de la red, lesionen bienes jurídicos como el patrimonio, la intimidad, el honor, etc. Debiendo quedar comprendidos los delitos informáticos bajo un nuevo título en nuestro Código penal, el mismo que deberá ser el de “Delitos contra la seguridad informática”.

Ahora bien, como hemos señalado en el punto 1.2 del Capítulo Segundo, Primera Parte, sobre las conductas nocivas que se cometen a través de sistemas informáticos y de Internet consideramos que -desde el punto de vista de la seguridad informática como bien jurídico protegido- podría distinguirse aquellas conductas que constituyen *per se* un delito informático por ser lesivas a la seguridad informática de aquellas que atentan contra el bien jurídico patrimonio, intimidad, honor, etc.

Así, por ejemplo, la conducta de “Introducción de Datos Falsos o Data Diddling” constituirá un delito informático, siempre que el agente haya ingresado, utilizado o interferido indebidamente a un sistemas. De lo contrario, será un delito de defraudación por medios informáticos, conducta que hasta el momento, no está recogida por nuestro Código penal. Por tanto, con base a las reflexiones anteriores, abogamos como propuesta de *lege ferenda*, la inclusión del inciso 5 en el artículo 197, la configuración del delito de defraudación informática en donde el tipo penal sería el siguiente: “El que, con el ánimo de procurar para sí o para otro un provecho ilícito, altere o modifique la configuración de algún programa, sistema, red de computadoras, base de datos u otro medio análogo en perjuicio del titular o de un tercero.”

En los casos que el agente no obtenga un provecho ilícito estaremos ante un delito informático en la medida que se trate de un ingreso indebido. En el supuesto caso que la persona tenga la autorización para ingresar al sistema y lo altere sin obtener un

provecho ilícito, dañando cualquier parte del sistema, nos encontraremos ante un delito de daños.

En cuanto a la conducta denominada como “Caballo de Troya” y el “Salame o Redondeo de Cuentas” consideramos que la diferencia respecto a la introducción de datos falsos es simplemente, las modalidades de alteración de los sistemas. Por tanto, resulta de aplicación los comentarios vertidos en el punto anterior.

Respecto a la conducta del “Superzapping” caracterizada por el uso no autorizado de un programa, constituye un delito informático en cuanto se trataría de una utilización indebida. Sin perjuicio de ello, podría configurarse también los delitos de daños, contra la intimidad, etc.

De otro lado, la conducta nociva denominada “Puertas Falsas” o “Traps Doors” se refiere básicamente a la copia indebida o no autorizada de archivos, programas con el fin de obtener un provecho ilícito. Por tanto, estaremos ante un delito informático y ante un delito patrimonial cuando se obtenga un provecho ilícito.

Las bombas lógicas se refieren a la introducción de programas a fin de borrar, alterar o destruir un programa o una base de datos. Comúnmente, es considerado el virus informático como bombas lógicas. En este caso, creemos que no se estaría ante un delito informático en cuanto, la introducción de una bomba lógica sea por medio de un correo electrónico, ya que no se estaría atentando contra la seguridad de un sistema, sino, contra los datos que el sistema posee. Por tanto, estaríamos ante un caso de daños. Por el contrario, cuando una persona ingrese indebidamente a un programa o a un sistema para introducir una bomba lógica, estaremos ante un delito informático y un delito de daños, en caso que haya perjuicio.

Los “Ataques Asincrónicos” -modalidades de ataques a un sistema o programa- constituyen igualmente un delito informático pudiendo tener una repercusión patrimonial.

Respecto al “Recojo de Información o Scavenging” consistente en aprovechar la información abandonada o depositada como residuo, consideramos que si para llegar a ella, se lleva a cabo un ingreso indebido al sistema, estaremos ante un delito informático. Si la información es recogida mediante el Scavenging físico, consideramos que no será un delito informático.

La conducta de “Divulgación No Autorizada de Datos o Data Leakage” -caracterizada por la sustracción de información- será un delito informático en cuanto el ingreso sea indebido y a la vez un delito de hurto, considerando a la información como un bien mueble.

Finalmente, el “Acceso a Áreas no autorizadas o Piggyn Banking”, la Suplantación de la Personalidad, el Interferencia de Líneas Telefónicas o Wiretapping y el Hurto de Tiempo” serán delitos informáticos debido a que todas estas conductas representan un ingreso indebido a un sistema informático. Ello, sin perjuicio de existir delitos posteriores como por ejemplo, delitos contra el patrimonio.

Si bien es cierto, que posiblemente se podrá dar un concurso real de delitos respecto al delito informático y el delito de daños o intimidad, etc., éste se podrá resolver desde la subsunción del delito informático -por ser el que menor pena tiene- o desde la calificación de delitos independientes, según la decisión de los aplicadores del Derecho. Como hemos podido ver, todas estas conductas nocivas que se comenten a diario, pueden ser castigadas desde la configuración de la seguridad informática como bien jurídico protegido en el delito informático, de ahí que resulte necesario considerar a la seguridad informática como bien jurídico penalmente relevante. De esta forma, no sólo se lleva a cabo una protección anticipada de bienes jurídicos individuales como pueden ser el patrimonio y la intimidad, sino también a través de la sanción penal de las conductas de ingresar, utilizar e interferir indebidamente una base de datos, un sistema o programa de computadoras, se ejerce una función preventiva respecto

a otras conductas más dañinas, significando una adecuada opción político criminal como la mejor forma de salvaguardar el patrimonio y la intimidad en el ámbito informático.

1.2 Clasificación de los Delitos Informáticos

Con respecto a la clasificación de los delitos informáticos, existen varios autores que han tratado de dar distintas clasificaciones para este tipo de conductas.

Así, algunos autores sostienen que "en todo delito de los llamados informáticos, hay que distinguir el medio y el fin. Para poder encuadrar una acción dolosa o imprudente dentro de este tipo de delitos, el medio por el que se cometan debe ser un elemento, bien o servicio, patrimonial del ámbito de responsabilidad de la informática y la telemática, y el fin que se persiga debe ser la producción de un beneficio al sujeto o autor del ilícito; una finalidad deseada que causa un perjuicio a otro, o a un tercero."[\[241\]](#)

-
Para SIEBER[\[242\]](#) la clasificación de los Delitos Informáticos se pueden agrupar en los siguientes puntos:

- a. Delitos de fraude mediante la manipulación de datos,
- b. Delitos de espionaje informático, piratería de software y sustracción de alta tecnología,
- c. Delito de sabotaje informático,
- d. Delitos de sustracción de servicios,
- e. Delitos de acceso indebido,
- f. Delitos de fraude fiscal relacionados con el computador.

Creemos que la clasificación antes mencionada se acerca en gran medida a entregar una cobertura de amplitud frente a la operación de distintos hechos delictivos informáticos.

Por su parte, TELLEZ VALDÉS [\[243\]](#) clasifica estas acciones en base a dos criterios:

- a. Como instrumento o medios, categoría en la que encuadra a las conductas que él llama “criminógenas que se valen de los ordenadores como método, medio o símbolo en la comisión del ilícito”,
- b. Como fin u objetivo, encuadrando en esta categoría a las “conductas criminógenas que van dirigidas en contra del ordenador, accesorios o programas como entidad física”.

De las principales clasificaciones que se manejan en la doctrina, podemos observar que se consideran delitos informáticos aquellas conductas en las cuales, el patrimonio o la intimidad son los bienes jurídicos. Como hemos visto anteriormente, esto no es tan cierto, las conductas idóneas para configurar un delito informático no han de estar en función de si lesionan el patrimonio o la intimidad, ya que ello sería una clasificación propiamente de los delitos patrimoniales o de los delitos contra la intimidad y estaríamos sólo distinguiendo modalidades de estos delitos en cuanto al empleo de medios informáticos para lesionar los referidos bienes jurídicos. Por lo tanto, nuestra clasificación de los delitos informáticos se centra principalmente en la idea de distinguir aquellas conductas que atenten contra la seguridad informática de redes o sistemas informáticos, las mismas que podrán ser identificadas a través de las dos características centrales del funcionamiento de los sistemas informáticos.

De ahí podemos distinguir dos niveles de conductas relevantes:

- a.- Conductas vinculadas a la fase de acceso a las redes o sistemas informáticos.
- b.- Conductas vinculadas al tránsito de la información a través de las redes o sistemas informáticos.

Desde esta perspectiva, la configuración de los delitos informáticos deberá permitir distinguir aquellas conductas referidas a los accesos indebidos o no autorizados a un sistema o red de computadoras y aquellas conductas referidas a la interferencia, interceptación, sustracción o manipulación de información en tránsito.

1.3 Principales manifestaciones de Delincuentes Informáticos

1.3.1 Piratas o Hackers

Conocidos también como “piratas informáticos”, personas que ingresan sin autorización a una computadora y exploran su interior. Para ellos no existe aparentemente un límite, pudiendo acceder por vía remota a servicios de noticias, servicios financieros, información financiera, instalaciones universitarias, correo electrónico, computadoras oficiales, etc.

Para SÁNCHEZ ALMEIDA, el *hacker* es la persona capaz de explorar un sistema hasta sus lugares más recónditos, en busca del conocimiento. [\[244\]](#)

1.3.2 Crackers

Es el típico *hacker* que no ingresa al sistema por curiosidad o porque le represente un reto para entender el funcionamiento de cualquier sistema. El *cracker* conscientemente ingresa a un sistema con la finalidad de destruir información. Existen dos tipos de *crackers*:

- a. El que ingresa a un sistema informático y roba información produciendo destrozos en el mismo.
- b. El que se dedica a desproteger todo tipo de programas, tanto para hacerlos plenamente operativas como para los programas que presentan anticopias.

1.3.3 Phreakers

Es el especialista en telefonía, el “pirata de los teléfonos”, sobre todo emplea sus conocimientos para poder utilizar las telecomunicaciones gratuitamente. Los principales perjudicados son los usuarios nacionales e internacionales y las compañías telefónicas. [\[245\]](#)

Por otro lado, todo parece indicar que las conductas antisociales por este tipo de personas se verán reducidas gracias a la iniciativa de la transnacional IBM que incorpora un chip de encriptación. Este chip tiene la misión nada menos que de proteger los datos de sus clientes contra asaltos informáticos. La habilidad de los mundialmente temidos *hackers* ha originado que los fabricantes de software se vean obligados a idear nuevas formas de protección que no puedan vencer por los *hackers*.

Según los especialistas que vienen desarrollando esta nueva forma de seguridad, se trata de atacar el problema de la seguridad basados en el hardware y no en el software, este chip estará capacitado para cifrar información con claves de 256 bits, que brindan un elevado grado de protección de datos y sistemas. Sin embargo, pareciera ser que estos personajes se valen de toda astucia para cometer sus fechorías utilizando hasta los medios de seguridad originados creados contra ellos, como, por ejemplo, el uso de la [criptología](#) por parte de los delincuentes, tanto para ocultar sus mensajes haciéndolos ininteligibles, como para ocultar sus propios movimientos en un sistema informático, haciendo incluso que aunque sean detectados no se pueda saber exactamente que es lo que estaban haciendo, al estar encriptados los archivos descubiertos. En este sentido, actualmente es muy inquietante la utilización de cripto-virus, los mismos que constituyen programas con códigos víricos encriptados.

Indudablemente, este tipo de delincuente tiene que ser sancionado penalmente por los delitos que produzca. Así, en las palabras de MARCHENA GOMEZ [\[246\]](#) “el delincuente informático que ve en la destrucción generalizada de sistemas

su objetivo, cualquiera que sea el móvil lúdico o vengativo que le impulse a ello, no puede seguir siendo considerado como un rebelde con aureola de vanguardia o como un simpático e introvertido muchacho que mata su tiempo libre retando a los diseñadores de los sistemas de seguridad en la red.”

Como hemos visto de los tipos de delincuentes informáticos, todos ellos necesitan del acceso a un sistema informático para poder realizar conductas ilícitas.

Por ello, nuestra posición en cuanto al bien jurídico en los delitos informáticos, ya que desde el momento en que se proteja la seguridad informática, se podrá sancionar a esta categoría de delincuentes cibernéticos y/o informáticos previniendo de manera adelantada la afectación de otros bienes jurídicos individuales como por ejemplo, la intimidad, el patrimonio, el honor, etc.

1.4 Tipología del “Delincuente Informático”

Como hemos visto al ocuparnos de las conductas lesivas en la red, los comportamientos pueden ser agrupados y clasificados por la doctrina, sucede lo mismo respecto de aquellos sujetos que los realizan, la doctrina viene discutiendo acerca de una posible tipología del delincuente informático.

Se ha de tener presente que para toda comisión de un hecho delictivo es necesario un sujeto activo, es decir, el autor o cómplice de la acción típica. La doctrina y la jurisprudencia tienden a denominar y clasificar a los autores de hechos delictivos de acuerdo al tipo de delito perpetrado, así, por ejemplo, homicida, estafador, etc. Por ello, las conductas ilícitas cometidas a través de las funciones de las computadoras son originadas por autores que devienen en ser llamados delincuentes informáticos. A este tipo de delincuentes también se le conoce como "ladrones de guante virtual" [\[247\]](#), en aras a distinguir la necesidad de conocimientos técnicos especiales por parte del agente.

Entendemos el concepto de delincuente informático como aquel individuo que realiza ataques a la seguridad informática; sin embargo, la tendencia de la doctrina es denominar delincuentes informáticos a aquellos sujetos que llevan a cabo conductas lesivas a la intimidad, patrimonio u honor a través del empleo de medios informáticos. Ello con la finalidad de poder destacar las características propias de las personas que llevan a cabo estas modalidades delictivas en relación con aquellos sujetos que cometen estos delitos desde otros medios.

Años atrás el sujeto activo de estos delitos era considerado como la persona que oscilaba entre los 15 y 30 años, de clase media, con una inteligencia dentro del promedio, que ingresaba a sistemas informáticos más que con un ánimo de lucro [\[248\]](#) o de dañar un sistema informático, con un afán de reto, de curiosidad y de superioridad por ingresar a sistemas que le eran ajenos.

Años más tarde se señalaba que el avance tecnológico desarrollaba cada vez más sofisticados sistemas de seguridad, que los sujetos activos ya no eran personas con un simple sentido de curiosidad, sino que, por el contrario, eran personas que poseían altos conocimientos en informática, con un nivel de inteligencia superior. Así, la doctrina argumentaba que los sujetos activos eran un 90% de los individuos que laboraban dentro de la empresa perjudicada.

Hoy en día la doctrina establece que los autores de conductas nocivas en sistemas informáticos no son ya personas que laboran en empresas, como anteriormente se señalaba, ya que uno puede desde su casa ingresar a cualquier sistema. En palabras de TIEDEMANN[249], actualmente los autores son usuarios normales. Igualmente BRAMONT-ARIAS[250], quien señala que ahora las personas no requieren tener grandes conocimientos de informática para cometer conductas delictuales en esta materia.[251]

Con respecto a este tema, somos de la opinión que debido al desarrollo tecnológico que cada día se acrecienta más, no tiene porque existir un *numerus clausus* en lo que se refiere al concepto de delincuente informático. Somos de la idea que mientras mayor seguridad en el ingreso a sistemas informáticos, mayor será el conocimiento especial que requerirá el delincuente informático, asimismo, a mayor expansión de Internet –a mayor crecimiento de la ciberpoblación en la red- mayor será la intervención del hombre medio. Por lo tanto, conductas que originen mayor impacto, estarán en relación a aquellas conductas que tengan mayor protección.[252]

En consecuencia, optamos por una tesis mixta que comprenda como delincuentes informáticos no sólo a sujetos con conocimientos especiales, que laboren o no dentro de la empresa afectada, sino también a personas normales, sin mayores conocimientos en informática que puedan cometer conductas nocivas a sistemas informáticos desde sus hogares. Así, pues, la red está siendo invadida por nuevos tipos de delincuentes. [253]

Por otro lado, en los casos de delitos informáticos los sujetos pasivos pueden ser tanto personas, como empresas, instituciones, gobiernos[254], etc., ya que la seguridad informática es un bien jurídico colectivo que está en función de todos y de cada uno de los miembros de la sociedad. Nos parece importante la clasificación que hace DE PABLO ORTIZ[255] de los delincuentes informáticos según su rol frente al sistema informático:

- a. Individuos con acceso autorizado al sistema: personas que conociendo las operaciones de la organización identifican las oportunidades para obtener un acceso fácil a los recursos informáticos y así cometer un delito.
- b. Individuos externos: que con los mismos objetivos que los anteriormente mencionados utilizan técnicas específicas para acceder a la información (ingeniería social, entre otras).

Como hemos señalado en la primera parte de la presente investigación, el elemento del anonimato como característica principal en la red, opera de un modo desfavorable para la persecución de los individuos en cuanto a la comisión de estas conductas. Así, una persona puede actuar con características distintas a las que originalmente posee, pudiendo alterar desde sus nombres hasta rasgos de su personalidad.

Otro problema que se adiciona es que la mayoría de los autores son jóvenes que poseen menos de 18 años, recordemos que fueron adolescentes de 16 y 17 años los que ingresaron en 1985 a los sistemas informáticos del Pentágono de los Estados Unidos, modificando y alterando información sobre la construcción de material de defensa y ubicación de satélites artificiales en el espacio. O el célebre caso Morris, en donde un joven interfirió los sistemas informáticos del Ministerio de Defensa, infectando con un virus más de seis mil computadoras oficiales que contenían valiosa información clasificada.[256]

Ahora, bien. Se ha señalado un punto importante: cuando un delincuente informático es menor de 18 años. Por razones de

seguridad jurídica y de política criminal, el legislador ha dejado fuera del Derecho penal a los menores de 18 años que cometen conductas criminales. Así, “el simple hecho de no haber cumplido la edad de 18 años, excluye de responsabilidad penal, aún cuando el desarrollo intelectual y volitivo del sujeto le permita comprender la significación ilícita de sus actos y obrar de acuerdo con esa comprensión (capacidad de comprensión o de encauzamiento), sometiéndolos a una legislación tutelar.”^[257] En este sentido, nos encontramos ante un problema de imputación, ya que como sabemos, aquellos individuos menores de 18 años no pueden ser sujetos activos de delito alguno. Problema, que el Derecho penal tendrá que solucionar ante el desarrollo y avance de la nueva criminalidad informática.

En definitiva, somos de la opinión que el delincuente informático en los denominados delitos informáticos no requiere de una calidad especial, pudiendo ser una persona con o sin amplio conocimiento en informática.

Capítulo III

Los delitos informáticos en el código penal peruano

1.1 Introducción

Años atrás era tal el desarrollo y avance tecnológico que el derecho positivo no lograba estar acorde con la necesidad de sancionar los ingresos indebidos a los sistemas informáticos, ni las manipulaciones a los mismos sistemas con fines nocivos o patrimoniales.

Podemos decir que por el delito de hurto, artículo 186 inciso 3 en la modalidad agravada, nuestro Código penal de 1991 empezó la preocupación por parte de legislador en incorporar delitos que estén acordes con las nuevas formas de criminalidad informática. En este precepto se establece que el hurto cometido mediante la utilización de sistemas de transferencia electrónica de fondos, de la telemática en general, o la violación del empleo de claves secretas, será reprimido con privación de libertad no menor de cuatro ni mayor de ocho años.

Evidentemente, como señala REYNA ALFARO^[258], el fenómeno informático no podía ser abarcado a través de un solo tipo penal patrimonial, por lo que el legislador peruano se ve en la necesidad de buscar una solución a este problema, optando por la configuración de los delitos informáticos en nuestro Código penal. Debido a ello, resulta conveniente comentar brevemente en esta introducción el artículo 186 inciso 3 del Código penal.

Sin lugar a dudas, se trata de un delito contra el patrimonio que toma como punto de partida el tipo básico del delito de hurto contenido en el artículo 185 del Código penal. El delito de hurto se caracteriza por el apoderamiento ilegítimo de un bien mueble, total o parcialmente ajeno, sustrayéndolo del lugar donde se encuentre. El objeto material sobre el que recae este delito es un bien mueble.

En palabras de MUÑOZ CONDE^[259], por bien mueble, se puede entender, como todo objeto del mundo exterior con valor económico, que sea susceptible de apoderamiento material y de desplazamiento. Esta definición nos condiciona el objeto de la acción, en la medida que resultaría discutible que los datos y la información puedan ser equiparados a los bienes muebles, de

allí ya se advierte su insuficiencia para afrontar las formas actuales de criminalidad informática.

Sin embargo, creemos que la información al tener un valor económico para su titular, es considerada un bien mueble y está comprendida dentro del artículo 886 del Código civil[260]. Máxime si, como hemos visto anteriormente, lo importante para los sistemas informáticos es la información almacenada en soportes lógicos.

Por otro lado, en cuanto a la sustracción del bien mueble del lugar donde se encuentra, se advierte que sólo podría comprenderse el retiro de datos o información en el supuesto que fueran considerados bienes muebles, más no su copia o alteración.

Con respecto a las sustracciones de dinero que se perpetren mediante cajeros automáticos, el dinero, determinado éste como un bien mueble, constituirían delito de hurto agravado, tipificado en el artículo 186 inciso 3 del Código penal peruano. Por ello, este delito ha de ser comprendido como un delito contra el patrimonio, en concreto como una modalidad del delito de hurto mediante sistemas informáticos, en el cual se protege el patrimonio.

Se trata, en definitiva, de una forma agravada del delito de hurto caracterizada por el uso de sistemas de transferencia electrónica de fondos, la telemática en general y la violación de claves secretas.

La criminalidad informática, como se ha podido observar a lo largo de la primera parte de la presente investigación, este tipo de criminalidad es de reciente aparición, sin embargo, en el año 1999 se había registrado 14 mil 826 ataques de los piratas del ciberespacio en todo el mundo[261]. En el Perú[262] se había registrado 27 de estas transgresiones. [263]

En nuestro medio, el ingreso indebido de un *hacker* a la página web de la Oficina Nacional de Procesos Electorales (ONPE) fue determinante para la elaboración de un proyecto de ley que encuadre las conductas delictuales del ciberespacio en el Código penal. [264]

Al respecto, muchos especialistas, tanto en Derecho penal como en otras ramas del Derecho, exigían una sanción acorde para estas conductas indebidas.[265] Asimismo, en el resto del mundo, organizaciones como la Organización de Estados Americanos, la Unión Europea, la Organización para la Cooperación y el Desarrollo Económico, Universidades y la INTERPOL vienen buscando una solución óptima para castigar éste tipo de conductas antisociales.

La respuesta de nuestros legisladores[266] no se hizo esperar más y se elaboró el correspondiente Proyecto de Ley, el mismo que a su tenor establecía lo siguiente:

Artículo Único.- Incorpórese al Código penal, promulgado por Decreto Legislativo N° 635, el Capítulo XI, Delitos Informáticos, los artículos 208A y 208B; con los siguientes textos:

Artículo 208A.- El que indebidamente utilice o ingrese a una base de datos, sistema o red de computadoras o a cualquier parte de la misma, con el propósito de diseñar, ejecutar, copiar o alterar un esquema o artificio con el fin de defraudar, obtener dinero, bienes información será reprimido con pena privativa de la libertad no menor de dos años, o con prestación de servicios comunitarios de cincuentidós a ciento cuatro jornadas.

Artículo 208B.- El que indebidamente, interfiera, reciba, utilice, altere, dañe o destruya un soporte o programa de computadora o los datos contenidos en la misma, en la base, sistema o red será reprimido con pena privativa de la libertad no mayor de dos años.

Así, lo que se sugería con el mencionado Proyecto de Ley era incorporar el Capítulo XI, Delitos Informáticos y los artículos 208-A y 208-B.

El artículo 208-A planteaba el ingreso indebido, con el fin de diseñar, ejecutar, copiar o alterar un esquema o artificio y defraudar, obtener dinero, bienes o información, mientras que el artículo 208-B proponía sancionar a aquel que indebidamente interfiera un sistema informático con la finalidad de dañarlo.

Luego, a finales del mes de mayo del año 2000, el Perú estaba a punto de sentar un precedente entre los países latinoamericanos con una legislación que tipifica el uso indebido de soporte electrónico para alterar o sustraer información.^[267] Las epidemias informáticas causadas por virus que destruyen a su paso archivos de todo tipo^[268], páginas web peruanas que son desde hace varios años blanco de ataques perpetrado por “hackers” peruanos y extranjeros^[269], la vulneración de sistemas informáticos por personas que ingresan indebidamente, la sustracción de información almacenada, etc., originaron que nuestros legisladores hayan optado por la tipificación de estas conductas delictuales, dictándose la ley correspondiente.

1.2 Ubicación Sistemática

Con fecha 17 de julio del año 2000, el Congreso de la República promulga la Ley N° 27309, ley que incorpora los delitos informáticos al Código penal. Así, con ésta innovadora ley se crea, pues, el nuevo mundo de los delitos informáticos, desconocidos hace más de un par de décadas atrás.

En su artículo único la ley modifica el Título V del Libro Segundo del Código penal, promulgado por el Decreto Legislativo N° 635, e incorpora los artículos 207-A, 207-B y 207-C en los siguientes términos:

"Artículo 207-A. 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 cincuentidós 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.

"Artículo 207-B.- 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 la libertad no menor de tres ni mayor de cinco años y con sesenta a noventa días multa."

"Artículo 207-C.- En los casos del artículo 207-A y 207-B, la pena será privativa de la 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."

Con estos artículos el legislador peruano incorpora al Código penal de 1991 las figuras delictivas denominándolas "delitos informáticos". Las modalidades incorporadas son: intrusismo informático, fraude informático y daño informático.

Llama la atención que el legislador haya decidido ubicar los delitos informáticos dentro de los delitos contra el patrimonio, sin considerar que se incluye la protección de la intimidad en una de sus modalidades. La razón parece haber sido aglutinar en un solo capítulo el empleo de los medios informáticos sin importar la afectación de distintos bienes jurídicos.

1.3 Análisis de la Ley N° 27309- "Ley de Delitos Informáticos"

Luego de todo lo expuesto, pasaremos a analizar los delitos informáticos en nuestra legislación penal. No es nuestro ánimo realizar una crítica sobre los problemas sistemáticos en que el legislador ha incurrido en la elaboración de dicha ley o en la falta de conocimientos jurídico-penales, sin embargo, su correspondiente análisis constituirá el inicio para la consagración de la debida protección penal de la seguridad informática, para que de este modo se puedan realizar modificaciones a la Ley N° 27309 - "Ley de Delitos Informáticos", las mismas que creemos que son necesarias.

1.4 Delito de Intrusismo Informático- Art. 207-A

El delito de intrusismo informático es conocido también por la doctrina internacional como el "*Hacking*" o "*Hacking lesivo*".[\[270\]](#)

Como se ha podido apreciar en el punto de la ubicación sistemática, podríamos decir que el bien jurídico protegido en este delito es el patrimonio, la intención del legislador pareciera haber sido la configuración de un delito de peligro abstracto. Sin embargo, de la lectura del tipo penal se puede advertir que el bien jurídico protegido en este delito no es el patrimonio, sino más bien, preliminarmente, la intimidad. Ello debido a que en el tipo no se exige que el sujeto tenga la finalidad de obtener un beneficio económico, este requisito es constitutivo de la modalidad agravada, más no de la conducta delictiva descrita en el tipo básico[\[271\]](#), ya que el legislador considera el mero ingreso no autorizado como afectación a la intimidad.

No obstante, consideramos que el bien jurídico protegido en el tipo penal del artículo 207-A es la seguridad informática, ya que la conducta descrita se refiere a la utilización o ingreso indebido a una base de datos, sistema o red de computadoras, lo cual está en relación a la afectación de la seguridad informática y no el patrimonio o la intimidad, en cuanto se lesiona una de sus manifestaciones como es el acceso o su utilización indebidos.

Es necesario señalar que el objeto material de la conducta realizada (no la que tiene en mente el agente) es la base de datos, sistema o redes informáticas. Desde esta perspectiva, debemos reconocer que el carácter complementario del bien jurídico seguridad informática no implica que los delitos que se configuran para protegerlo hayan de vincularse en su construcción típica con aquellos bienes jurídicos individuales complementados; a ello se ha de agregar que la protección de la seguridad informática no equivale a la protección de la suma de bienes jurídicos individuales, sino de aquellas condiciones que permiten garantizar en el caso concreto su indemnidad como objeto diferenciado y anticipado de tutela y única forma posible de prevenir su lesión en la red y en los sistemas informáticos.[\[272\]](#) Con respecto a la conducta típica, ésta comprende el hecho de utilizar o ingresar indebidamente a una base de datos, sistema o red de computadoras.

Por el término "indebidamente" podemos entender el ingreso o la utilización de manera indebida o ilícitamente.[\[273\]](#) El

término “indebido” se refiere a lo injusto, ilícito y falto de equidad.^[274] El carácter indebido adjetiviza las conductas de ingresar o utilizar una base de datos, sistema o red de computadoras, lamentablemente el legislador penal no ha tomado en la promulgación de la ley el hecho que aún no se ha regulado el ingreso o no debidos de la red, por lo que se encuentra vacío de contenido material este precepto, ya que no se ha dicho nada al respecto; no obstante podemos señalar que una de las características del carácter indebido de la conducta será la falta de autorización para el ingreso o utilización de la red o sistemas informáticos. El carácter indebido califica, precisamente, la conducta constituye un elemento del tipo, por lo que su ausencia no ha de ser apreciada como causa de justificación sino de atipicidad.

Al respecto, BRAMONT-ARIAS^[275] hace una descripción de los verbos típicos que se encuentran comprendidos en el artículo 207-A. Así, el verbo ingresar esta referido a entrar a una base de datos, sistema o red de computadoras. El verbo utilizar, por su parte, hace referencia al uso de la base de datos, sistema o red de computadoras.

Este caso se aplicará cuando el sujeto activo no ingresa indebidamente a la base de datos o red de las computadoras, ya que en estos casos se aplica el supuesto anterior, sino cuando el sujeto activo se encuentra ya dentro de la base de datos o red y comienza a utilizarla sin autorización, por ejemplo, la persona, en un descuido de un trabajador de la empresa que ha dejado encendida su computadora porque se ha ido a su refrigerio, se aprovecha para utilizar la base de datos o el sistema. Para todos estos casos, se requiere que no se tenga la autorización debida, ya que el tipo señala "el que utiliza o ingrese indebidamente". Se trata de un delito de mera actividad, siendo suficiente la realización de las conductas descritas en la norma sin que concurra un resultado externo.

Ello no obsta a que afirmemos que respecto del bien jurídico seguridad informática las conductas descritas en el artículo 207-A producen su lesión, por lo que sostenemos que se trata de un tipo penal de lesión y no de puesta en peligro. En efecto, para la lesión de la seguridad informática sería suficiente que el agente haya ingresado o utilizado indebidamente una base de datos o sistemas informáticos sin la necesidad de otro tipo de ánimo adicional.

Distinta es la configuración actual del artículo 207-A, en cuanto el legislador vincula la norma a la protección de bienes jurídicos individuales como la intimidad y el patrimonio, para lo cual configura el tipo penal como delito de peligro abstracto, lo cual creemos que no es necesario a partir de reconocer a la seguridad informática como bien jurídico protegido en el delito de intrusismo informático.

Por otra parte, se trata de un delito doloso, se requiere que el agente actúe con conciencia y voluntad de ingresar o utilizar el elemento informático indebidamente. El sujeto ha de ser conciente del carácter indebido de la conducta, ya que este es el sustento central de la conducta prohibida.

El desconocimiento por parte del sujeto acerca del carácter indebido de la conducta realizada constituye un error de tipo vencible, cuya solución a tenor de lo establecido en el artículo 14 del Código penal será la aplicación del tipo penal culposo, pero debido a una inexistencia deberá excluirse de toda sanción penal.

En el artículo 207-A si bien se sanciona la utilización o ingreso indebido a una base de datos o sistema informático, con la finalidad de diseñar, ejecutar, interferir, interceptar, existirán problemas para distinguir el denominado "*Hacking* blanco", máxime cuando el propio legislador concibe como finalidad del ingreso el acceso, luego no puede darse una conducta de ingresar para acceder. No obstante, debemos señalar que en cuanto al aspecto subjetivo, el primer párrafo del artículo 207-A exige las finalidades antes descritos como elementos subjetivos de intención trascendente, no siendo necesario su realización material.

Al considerarse dentro del carácter indebido de la conducta al hecho de no contar con autorización, el consentimiento del

titular del sistema, base de datos o red de computadoras constituye causa de atipicidad.

El segundo párrafo del artículo 207-A contempla una modalidad agravada del intrusismo informático, en la medida que sanciona el ingreso o utilización indebida de una base de datos o sistema informático con el fin de obtener un beneficio económico.

Sobre los sujetos activos de esta figura penal, BRAMONT-ARIAS[276] opina que cualquier persona puede cometer este ilícito penal y que no requiere tener grandes conocimientos de informática.

Por lo tanto, el sujeto activo puede ser cualquier persona mientras que el sujeto pasivo puede ser una persona natural y en el supuesto del último párrafo del artículo 207-A, una persona natural y una persona jurídica.

En el aspecto subjetivo necesariamente este tipo de delito exige el dolo del sujeto activo, ya que se requiere en el sujeto conciencia y voluntad de utilizar o ingresar indebidamente a una base de datos o sistema informático. Para la modalidad agravada se ha de exigir además del dolo, la concurrencia de una finalidad económica en la realización de la conducta.

Se ha de advertir que el legislador acude a la fórmula de los elementos subjetivos de intención trascendente, los cuales establecen una finalidad específica cuya realización material no es exigida por el tipo penal, bastando sólo que el sujeto la persiga. Lo cual está acorde con la elaboración por parte del legislador nacional de los delitos informáticos como delitos de peligro abstracto.

Por ello, las acciones de ejecutar, alterar, interceptar, interferir o copiar la información o la de obtener un beneficio económico, no son exigidas en cuanto a su realización material, basta que constituyan las finalidades queridas por el autor.

Por otra parte, bien hace en señalar BRAMONT-ARIAS[277] la relación existente entre el artículo 207-A segundo párrafo y el artículo 186 inciso 3 en la modalidad agravada en el caso de una persona que descubre el password de otra, e ingresa al sistema, copia información y luego la vende a una empresa de la competencia obteniendo un provecho económico, por lo que se generaría un concurso de delitos. El referido autor considera que en estos casos, el tipo penal aplicable sería el delito de hurto agravado en la medida que entre ambos existe un concurso aparente de leyes, el cual se solucionaría a través de las reglas de la consunción, dado que, en este caso, el delito de resultado, es decir, el hurto agravado, absorbería al delito de peligro, es decir, al delito informático.

Desde la concepción de la seguridad informática como bien jurídico protegido en el delito informático, se ha de precisar que no se deberá acudir al empleo de elementos subjetivos de intención trascendente que pretendan vincular la conducta realizada con los bienes jurídicos intimidad y patrimonio, ya que las conductas objetivamente descritas en el artículo 207-A son suficientes para su lesión. De ahí que aquí abogemos de *lege ferenda* por la eliminación de tales elementos subjetivos y la configuración del delito de intrusismo informático vinculado a la afectación de la seguridad informática, ejerciendo así una protección adelantada de los mencionados bienes jurídicos individuales. Ello no obsta a que pueda configurar tipos penales específicos que sancionan la lesión del patrimonio o la intimidad a través de medios informáticos.

1.5 Delito de Daño Informático - Art. 207-B

El delito de daño informático es conocido también como “sabotaje informático”.

Creemos que en principio, el artículo 207-B ha sido adecuadamente comprendido en los delitos contra el patrimonio, ya que la conducta es la de ingresar o utilizar un sistema para dañarlo o alterarlo, por lo tanto, el bien jurídico protegido es en este caso el patrimonio, representado por el valor económico que encierra un sistema o programa de computadoras.

Al igual que en el artículo 207-A, la intención del legislador ha sido configurar este delito como delito de peligro abstracto, en cuyo caso, para una mejor configuración típica del mismo, deberá sancionarse la lesión efectiva al patrimonio, de esta forma se hallaría una mayor armonía con los principios de lesividad y proporcionalidad.

De acuerdo al texto vigente del artículo 207-B el bien jurídico protegido resulta ser la seguridad informática, pues las conductas descritas son las mismas que las del artículo 207-A, salvo el caso de la interferencia, variando únicamente la intención trascendente exigida al autor.

En efecto, el delito de daño informático comprende las conductas de utilizar, ingresar o interferir (una nueva conducta a diferencia del artículo 207-A) indebidamente una base de datos, sistema, red o programa de computadoras o cualquier parte de la misma con el único ánimo de alterarlos, dañarlos o destruirlos.

El verbo que se adiciona a diferencia del artículo 207-A es el "interferir", es decir, la persona que no permite la utilización o comunicación adecuada dentro del programa o sistema informático.[\[278\]](#)

En cuanto al empleo del término “indebidamente”, resulta aquí de aplicación los comentarios expuestos con relación al artículo 207-A.

El sujeto activo, al igual que el artículo 207-A, puede ser cualquier persona natural, así como el sujeto pasivo será el titular del bien afectado. Igualmente, en el aspecto subjetivo tenemos al dolo sumado al ánimo de dañar, destruir o alterar la base de datos o sistema informático, que constituye un elemento subjetivo de intención trascendente, cuya realización material no es exigida por el tipo penal.

Según BRAMONT-ARIAS[\[279\]](#), la diferencia entre los artículos 207-A y 207-B gira

en torno al aspecto subjetivo, esto es, la finalidad que tienen el sujeto activo al

momento de realizar su conducta, ya que si una persona es detenida en el

momento que está utilizando sin autorización una base de datos, para poder determinar que tipo penal se aplicaría, habría que preguntarse cual es su intención en ese momento, es decir, si la persona quiere destruir se le aplicará el artículo 207-B, en caso contrario, habría que demostrar alguna de las finalidades previstas en el artículo 207-A.

Por otro lado, respecto de este delito existirá el problema acerca de los elementos de prueba para determinar la intención del delincuente informático, ya que sino se puede determinar el ánimo del sujeto activo, estaremos ante un delito de mero intrusismo informático con una pena no mayor de dos años, de lo contrario, nos encontraríamos en el caso del delito de daño informático, con una pena no mayor de cinco años. Respecto a este punto, creemos que el legislador ha debido determinar la alteración, daño o destrucción de sistemas informáticos como consumación del delito.

En este sentido, entendemos que para estos supuestos es perfectamente de aplicación el artículo 205 del Código penal, en la medida que el objeto material es amplio y no excluye a los sistemas informáticos, redes o programas de computadoras.

Desde este orden de ideas, sería suficiente el tipo penal del artículo 207-A que recoge las conductas de utilizar e ingresar, añadiéndose la de interferir, pues todas ellas lesionan la seguridad informática, quedando el tipo penal del delito de daños previsto en el artículo 205 del Código penal para una lesión efectiva del patrimonio representado por el valor económico que contienen las redes o sistemas informáticos y los programas de computadoras.

Por último, podemos advertir el concurso de delitos que se daría, desde esta perspectiva, entre el delito de intrusismo informático y el delito de daños del artículo 205 del Código penal, en la medida que para la realización de la conducta de daños se haya llevado a cabo un acceso o utilización indebida. Así, se trataría de un concurso real de delitos debido a tratarse de hechos independientes y a la afectación de dos bienes jurídicos distintos.

Es oportuno hacer una breve referencia en cuanto a la pena que se establece en este delito. REYNA ALFARO[280] opina que en el presente supuesto el legislador ha debido incluir la inhabilitación como pena principal. Sin embargo, para el referido autor, esta posibilidad queda abierta para que en una sentencia, el Juez Penal fije la inhabilitación como pena accesoria según lo dispuesto por el artículo 39 del Código penal.[281]

1.6 Delito Informático Agravado - Art. 207-C

En el artículo 207-C de nuestro Código penal se establecen dos agravantes; la primera en función al cargo que posee el sujeto activo, la segunda, en razón a la seguridad nacional.

Se establece como agravante si la persona se aprovecha de la información que obtiene por la función que desempeña. Esta agravación está en relación a la confianza depositada en la persona del autor y al manejo de determinada información, como pueden ser claves de acceso, passwords, etc.

Evidentemente, para este supuesto resulta de aplicación la exigencia de los tipos penales de los artículos 207-A y 207-B acerca del carácter indebido de la conducta, el mismo que no ha de verificarse respecto de la obtención de la información privilegiada, ya que ello no es lo prohibido por el artículo 207-C, pues se sanciona su abuso o aprovechamiento, sino de las propias conductas descritas en los referidos tipos penales.

Ello nos permite afirmar que las agravantes descritas en el artículo 207-C parten de la afectación a la seguridad informática. Creemos que aquí se incurriría en una confusión, creándose un concurso de delitos respecto del delito de abuso de información privilegiada tipificado en el artículo 251-A de nuestro Código penal.[282]

En todo caso, los puntos de coincidencia entre el tipo penal del artículo 251-A y los delitos informáticos sólo serían respecto del segundo párrafo del artículo 207-A, en cuanto el sujeto actúa con el fin de obtener un beneficio económico; ahora bien, atendiendo al principio de especialidad se debería optar por el tipo penal del 207-A en aquellos casos que se hubiera realizado la conducta mediante la utilización o ingreso indebido a una base de datos, sistema o red de computadoras.

En cuanto al aspecto subjetivo, esta agravante deberá comprender el dolo previsto para los artículos 207-A o 207-B y, adicionalmente, el ánimo del agente respecto del preavalecimiento de la función que desempeña.

En cuanto al segundo inciso del artículo 207-C, el tipo penal agravado parte de la realización de las conductas descritas en los artículos 207-A y 207-B, estas son, utilizar, ingresar o interferir indebidamente una base de datos, sistema, red o programas de computadoras, tales conductas han de estar vinculadas a la seguridad nacional, pues se sanciona, precisamente, su puesta en peligro.

Aquí, si podrían entrar en consideración en cuanto de la realización de las conductas materiales exigidas por los artículos 207-A y 207-B, todas aquellas normas que regulan y protegen la seguridad nacional, tanto desde la Constitución Política, como leyes especiales y reglamentos.

En cuanto al aspecto subjetivo de la conducta, el dolo del autor deberá referirse a la conciencia y voluntad de poner en peligro la seguridad nacional.

1.7 Aspectos problemáticos de la tipificación de los delitos informáticos en la legislación penal peruana.

Como se puede desprender de los delitos enunciados y por cruda que parezca la realidad, la nueva ley carece de temas tan elementales como, por ejemplo, la delimitación del bien jurídico protegido. Del análisis de la Ley N° 27309 -sobre Delitos Informáticos- se presentan muchos cuestionamientos debido a la gran cantidad de inexactitudes que ésta contiene, tanto conceptuales, gramaticales y relativas a los principios generales del Derecho penal.

-
Con un afán eminentemente técnico, veremos los desaciertos en que el legislador peruano ha incurrido en cuanto a la tipificación de las conductas nocivas en la red, denominadas por éste como “delitos informáticos”.

1.7.1 Exceso del uso de elementos subjetivos en los tipos penales informáticos.

El legislador al momento de configurar la tipicidad de los delitos informáticos utiliza como aspecto subjetivo de la conducta tres tipos de finalidades que han de ser perseguidas por el autor, como por ejemplo, diseñar, ejecutar, alterar, interferir, interceptar, acceder o copiar (art. 207-A, primer párrafo). Luego, la obtención de un beneficio económico (art. 207-A, segundo párrafo). Y por último, alterar, dañar o destruir (art. 207-B).

Estas finalidades difícilmente podrán ser apreciadas en la realidad, toda vez que las conductas descritas en cuanto a su aspecto objetivo, son exactamente las mismas, con la salvedad de la conducta de interferir recogida en el artículo 207-B. Por consiguiente, todas estas finalidades quedan en la cabeza del autor, lo cual genera serios problemas probatorios en el marco de un proceso penal, pues deben concurrir no solamente el aspecto objetivo de la tipicidad, sino también su aspecto subjetivo que comprende el dolo y los mencionados elementos subjetivos de intención trascendente. Así, difícilmente podremos distinguir entre el sujeto que ingresa indebidamente a una base de datos, con la finalidad de copiar información de aquel que ingresa indebidamente con el fin de destruir un programa.

Como hemos visto al revisar los delitos informáticos en nuestra legislación, el legislador ha optado por el empleo de elementos subjetivos de intención trascendente, cuya realización fáctica no es necesaria, sino sólo que sean la finalidad perseguida por el autor.

Esto trae consigo problemas de adecuación típica, ya que difícilmente podrá distinguirse entre un acceso indebido con ánimo de lucro de aquel en que el sujeto persigue causar un daño, si es que no media fácticamente un elemento adicional al mero acceso. Esta situación obedece fundamentalmente a que el legislador ha optado por configurar los delitos informáticos como

delitos de peligro abstracto para bienes jurídicos como el patrimonio y la intimidad.

Como hemos observado anteriormente, este problema se supera a partir de concebir a la seguridad informática como bien jurídico en estos delitos, brindándose una protección antelada a bienes jurídicos individuales. Desde este orden de ideas, resultará innecesario acudir a los elementos subjetivos de intención trascendente en la medida que se exige al autor únicamente el dolo de ingresar, utilizar o interferir indebidamente una base de datos, sistema informático o programa de computadoras.

El artículo 207-A, tal y como ha sido creado por el legislador, está configurado como un delito de peligro abstracto para los bienes jurídicos intimidad y patrimonio y emplea como elemento subjetivo de intención trascendente que el sujeto persiga el ánimo de afectarlos, por lo que sólo puede afirmarse el dolo de ingresar o utilizar indebidamente un sistema o red de computadoras sin que a través de tales de conductas pueda inferirse el ánimo trascendente a la acción perseguido por el sujeto. Desde esta perspectiva, existe inconvenientes para sancionar a un individuo que por pura curiosidad ingresa indebidamente a un sistema informático o a alguna base de datos, sin causar ningún daño o perjuicio para un tercero.

Si bien esta conducta no afecta ni pone en peligro inminente a la intimidad o al patrimonio, consideramos que sí lesiona la seguridad informática, por lo que desde las tesis aquí sostenida debe ser materia de sanción por el Derecho penal. Esta afirmación no es del todo aceptada por la doctrina.

Así, SÁNCHEZ ALMEIDA[283] entiende que para que pueda ser penado el *Hacking*, éste debe estar orientado a la obtención de secretos, o bien a la causación de daños. El acceso en sí mismo a un sistema no puede ser considerado a priori como delito, si no se dan los requisitos, objetivos y subjetivos, que configuran los tipos penales correspondientes. Desde este orden de ideas, si el acceso a un sistema se realiza sin ánimo de descubrir secretos, vulnerar la intimidad de otro, o causar daños, no puede ser penado, y ello porque no existe un precepto penal que castigue el acceso a un sistema en sí mismo, con el único y exclusivo ánimo de aprender como, por ejemplo, el *Hacking* blanco.

En el mismo sentido se señala que la apología del *Hacking* es impune cuando se elabora y publica una página web en la que se haga elogio en abstracto del *Hacking* o de determinados *hackers*, ya que, a su entender, el Código español sólo castiga la apología como forma de provocación o de incitación directa a cometer un delito. Consideramos que la tipificación en materia penal de la conducta de *Hacking*, evita la impunidad de otros hechos de mayor entidad difíciles de probar.[284] En la misma posición, RIQUERT[285] quien señala que los estudios criminológicos realizados en otros países con más experiencia en la materia demuestran que comportamientos inicialmente de mero intrusismo informático -detectados pero no reprimidos en su momento-, terminaron convirtiéndose en otros ilícitos muchos más graves, como fraudes, espionaje, sabotaje, atentados contra la intimidad, etc. Se argumenta en este sentido que castigando el *Hacking* se adelanta la barrera de protección frente a hechos más graves (se habla así, de una suerte de delito barrera o delito obstáculo). Igualmente, LLANEZA GONZÁLES[286] expresa que “no podemos estar de acuerdo con Sánchez Almeida cuando mantiene que ha de haber apoderamiento de los datos de carácter personal para que haya punición, ya que el último inciso del artículo 197.2 castiga a los que accedan por cualquier medio y de manera in consentida a los datos personales de un tercero”. Por tanto, el mero acceso es delictivo y el *Hacking* blanco, a nuestro entender, siempre que se acceda a datos de carácter personal, es punible. Cabría preguntarse si la acción del *hacker* borrando sus huellas del fichero de “logs”, para ocultar cualquier referencia a su acceso, es una modificación punible. Parece que no, ya que no se modifican datos de carácter personal de un tercero sino, curiosamente, del propio *hacker*.

Por último, se sostiene también que el hecho de entrar a un sistema no genera necesariamente un daño. Al respecto, SÁNCHEZ ALMEIDA[287] señala que “el hecho de entrar a un sistema, por sí mismo, ya genera un daño: el que sufre el administrador al descubrir que su sistema es inseguro, con las consiguientes horas de paranoia invertidas en la búsqueda de la invulnerabilidad.

Así, la respuesta se encuentra en la misma pregunta: si el sistema era ya inseguro, esa inseguridad no la ha creado el *hacker*, y en consecuencia no cabe hablar de daño, pues el deterioro que debería de sufrir la cosa dañada es preexistente a la acción del intruso. Sólo podemos hablar de un daño si existe la destrucción de datos, o alteración de los mismos, por tanto, la situación de inseguridad no ha sido creada por el *Hacking* blanco, sino por una administración negligente, que no ha podido proteger sus sistemas o por la irresponsabilidad de los diseñadores de los sistemas operativos.”

Sin embargo, esta afirmación esta vinculada con una perspectiva materialista del daño y parte por admitir que sólo habría daño en la medida de una afectación al patrimonio, mediante la destrucción del sistema o a través de la causación de un perjuicio económico. Desde la tesis sostenida acerca del bien jurídico seguridad informática y su relación respecto de los bienes jurídicos como el patrimonio o la intimidad, podemos afirmar que el ingreso o su utilización indebidos de una base de datos, redes o sistema informáticos constituyen ya su afectación, por lo que se genera un perjuicio.

En definitiva, este problema puede superarse desde la perspectiva del bien jurídico seguridad informática, pues permite delimitar en cuanto a las funciones de acceso al sistema y transmisión de información, cuando nos encontramos frente a una conducta de intrusismo con relevancia penal. De allí que abogemos por la configuración del tipo penal de intrusismo informático en referencia a la seguridad informática como delito de lesión y no de puesta en peligro abstracto respecto del patrimonio y la intimidad.

Sin perjuicio de sancionarse, en este orden de ideas, la afectación efectiva de tales bienes y no su puesta en peligro, en el delito de intrusismo -cuyo bien jurídico constituye la seguridad informática- deberían erradicarse aquellos elementos subjetivos de intención trascendente, quedando como una protección anticipada de bienes jurídicos individuales, dada su naturaleza de bien jurídico colectivo.

1.7.2 El Principio de Territorialidad

Para determinar la competencia de los Estados en la persecución de los delitos se atiende al lugar de su comisión. A esta competencia se la denomina Principio de Territorialidad, el mismo que se encuentra contenido en el artículo 1 del Capítulo I de la Parte General de nuestro Código penal.[\[288\]](#)

Para MUÑOZ CONDE y GARCÍA ARÁN[\[289\]](#), el Estado es competente para sancionar, con arreglo a las leyes propias, los hechos cometidos en su territorio (*locus regit actum*), independientemente de la nacionalidad de quien los haya cometido.

Respecto a este apartado, somos de la opinión que se originarán una serie de problemas con relación a los delitos informáticos, para determinar el lugar de comisión del hecho delictuoso. Como hemos visto anteriormente, se pueden cometer conductas nocivas para sistemas informáticos desde el otro lado del mundo, como desde el vecino de al lado.

Así, no existirá mayor problema cuando el delito sea cometido en territorio peruano. Sin embargo, cuando la comisión del delito sea en un país extranjero, será difícil determinar si la acción y la afectación a la seguridad informática se produjeron en el mismo lugar o no.

A modo de ejemplo, que sucedería en el caso de un malicioso *hacker* japonés que ingrese a un sistema informático desde Arabia Saudita y envía desde allí un virus informático al gobierno de Estados Unidos. Se podría llegar a decir que el delito se ha cometido en Arabia Saudita o por el contrario en Estados Unidos? Creemos que va a depender del lugar donde se produjo el acceso o la utilización indebida.

Debido a las diversas discusiones entre la Teoría de la Actividad –el delito es cometido en donde se ha realizado la acción- y la Teoría del Resultado – el delito es cometido en donde se ha producido el resultado, la doctrina se apoya mayoritariamente en la Teoría de la Ubicuidad[290], es decir, se puede considerar cometido el hecho tanto en el lugar donde se ha llevado a cabo la acción como en aquel en el que se ha producido el resultado[291], esta teoría es la seguida por nuestra legislación tal y como lo prevé el artículo 5 del Código penal peruano.[292]

Desde la perspectiva de la teoría de la ubicuidad, la comisión del delito informático se ha de verificar indistintamente donde se lleva cabo una conducta o donde se produce el resultado.

Ello ha de propiciar, en atención a la globalización de los sistemas informáticos, una estrecha colaboración entre los Estados para la lucha contra la criminalidad informática.

Es por esto que desde el principio de la presente investigación hemos hecho hincapié en que debe existir una regulación universal, para sancionar estas conductas, en donde aplicaríamos la excepción del artículo 1, en cuanto se refiere a las excepciones del Derecho Internacional.

Creemos que una gran iniciativa contra la delincuencia de alta tecnología es la asumida por el Consejo Europeo sobre la elaboración de un convenio sobre la delincuencia en el ciberespacio iniciada desde febrero del año 1997 y que debe concluir este año. Asimismo, existe la Posición Común que ha sido adoptada el 27 de mayo de 1999 por el Consejo de Europa relativa al Proyecto de Convenio sobre la Delincuencia en el Ciberespacio.[293] [294].

Las principales características de ésta Posición Común, son las del compromiso de los Estados miembros de apoyar la inclusión en el Convenio, facilitar una investigación y persecución eficaces de los delitos penales relacionados con sistemas y datos informáticos, así como complementar de manera adecuada el Derecho penal sustantivo.

De esta manera, los Estados miembros abogarán, si procede, por la inclusión de normas que exijan la tipificación como delitos relacionados con el contenido de los comportamientos delictivos llevados a cabo mediante un sistema informático. Así, “la Comisión concluye destacando el compromiso de garantizar que se establezca una jurisdicción pertinente para los delitos previstos en el citado Convenio, reforzando las disposiciones relativas a la cooperación y asistencia judicial, estudiando la posibilidad de una búsqueda informática transfronteriza, a efectos de un delito penal grave”. [295]

1.7.3 La inexistencia de peritos informáticos en el Perú.

Hasta el momento no existe un proceso penal concluido en donde se haya discutido la existencia o no de un delito informático. Cuando ello ocurra, sería necesario saber qué criterios utilizó el Juez penal para llevar a cabo su fallo.

Como todos sabemos, en la etapa de investigación de un proceso penal es necesario -en algunos casos- una pericia emitida por peritos judiciales designados por el Juez, a fin de determinar el perjuicio causado. Hasta donde tenemos conocimiento, no existen peritos informáticos especializados para este tipo de delitos, menos aún, Jueces capaces de resolver un problema de informática. Yendo mucho más atrás, tenemos conocimiento que no existen policías especializados en informática para determinar en un parte o en un atestado policial, la comisión de un delito informático.

Creemos que la preparación en informática de las personas mencionadas, llevará mucho tiempo, pero es necesaria para poder afrontar con efectividad este tipo de delincuencia.

Además, tecnológicamente es más fácil y económico probar un acceso o una utilización indebida a una base de datos, redes o sistema informático que probar otros delitos adicionales que se cometen por medio de sistemas informáticos, sobre todo para la afirmación de la relación de causalidad.

En este orden de ideas, la seguridad informática como bien jurídico protegido en los delitos informáticos, contribuye no sólo a una mejor configuración de los tipos penales, sino también a una mejor y efectiva intervención de la justicia penal.

1.7.4 Ausencia de proporcionalidad de las penas establecidas

Existe una diferencia sustancial entre la penalidad prevista para el delito de daños informáticos y la del de daños del artículo 205 del Código penal, en cuanto a que el primero tiene un máximo de cinco años de privación de libertad y el segundo un máximo de dos años.

En la actual configuración del delito de daños informáticos, no existe una justificación del por qué una mayor sanción contenido en el artículo 207-B, ya que el delito común de daños puede tener una mayor significación económica dependiendo del bien que se trate. A ello, se ha de agregar que el daño común exige la producción efectiva del resultado (delito de lesión), mientras que el daño informático tal y como lo prevé actualmente el artículo 207-B requiere para su configuración sólo la puesta en peligro del patrimonio, significando un menor desvalor del resultado en comparación con el primero, por lo que se deberá tener una pena inferior o no tan elevada.

Este problema de falta de proporcionalidad de las penas previstas se supera no sólo desde la consideración de la seguridad informática como bien jurídico protegido, sino desde la comprensión del delito de daño informático dentro de los alcances del tipo penal de daños del artículo 205 del Código penal, para lo cual no existe problemas en considerar como objeto material a una base de datos, sistema o programa de computadoras, teniendo, en consecuencia, la misma penalidad que la afectación a cualquier bien.

1.7.5 Principio de *Ultima Ratio*

Para proteger los intereses sociales el Estado debe agotar los medios menos lesivos que el Derecho penal antes de acudir a éste, que en este sentido debe constituir un arma subsidiaria, una *ultima ratio*.[\[296\]](#)

Todo ello dice relación con la necesidad de afirmar que tanto el ingreso, utilización e interferencia de los programas o sistemas informáticos sean indebidos, lo cual podrá determinarse sólo a través de una regulación previa a la penal que determine que es lo debido y lo indebido en la red.

Como bien señala MIR PUIG[\[297\]](#), sólo cuando ningún mecanismo administrativo o civil sea suficiente, entonces estará legitimado el recurso de la pena o de la medida de seguridad pues ello, como hemos visto, las funciones del acceso y tránsito de la red y sistemas informáticos resultan ser las pautas sobre las que deberá construirse la regulación.

De aquí que se sostenga la institucionalización de mecanismos orientados a la protección extrapenal, es decir, a mecanismos administrativos, ya que sólo de cumplirse con estos mecanismos de política criminal, la intervención penal en el terreno

informático podrá ajustarse al principio de *ultima ratio*. [298]

Así, la existencia de una normativa administrativa que regule el funcionamiento de la red y los sistemas informáticos permitirá determinar que tipo de conductas atentan contra la seguridad informática.

Esta afirmación está acorde también con la naturaleza de la seguridad informática como bien jurídico colectivo de carácter institucional, referido a establecer mecanismos y procedimientos organizativos para asegurar determinados bienes jurídicos personales en el marco del funcionamiento de sistemas informáticos.

Capítulo IV

Los delitos informáticos en la legislación comparada

-
-
-
-
-

Introducción

Como ha sido explicado anteriormente, el desarrollo de la tecnología ha producido y sigue produciendo problemas por malos usos de sistemas informáticos y de la red. Por ello, el tratamiento que el derecho penal le otorga al ámbito internacional varía mucho según cada legislación. Se puede decir, que aún no se ha llevado a cabo un consenso internacional a favor de la tipificación de los delitos informáticos.

A continuación, explicaremos como los países de Alemania, España, Estados Unidos de Norteamérica y Chile han dado un tratamiento para estas clases de conductas ilícitas que se producen en la red y en los sistemas informáticos.

1.1 Alemania

El sistema penal alemán

El modelo seguido por la legislación penal alemana respecto a la lucha contra la criminalidad informática se construye bajo la base de identificar dos supuestos de acciones atentatorias para determinados bienes jurídicos, así, por ejemplo, se tiene la tipificación del delito de fraude informático del Parágrafo 263 a y la del delito de sabotaje informático del Parágrafo 303 b. De esta forma podemos advertir que el interés en juego en la denominada criminalidad informática se circunscribe preponderantemente al patrimonio.

En cuanto a las conductas atentatorias a la vida personal y la privacidad, el Código penal alemán (Straf gesezt buch -StGB-) sanciona el espionaje de datos (Ausspähen von Daten) en el Parágrafo 202 a [299], sin embargo, 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.

Por otra parte, el legislador alemán ha decidido no criminalizar el mero intrusismo informático, sino sólo en aquellos casos de

conductas que signifiquen la manipulación de las computadoras y persigan un ánimo de lucro, ello se evidencia de la no inclusión como tipo penal de la conducta de utilizar o ingresar a un sistema informático sin autorización pues se deja de lado los datos almacenados electrónicamente o transmitidos.

El Código penal alemán sanciona en su artículo 263a el denominado delito de fraude informático (Computerbetrug) en los siguientes términos[300]:

“263a I. Quien, con la intención de procurar para sí o para un tercero una ventaja patrimonial ilícita, perjudique el patrimonio de otro influyendo en el resultado de un proceso de elaboración de datos por medio de una errónea configuración del programa, por medio del uso de datos incorrectos o incompletos, a través del uso no autorizado de datos o a través de intervención desautorizada en el proceso, será castigado con pena de privación de libertad de hasta cinco años o con multa.

II. Procede aplicar el 263, apartados II a V”.

El fraude informático viene regulado a continuación del delito de estafa[301], con la finalidad de solventar los problemas que presenta la estafa para comprender los casos en los que el error recae sobre una persona; así, por ejemplo, el engaño, el error y debido a ello la disposición patrimonial, elementos propios de la estructura típica del delito de estafa, no concurren en el fraude informático. En consecuencia, la construcción de los elementos del tipo del Parágrafo 263 a es más estrecha en comparación con aquellos previstos para el Parágrafo 263; sin embargo, se puede advertir en el fraude informático la concurrencia de elementos propios de los delitos contra el patrimonio y el fraude.

En cuanto al bien jurídico protegido en el delito de fraude informático, la ubicación sistemática de esta figura delictiva nos coloca en los delitos contra el patrimonio y así expresamente lo ha consignado el legislador alemán al hacer alusión directa en la redacción del tipo al perjuicio patrimonial; esta acentuación del legislador nos conduce a inferir que aunque el fraude informático se realiza por lo general en el ámbito de las actividades de una empresa, no se convierte por ello en un delito económico, ya que no está en juego en ningún momento el orden económico.

El objeto de la acción es el “resultado de un proceso de elaboración de datos”, la doctrina alemana sostiene que por datos se ha de comprender a toda información que se puede codificar. No obstante, debemos advertir que en el tipo penal alemán referido al delito de espionaje de datos, Parágrafo 202 a, se hace alusión expresa a que la idea de datos a efectos de este delito no deberá comprender a aquellos almacenados, transmitidos electrónicamente, magnéticamente, o de forma inmediatamente accesible. Por lo tanto, podremos suponer que esto está en función de que el legislador alemán no ha querido conceder una sanción penal para la conducta de "mero" intrusismo informático.

Las conductas descritas en el numeral 263 a se refieren a una errónea configuración del programa, al uso de datos incorrectos o incompletos y al uso no autorizado de datos o a través de intervención desautorizada en el proceso; todas estas conductas han de ser llevadas a cabo por el autor con la finalidad de procurar para sí o para un tercero una ventaja patrimonial ilícita.

Se evidencia claramente que el legislador alemán ha optado en la construcción del tipo penal del delito de fraude informático por la concurrencia de un elemento subjetivo específico, como es la finalidad de procurar una ventaja ilícita.

Se trata de un elemento subjetivo de intención trascendente, el tipo exige sólo la presencia de alguna de las conductas típicas como errónea configuración del programa, uso de datos incorrectos o incompletos y uso no autorizado de datos o intervención

desautorizada en el proceso, sin que se exija en el plano objetivo que se llegue a materializar la obtención de la ventaja patrimonial para el autor o para un tercero.

En este sentido, el dolo del autor sólo deberá de abarcar las conductas cuya objetividad es exigida por el tipo penal, ya que el dolo representa la voluntad exteriorizada.

Lo importante en la construcción germana del delito informático radica en que no se pretende conceptualizar un nuevo bien jurídico, ya que el legislador ha puesto el acento en el patrimonio como objeto de protección, de allí también la ubicación sistemática del Parágrafo 263 a en el Código penal alemán dentro del rubro de los delitos contra el patrimonio.

Por otro lado, el tipo penal del fraude informático se construye como una modalidad específica del delito de estafa, sin que se recojan todos los elementos propios de esta figura delictiva para permitir, precisamente, la adecuación típica de los hechos producidos por medios informáticos. Por ello resulta discutible que pueda hablarse específicamente de una identidad y autonomía propias del delito informático, pues más bien pareciera ser una modalidad más de los delitos contra el patrimonio caracterizada por el medio empleado. Ello también se deduce de la penalidad prevista que es de privación de libertad hasta de 5 años y multa, similar a la sanción prevista para el delito de estafa.

El delito de sabotaje informático (Computersabotage) se sanciona en los siguientes términos:

“303 b.- I. Quien destruya una elaboración de datos que sea de esencial importancia para una industria ajena, una empresa ajena o una autoridad,

1. cometiendo un hecho de acuerdo al 303 a, apartado I, o
 2. destruyendo, dañando, inutilizando, eliminando o alterando una instalación de elaboración de datos o un soporte de datos,
- será castigado con pena de privación de libertad de hasta cinco años o con multa.

II. La tentativa será punible.”

El delito de sabotaje informático presenta la característica especial de referirse sólo a datos de esencial importancia, relacionados con la industria, la empresa o una autoridad. Desde esta perspectiva, debemos señalar que no se encuentra comprendida dentro del sabotaje informático los daños a particulares que en forma aislada puedan perpetrarse sobre sus datos informatizados, en estos casos resulta una desprotección, si observamos que, a su vez el parágrafo 303 que sanciona el delito de daños, hace referencia como objeto material a una “cosa”, el cual presenta problema para comprender a la información almacenada.

El delito de alteración de datos que el Código penal alemán contempla en el Parágrafo 303 a, si bien sanciona a quien borre, elimine, inutilice o altere ilícitamente datos con una pena de privación de libertad de hasta 2 años o con multa, no resulta de aplicación para la figura en análisis, ya que dicho dispositivo expresamente remite la interpretación del término datos a lo conceptualizado en el Parágrafo 202 b II del mismo Código, en cuanto quedan fuera de protección aquellos datos que son objeto de almacenamiento, transmisión electrónica o magnética o de forma inmediatamente accesible. En atención a ello, insistimos que en el caso de la legislación alemana, todos los supuestos de daños a sistemas o programas informáticos de particulares en forma individual deberán ser comprendidos en el tipo básico del delito de daños del Parágrafo 303.

Ahora bien, uno de los supuestos del delito de sabotaje informático (Parágrafo 303 b I. 1.) constituye la conducta descrita en el Apartado I del Parágrafo 303 a que castiga al que borre, elimine, inutilice o altere ilícitamente datos, sin embargo se trataría sólo de datos relacionados con la industria, la empresa o las autoridades, de acuerdo a la propia redacción del Parágrafo en mención. En este sentido, podríamos sostener que el numeral 1. del Apartado I del Parágrafo 303 b resulta ser una circunstancia agravante del tipo penal del Parágrafo 303 a, siempre que se trate de datos de esencial importancia para la industria, la empresa o las autoridades.

El segundo supuesto del delito de sabotaje informático se caracteriza por sancionar las conductas de destruir, dañar, inutilizar, eliminar o alterar una instalación de elaboración de datos o un soporte de datos. Se trata de la protección del hardware.

Llama la atención, no obstante, la diferencia de penas entre los delitos de daños y de sabotaje informático, ya que para el primer supuesto la pena de privación de libertad es de un máximo de 2 años, mientras que para el segundo es de 5 años. Desde este orden de ideas, podemos advertir que el legislador alemán brinda una mayor protección penal a los datos importantes para la industria, la empresa o las autoridades, en comparación con aquellos vinculados a las personas individuales; por otro lado, se observa un mayor incremento de la protección de los datos respecto de los bienes en general propios del delito de daños, ya que este último supuesto tiene una sanción de privación de libertad no mayor de 2 años. De esta forma se advierte una mayor valoración de un determinado tipo de datos relacionados con la actividad económica (industria y empresa), por lo que puede señalarse que el bien jurídico protegido en este caso no está vinculado tanto a la protección material de los datos sino al interés de la economía y la administración en la capacidad de funcionamiento de sus datos.

El sabotaje informático es un delito eminentemente doloso, descartándose toda forma de realización culposa.

Por otro lado, la conducta de falsificación de datos probatorios relevantes se encuentra descrita en el Parágrafo 269 del Código penal alemán el mismo que establece lo siguiente:

“269 I. Quien, para engañar en el tráfico jurídico, almacene o altere datos probatorios relevantes de manera que en el momento de su recepción existiría un documento no auténtico o falsificado, o utilice datos almacenados o alterados de ese modo será castigado con pena de privación de libertad de hasta cinco años o con multa.

II. La tentativa será punible.

III. Deberá aplicarse el Parágrafo 267, apartado III.”[\[302\]](#)

Como se puede apreciar, el legislador sanciona con una pena mayor al que para engañar al tráfico jurídico utilice datos almacenados o alterados de ese modo, refiriéndose a datos que estén almacenados en archivos o en sistemas informáticos o ser alterados por medios informáticos.

En definitiva, la regulación de los llamados delitos informáticos en el Código penal alemán no sanciona el denominado intrusismo informático, se orienta a sancionar sólo las conductas fraudulentas a través de medios informáticos y los daños sobre los soportes técnicos. La ubicación sistemática de los tipos penales responde a la delimitación del fraude informático como un delito patrimonial y del sabotaje informático como una modalidad del delito de daños, por lo que a pesar de las denominaciones empleadas no podemos sostener la autonomía e identidad propias de estos delitos en la legislación penal alemana, menos aún puede concebirse un bien jurídico distinto al patrimonio en estas figuras delictivas. Tanto para el delito de fraude informático como para el delito de sabotaje informático, resulta de enorme importancia el consentimiento del titular del bien, pues elimina, como en todos los delitos patrimoniales, la tipicidad de la conducta.

1.2 España

El sistema penal español

El 26 de octubre de 1995 se aprobó, por el pleno del Senado, la nueva Ley Orgánica 10/1995 del nuevo Código penal español el mismo que entro en vigor el 24 de mayo de 1996.[\[303\]](#) Así, el Código penal español se ha visto obligado a intentar solucionar el problema[\[304\]](#) de conductas delictuosas que surge a raíz del incremento de las nuevas tecnologías. Así, se introdujo tipos nuevos y se modificó 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. Cabe señalar que la reforma cubre desde la delincuencia clásica con medios tecnológicos a los delitos cometidos a través de redes informáticas, como Internet.

El Título X del Código penal español, recoge en el artículo 197, bajo la denominación de "Delitos contra la Intimidad, el derecho a la propia imagen y a la inviolabilidad del domicilio, dicho precepto establece lo siguiente:

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.[\[305\]](#) [\[306\]](#)

Se puede apreciar que el legislador ha dado un giro en lo que respecta al concepto tradicional de documento. Ahora, para el Derecho penal español un documento puede comprender tanto un soporte físico como informático.[\[307\]](#)

Igualmente, el Código penal español equipara, a efectos de protección penal, la intrusión de las comunicaciones y la interceptación de las mismas con la intervención del correo electrónico, que queda asimilada a la violación de correspondencia. Y así se protege penalmente del apoderamiento del correo electrónico y la interceptación de las telecomunicaciones. Estas actividades deben producirse sin el consentimiento del afectado y con la intención de descubrir sus secretos[\[308\]](#) o vulnerar su intimidad.[\[309\]](#) [\[310\]](#)

El acceso in consentido, entonces, encajaría en el tipo relativo al descubrimiento y revelación de secretos previsto en el artículo 197.2 que requiere, para su punición, acceso, apoderamiento, utilización o modificación de datos reservados de carácter personal registrados digitalmente (ficheros o soportes informáticos, electrónicos o telemáticos) en perjuicio de tercero, en cualquier otro tipo de archivo o registro público o privado. Dichas conductas generalmente son producidas por los "sniffers".

El legislador español ha decidido configurar expresamente la realización de las conductas descritas en el artículo 197 por parte de autoridad o funcionario público, destacando el prevailecimiento del cargo, así lo expresa el artículo 198 del Código penal.[\[311\]](#)

El artículo 211 del Código penal español establece que 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. [\[312\]](#)

Podemos concluir que para el Derecho penal español, “por otro medio semejante” podemos llegar a la conclusión que los foros de discusión, el correo electrónico o la Internet, estarán considerados para el legislador español, como medios de difusión.

El tipo de “estafa informática” es recogido en el artículo 248.2, cuando "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." El numeral dos fue introducido recién en el texto penal de 1995, debido a las crecientes estafas mediante sistemas informáticos. Dicho texto se debió a que la doctrina española rechazaba la aplicación del tipo tradicional de estafa a los casos de transferencias informáticas de fondos, consistentes en introducir datos u órdenes falsas o efectuar alteraciones en los programas que gestionan automáticamente transferencias bancarias, ingresos o reconocimiento de créditos a favor de quien realiza la manipulación. Para salvar esta laguna de punición y no forzar los contornos del tipo de estafa más allá de los límites de lo permitido por el principio de legalidad sin incurrir en formas de analogía en contra del reo, el Derecho penal español encontró la solución al incorporar un tipo específico de estafa que acogiera la peculiaridad de que la transferencia del activo patrimonial se realizara mediante “alguna manipulación informática o artificio semejante”, ya sea por modificaciones de programas o alteraciones en el procesamiento. [\[313\]](#)

El artículo 256 señala lo siguiente; "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."

En el apartado de las conductas nocivas que se comenten en sistemas informáticos, se señaló la conducta “hurto de tiempo”. Pues bien, este delito es un claro ejemplo que el legislador español ha implementado a fin de acabar con este tipo de conductas.

Con respecto a este delito, creemos que pueden originarse figuras concursales con el delito de sabotaje.

Dentro del Capítulo IX, “De los Daños” el artículo 264 comprende la figura del sabotaje informático en donde se castiga con la pena de prisión de uno a tres años y multa de doce a veinticuatro meses "el 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." Así, el delito de sabotaje informático se encuadra dentro de este precepto como el supuesto de daños a programas, archivos y ficheros económicamente valubles para la actividad empresarial. La información de carácter personal, es objeto de protección del artículo 197.

Para LLANEZA GONZÁLES [\[314\]](#), la antigua redacción del Código no tuvo en cuenta el valor de la información como bien jurídico objeto de protección, refiriéndose entonces el delito de daños a bienes materiales. [\[315\]](#)

El artículo 270 incluye en la categoría de los delitos contra la propiedad intelectual la fabricación, puesta en circulación y tenencia de cualquier medio específicamente destinado a facilitar la supresión no autorizada o la neutralización de cualquier dispositivo técnico que se haya utilizado para proteger programas de ordenador. Es decir, se castiga el uso de “cracks” dentro y fuera de la Red.

El Código establece dos subtipos agravados, en el caso de que el beneficio obtenido posea especial trascendencia económica o que el daño revista especial gravedad (art. 271), todo ello sin perjuicio de la responsabilidad civil.

Este tipo penal no sólo resulta de aplicación, obviamente, al pirateo de los programas de ordenador y al uso de “cracks”, sino a la reproducción y explotación inconsentida de obras protegidas por los derechos de autor en su formato digital que se incorporen a las páginas webs, así como que las bases de datos accesibles a través de Internet reproducidas sin autorización del titular de los derechos.[\[316\]](#)

El artículo 278, por su parte, comprende el delito de espionaje informático. Conducta que está constituida por la obtención sin autorización de datos almacenados en un fichero informatizado, que se caracterizan por su confidencialidad, exclusividad y valor económico.

- 1.- El que, para descubrir un secreto de empresa se apoderase por cualquier medio de datos, documentos escritos o electrónicos, soportes informáticos u otros objetos que se refieran al mecanismo, 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.

Podemos señalar que el legislador ha generado en el contexto del artículo 278 una laguna. “El precepto no prevé atentados a la información empresarial reservada mediante abuso informático, puesto que no alude a los medios comisivos del artículo 197.2 . Ante este vacío normativo sólo cabe interpretar que el artículo 200 cumple una función subsidiaria, de recogida de conductas no abarcadas por el artículo 278. Así, el artículo 200 acogería conductas ilícitas de descubrimiento y de revelación o cesión de datos automatizados de personas jurídicas (en relación a los incisos 2 y 3 del artículo 197 CP.) pero al precio de desconocer su ubicación sistemática entre los delitos contra la intimidad de la persona física.[\[317\]](#)

1.3 Estados Unidos de Norte América

El sistema penal americano

Igual que en todos los países del mundo, Estados Unidos se ve envuelto en actividades delictuales mediante sistemas informáticos y dentro de la Red.[\[318\]](#)

Con respecto a la legislación sobre delitos informáticos en los Estados Unidos de Norteamérica, existen dos estatutos importantes sobre leyes federales de delitos informáticos; el 18 USC, Capítulo 47, Sección 1029, y Sección 1030, conocida como el Pronunciamiento sobre el Abuso y el Fraude Informático de 1986.

Estas no son las únicas leyes sobre el delito informático en los Estados Unidos, lo que sucede es que estas son las dos leyes más importantes usadas en los Juzgados Federales de los Estados Unidos para poner a los delincuentes informáticos en prisión.

El Departamento Nacional de Delitos Informáticos del FBI estima que entre el 85 y el 97 por ciento de las intrusiones en ordenadores no son detectadas. En un reciente informe del Departamento de Defensa, las estadísticas eran alarmantes. Se registraron un total de 8,932 sistemas atacados. A 7,860 de ellos los *hackers* accedieron con éxito. Se detectaron 390 de esas 7,860 intrusiones, y sólo 19 de ellas fueron

denunciadas. "La razón de por qué sólo 19 de esos ataques fueron denunciados fue porque las organizaciones que asustan a sus empleados, clientes y accionistas harán que se pierda la fe en esa compañía si se admite que sus ordenadores han sido atacados." [319] Además, muy pocos de los delitos informáticos que se denuncian se resuelven alguna vez. De acuerdo con el CSI (Computer Security Institute) es decir, el Instituto de Seguridad Informática), estos son los tipos de delitos y/ pérdidas informáticos:

1. Errores humanos: 55%
2. Problemas de seguridad físicos: 20% (p. ej. desastres naturales, o caídas de tensión)
3. Ataques internos con objetivo de beneficiarse de esos delitos informáticos: 10%
4. Empleados descontentos buscando venganza: 9%
5. Virus: 4%
6. Ataques externos: 1-3%

Si tenemos en cuenta que muchos de los ataques externos provienen de delincuentes informáticos profesionales -muchos de los cuales son empleados de la competencia de las víctimas-, los *hackers* son responsables de casi ningún daño producido a todos estos ordenadores.

Con esto estaríamos diciendo que el *hacker* "recreacional" que disfruta únicamente con curiosear por los ordenadores de otras personas no es el tipo de persona del que debemos tener miedo, ya que posiblemente el causante del daño sea un empleado que trabaje en la empresa de la víctima.

—
Para los Estados Unidos de Norteamérica el delito informático es considerado como tal, cuando entra en alguna de las siguientes categorías:

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

En estos casos, el FBI ordinariamente tiene jurisdicción sobre los casos que impliquen o sean referentes a la seguridad nacional, terrorismo, desfalcos a bancos y crimen organizado. El Servicio Secreto americano tiene jurisdicción en cualquier momento que el Ministerio de Hacienda sea atacado, o si los ataques no están bajo la jurisdicción del FBI. [320]

En ciertos casos federales puede que sean secciones como el Departamento de Aduanas, el Departamento de Comercio, o alguna organización militar, como la Oficina de Investigaciones de las Fuerzas Aéreas, las que posean la jurisdicción.

En los Estados Unidos existen leyes federales que protegen contra el ataque de ordenadores, uso ilegítimo de passwords, invasiones electrónicas en la privacidad, y otras transgresiones. El Pronunciamiento sobre Abuso y Fraude Informático de 1986 es la principal pieza legislativa que gobierna la mayoría de los delitos informáticos, aunque muchas otras leyes pueden ser usadas para perseguir diferentes tipos de delitos informáticos. El pronunciamiento fue modificado con 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 y había sido recién aprobada. 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.

En adición a las leyes federales, la mayoría de los estados han adoptado sus propias leyes de delitos informáticos. Como se mencionó líneas arriba, las dos leyes federales más importantes en los Estados Unidos de Norteamérica contra los delitos informáticos son 18 ASC: Capítulo 47, Secciones 1029 y 1030.

La Sección 1029 prohíbe el fraude y cualquier actividad relacionada que pueda realizarse mediante el acceso o uso de dispositivos falsificados como claves, tarjetas de crédito, números de cuentas, y algunos tipos más de identificadores electrónicos.

Existen nueve áreas de actividad criminal que se encuadran en la Sección 1029, las mismas que son las siguiente:

1. Producción, uso o tráfico de dispositivos de acceso falsificados. [\[321\]](#) 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 a dispositivos de acceso para obtener algo de valor totalizando \$1000 o más durante un periodo de un año. 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. 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. 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 objetivo de obtener dinero o algo de valor totalizando \$1000 o más durante un periodo de un año. 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 objetivo de ofrecerle algún dispositivo de acceso o venderle información que pueda ser usada para conseguir acceso a algún sistema. 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. [\[322\]](#) 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. [\[323\]](#) 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 que uno 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 somos la persona legítima. Pena: Multa de \$10,000 o dos veces el valor del crimen y/o hasta 10 años de cárcel, \$100,000 y/o hasta 20 años si se reincide.

En el 18 USC, Capítulo 47, Sección 1030, decretado como parte de la Ley sobre Abuso y Fraude Informático de 1986, prohíbe el acceso no autorizado o fraudulento a ordenadores gubernamentales [\[324\]](#), y establece diversas condenas para esa clase de accesos. Esta ley es considerada una de las pocas piezas de legislación federal únicamente referidas a ordenadores.

Bajo la Ley de Abuso y Fraude Informático, el Servicio Secreto americano y el FBI 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. Pena: Multa y/o hasta 1 año de cárcel, hasta 10 años si se reincide.

2. Obtención de información en un registro financiero de una institución fiscal o de un propietario de tarjeta de crédito, o información de un cliente en un archivo de una agencia de información de clientes. Pena: Multa y/o hasta 1 año de cárcel, hasta 10 años si se reincide.

3. Atacar un ordenador que sólo corresponda usar a algún departamento o agencia del gobierno de los EEUU, o, si 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. [\[325\]](#) Pena: Multa y/o hasta 1 año de cárcel, hasta 10 años si se reincide.

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. 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, código o comandos a otro sistema informático. [\[326\]](#) Pena con intento de dañar: Multa y/o hasta 5 años de cárcel, hasta 10 años si se reincide. Pena por actuación temeraria: Multa y/o hasta 1 año de cárcel.

6. 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. Pena: Multa y/o hasta 1 año de cárcel, hasta 10 años si se reincide.

Las personas encargadas de atrapar a los intrusos son el FBI (Federal Bureau of Investigation), en español, la Oficina de Investigación Federal; y la USSS (US Secret Service), en español el Servicio Secreto de los EEUU.

Así, la legislación americana amplía el tratamiento a aquellos que de manera temeraria lanzan ataques de virus de aquellos que lo realizan con la intención de hacer estragos, imponiendo para ambos, además de la aplicación de multa, un año de prisión para los primeros y 10 años para los segundos. Asimismo, se contempla la regulación de los virus, 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.[\[327\]](#)

1.4 Chile

El sistema penal chileno

La legislación penal chilena abordó la problemática de los delitos informáticos desde hace ya varios años, pues mediante la Ley N° 19223 de fecha 28 de Mayo de 1993 se instauraron determinados delitos con una gran incidencia en esta materia.[\[328\]](#)

Una de las primeras características que presenta esta legislación es la creación de una ley especial separada del texto penal sustantivo, ello obedecería, en nuestra opinión, a dos razones. Una vinculada a la necesidad de distinguir desde una norma independiente, la incorporación de nuevas figuras delictivas, caracterizadas por enmarcarse en un elevado desarrollo tecnológico, tratando así de lograr una mayor connotación y difusión social de carácter preventivo respecto de estas conductas, y, una segunda, referida a los bienes jurídicos protegidos que marca el acento en la protección de los datos informatizados y la información en la red o en sistemas informáticos, por lo que se pretende configurar a los datos y a la información como un valor autónomo diferenciado de la intimidad y el patrimonio.

La estructura de los tipos penales informáticos en la legislación en análisis gira en torno a la regulación de distintas conductas de sabotaje informático, sin considerar conductas vinculadas a la afectación de la intimidad o del patrimonio. Desde esta perspectiva, podemos sostener que se ha pretendido dotar a los delitos informáticos de una autonomía e identidad propias, distinguiéndolos de aquellas modalidades de delitos contra la intimidad o contra el patrimonio realizados por medios informáticos. Esta orientación político criminal coincide con la tesis asumida en la presente investigación, en cuanto somos de la opinión que las afectaciones a la intimidad y al patrimonio mediante el empleo de medios informáticos no constituyen delitos informáticos, sino modalidades de estos delitos en cuya realización se ha empleado una computadora o un sistema informático.

Ahora bien, en cuanto a lo que es la protección misma de la información o datos contenidos en los sistemas y los sistemas como tales, se advierte que el legislador expresamente hace la distinción de la afectación de ambos, considerando así la importancia del funcionamiento del sistema.

Desde esta perspectiva, podemos sostener que la información adquiere un valor propio en la legislación penal chilena, aunque no se le haya dado una connotación económica, ésta puede ser apreciada en toda su dimensión, por lo que nada obsta a que sea apreciada como valor económico.

El artículo 1 de la Ley sanciona la conducta de sabotaje informático en los siguientes términos:

“Artículo 1°.- El que maliciosamente destruya o inutilice un sistema de tratamiento de información o sus partes o componentes, o impida, obstaculice o modifique su funcionamiento, sufrirá la pena de presidio menor en su grado medio a

máximo. [\[329\]](#)

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”.

Como ya hemos advertido, una de las notas especiales de este delito es que no sólo se concibe como sabotaje informático el hecho de destruir o inutilizar

un sistema informático, lo cual nos vincularía con el delito de daños y de ahí con el patrimonio como objeto jurídico de protección, sino que, además, se castiga los ataques al funcionamiento del propio sistema, de tal manera que se puede advertir que dicho funcionamiento se erige también como objeto material de este delito.

Este primer párrafo del artículo 1º de la Ley hace alusión directa al soporte y a su funcionamiento, de esta forma queda recogida también la protección del software y el hardware. Este acento puesto por el legislador penal chileno en cuanto al funcionamiento de los propios sistema no se observa en la legislación nacional ni en la de aquellos países que comentamos en la presente investigación, por lo que podemos señalar que es una cualidad propia de esta legislación.

Ahora bien, el funcionamiento del sistema informático se encontraría en función de la seguridad informática, ya que, precisamente, lo que se pretende proteger salvaguardar son las funciones de acceso y transmisión propias de la red y sistemas informáticos, lo cual implicaría el acceso a la misma y su libre tránsito por la red, estos se ven afectados, sin lugar a dudas, cuando se atenta contra el funcionamiento del sistema informático.

En el precepto en comentario se advierte que la destrucción o inutilización de los sistemas de tratamiento de información ha de ir acompañada del adjetivo malicia, lo cual indica que se refiere a una conducta dolosa, esto es, a la conciencia y voluntad de llevar a cabo las conductas de destruir o inutilizar tales bienes, se descarta, en consecuencia, cualquier realización culposa de este delito.

Adicionalmente, el término “maliciosamente” contenido en este precepto hace alusión al conocimiento por parte del autor del carácter indebido de la conducta, lo cual permitiría comprender por qué el legislador no ha consignado expresamente que la conducta ha de ser sin la autorización del titular. Este tema está vinculado con la repercusión del consentimiento del titular en este delito, ya que a pesar de no haberse consignado expresamente que la conducta ha de ser sin la autorización del titular, el consentimiento tiene enorme significación para la tipicidad de la conducta, en la medida que el sujeto puede disponer de sus sistemas de tratamiento de información, sus datos e información.

El segundo párrafo del artículo 1º se refiere expresamente a la afectación de los datos contenidos en los sistemas (la información codificada) a través de las conductas descritas en el primer párrafo, esto es, la destrucción o inutilización de los sistemas de tratamiento de información o la alteración de su funcionamiento, esta referencia a los datos como objeto de protección los realza precisamente al dotársele de protección penal y al sancionar su afectación con una mayor penalidad respecto de los ataques a los sistemas mismos. No obstante, la afectación al sistema aparejada de la afectación de los datos encierra un mayor desvalor de resultado y, en consecuencia, a ello también obedecería la elevación de la pena para este supuesto.

El artículo 2º de la Ley sanciona el denominado delito de intrusismo informático en los siguientes términos:

“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 mínimo a medio”.[\[330\]](#)

En este precepto se sanciona el acceso, la interceptación o interferencia a un sistema de tratamiento de información. Lo especial de este artículo es que no se hace una referencia a si este tipo de ingreso ha de ser sin la autorización del titular, lo cual muestra un vacío, ya que podría interpretarse que quedaría comprendido también el ingreso consentido, bastando sólo alguna de las finalidades señaladas en la norma: apoderarse, usar o conocer indebidamente la información. Por ello, resultaría necesario en este caso acudir a una interpretación restrictiva de este tipo penal, con la finalidad de evitar excesos en la intervención penal.

Por otra parte, no se trata del mero intrusismo blanco que se caracteriza por el solo hecho de entrar a un sistema sin una finalidad distinta al ingreso, sino de un intrusismo con una finalidad específica que es la de apoderarse, usar o conocer indebidamente de la información contenida en un sistema de tratamiento, por lo que se trataría, como en el caso de la legislación penal peruana, de un elemento subjetivo de intención trascendente cuya materialización no es requerida por el tipo penal, ya que éste sólo exige la realización de las conductas de interceptar, interferir o acceder al sistema informático.

Ahora bien, el legislador chileno sí ha puesto el acento en cuanto al aspecto subjetivo de este delito en la exigencia de que el sujeto persiga un ánimo de apoderarse, usar o conocer la información que sea “indebido”, quizá pensando en que con ello solventaría el tema de los excesos que significaría comprender conductas autorizadas; sin embargo, se debe advertir que la calidad indebida de las mencionadas conductas no se exige en un plano material ni en un plano formal, sino sólo en la cabeza del autor, por lo que resultaría de difícil determinación; en efecto, cómo podría distinguirse un acceso autorizado con el ánimo de conocer indebidamente la información de un acceso autorizado sin dicho ánimo; creemos que, precisamente, lo que permite apreciar la finalidad indebida perseguida por el autor es el carácter de no autorizado de la conducta realizada.

El artículo 3° de la Ley sanciona la lesión de los datos informatizados en los siguientes términos:

“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”.[\[331\]](#)

Se trata de una modalidad de afectación de los datos distinta a la contenida en el segundo párrafo del artículo 1° de la Ley, ya que en este último caso lo que se sanciona es la afectación de los datos contenidos en sistemas de tratamiento de información a través de la destrucción o inutilización del propio sistema, mientras que en el dispositivo en análisis se trata de la alteración, destrucción o inutilización de los datos por cualquier otra forma distinta a la mencionada.

El legislador chileno acude a la expresión “maliciosamente” para acentuar el carácter doloso de la conducta, descartando así la sanción de cualquier forma de realización culposa de esta conducta.

Por otra parte, no se hace alusión al carácter indebido de la conducta o a la falta de autorización, lo cual no permite determinar con exactitud los alcances de la prohibición contenida en el tipo penal; sin embargo, del término “maliciosamente” puede inferirse no sólo la realización dolosa de la conducta, sino también un aspecto subjetivo de la misma vinculado al aspecto cognoscitivo de la conducta, en cuanto que el autor ha de obrar a sabiendas del carácter indebido de su accionar.

Una característica de la penalidad establecida en este delito es el hecho que es inferior a la penalidad establecida para aquel supuesto en que se lesiona los datos bajo la modalidad que comprende también la lesión del sistema de tratamiento de información o la afectación de su funcionamiento, ello nos conduciría a pensar que se trata de darle una mayor significación en cuanto a la protección de los datos en el artículo 1º de la Ley, debido al mayor desvalor de resultado que dicho tipo penal encierra.

El artículo 4º de la Ley no se trata propiamente de un delito informático, ya que refiere a la protección de los datos o información en los siguientes términos:

“Artículo 4º.- 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.”[\[332\]](#)

A pesar que el legislador hace referencia expresa a la protección de aquellos datos contenidos en un sistema de información, la difusión in consentida de los mismos no constituye, en nuestra opinión, una infracción informática en la medida en que no se trata de la afectación a la seguridad informática, menos aún un delito informático.

En efecto, como se ha sostenido a lo largo de la presente investigación, la afectación a determinados bienes jurídicos como la intimidad, el patrimonio, el honor, etc., a través de medios informáticos no convierte a estas conductas en delitos informáticos, sino en modalidades específicas de los delitos que protegen estos bienes jurídicos caracterizadas por el uso de un medio informático. Lo mismo sucede en el presente caso, si bien se trata de datos o información contenidos en un sistema de tratamiento informático, la revelación o difusión de los mismos es una conducta posterior al acceso indebido o a la interferencia de la red.

Es importante tener presente que la Ley chilena no ha tipificado el delito de *Hacking* en cuanto acceso indebido.[\[333\]](#) La ley, sólo en su artículo 2, se refiere al acceso a secas. Con esto podría presentarse confusión y estimarse que se trata de cualquier acceso, autorizado o indebido.[\[334\]](#)

Debido a que el legislador mantuvo en la atipicidad el delito de *Hacking*, se produce que en Chile es impune la conducta del *hacker* que por pruebas de carácter intelectual o mera diversión accede indebidamente a los sistemas, transgrediendo las medidas de seguridad.[\[335\]](#)

Para HERRERA [\[336\]](#) “la ubicación del texto fuera del Código penal chileno es una desafortunada técnica legislativa, por lo que mientras no se incorporen los nuevos delitos que exige la realidad social en el Código penal chileno, dicho cuerpo legal quedará desadaptado a los tiempos actuales.” Asimismo, el referido autor opina que lo más adecuado habría sido tipificar en el Código penal chileno los nuevos delitos que surgen del mal uso que se le da a las tecnologías de la información y que por sus características no puedan encuadrarse dentro de los delitos tradicionales. La misma opinión es seguida por nosotros, respecto a los denominados delitos informáticos en la legislación peruana.

Tercera Parte

PROPUESTA DE *LEGE FERENDA*

Capítulo I

Fundamentos de la regulación administrativa

1.1 Necesidad de un ente regulador

Creemos que el problema principal empieza por la búsqueda de fórmulas efectivas de control para la prevención de las conductas nocivas en el ciberespacio. Por tanto, es necesario que existan cuerpos normativos que regulen la concreta participación de los sujetos en la red y el funcionamiento de la misma.

Por otro lado, como existe un peligro real para aquellas personas cuyos datos están almacenados en un archivo, necesariamente hay que estructurar una normativa específica orientada a la protección del uso de la información personal. Aquí, habrá de regularse esencialmente su recolección, correcta administración, permanente actualización, así como su debida utilización para fines específicos.[\[337\]](#)

Dentro de los mecanismos de control institucional, preventivo a *priori*, se tendrá que reflexionar específicamente acerca de la conveniencia de la creación de una Institución que regule y fiscalice la actuación en los sistemas informáticos, en cuyo ámbito deberá de definirse qué es lo debido y lo indebido en la red y en los sistemas informáticos, lo cual permitirá una mejor interpretación de los tipos penales del delito informático.

Si bien esta materia puede ser desarrollada con un mayor conocimiento por parte de analistas de sistemas, programadores, ingenieros de sistemas, etc., creemos importante que la intervención administrativa deberá seguir las siguientes pautas:

1.- Establecer la obligación de declarar a la Administración la existencia de licencias o programas de seguridad de sistemas y archivos informáticos por parte de sus titulares, tanto personas individuales como personas jurídicas, gobiernos, instituciones, fundaciones, etc. para salvaguardar información que se crea valiosa, importante y con un valor económico.

2.- Establecer un órgano de vigilancia con personas especializadas, para determinar las conductas consideradas como nocivas,

tanto en la red, como en sistemas informáticos.

En esta propuesta no se pretende responder a la interrogante sobre cuales serían los mecanismos estrictamente técnicos o de seguridad de la información y cuales serían los sistemas informáticos adecuados, ya que ese tema deberá ser tratado por especialistas en informática.

Con mucho esfuerzo estamos proponiendo implementar un ámbito de seguridad informática, en donde se estudie la prevención del acceso furtivo a los sistemas informáticos, pues se trata de prevenir, detectar y detener interferencias a los sistemas informáticos.

No podemos alejarnos de la idea que más que un problema de diseño o construcción de una Instancia administrativa previa, esta propuesta será un problema de cultura tecnológica. Como sabemos, el Perú no se encuentra tan avanzado en tecnología como lo pueden estar las grandes potencias, sin embargo, las conductas nocivas en los sistemas informáticos y redes son un problema que seguirá incrementándose con el avance y el desarrollo de la informática, frente al cual desde ahora no podemos ser ajenos.

Creemos, que las funciones específicas que tendrá que optar la Instancia administrativa que se cree, la misma que podría ser denominada como INPRODIN (Instituto Nacional para la Protección del Uso de Información), deberá cumplir las siguientes funciones:

- 1.- Funciones de Prevención: En donde se restringe el acceso por parte de *hackers*, *crackers*, etc. a sistemas informáticos o archivos de datos, a través de la regulación de los mecanismos de seguridad a ser adoptados por los usuarios de la red.
- 2.- Funciones de Detección: En donde se descubran los fraudes, en cuanto a la actuación de los *hackers*, *crackers*, etc. tras pase los mecanismos de prevención establecidos, y;
- 3.- Función Sancionadora: Que determina sanciones administrativas para aquellos operadores de sistemas informáticos que no cuentan con mecanismos de seguridad para los usuarios en la prestación de sus servicios, así como respecto de aquellas conductas nocivas en la red que atenten contra su concreto funcionamiento, sin llegar a configurar atentados a la seguridad informática, como puede ser el caso del envío no consentido de publicidad.

1.2 Propuesta

1.2.1 Reformulación de los tipos penales del Delito Informático

Como hemos visto, el instrumental normativo, es decir la Ley 27309, escogido por el legislador no es apropiado ni suficientemente efectivo en relación con la realidad expuesta.

Resulta muy difícil tipificar en materia penal los denominados delitos informáticos. Existe un número ilimitado de conductas y situaciones que están constantemente sometidas a los adelantos tecnológicos, lo cual conlleva necesariamente a nuevas modalidades delictuales.

Como se ha explicado a lo largo de la presente investigación, no se trata de pensar en un nuevo Derecho penal sino de adaptar el vigente a las nuevas exigencias de la tecnología, y a partir de ahí, considerar que bienes jurídicos como la intimidad, patrimonio, honor, requieren de una protección antelada, la misma que, en nuestra opinión, les brinda la seguridad informática, desde esta perspectiva han de ser reformulados los tipos penales de los delitos informáticos vigentes.

Es evidente que los ilícitos y los abusos informáticos en cierta forma han sorprendido a los penalistas, situación que en parte se debe a que el Derecho penal anterior al desarrollo de la informática no pudo prever sus implicancias criminales y, además, a que por ser novedoso el tratamiento de esta temática, se caracteriza por una notable falta de precisión. [\[338\]](#)

Sin embargo, creemos que los delitos informáticos actualmente consagrados en el Código penal peruano, deben estar referidos a la protección del bien jurídico seguridad informática y no a la intimidad y patrimonio, para lo cual será suficiente la eliminación de todos los elementos subjetivos de intención trascendente contenidos en el artículo 207-A del Código penal.

De esta forma a través de la sanción de las conductas de acceso, utilización e interferencia indebidos de sistemas informáticos se brindará una protección antelada de tales bienes jurídicos. De otro caso, los ataques a bienes jurídicos como la intimidad y el patrimonio a través del empleo de medios informáticos, podrán recogerse en los tipos penales tradicionales como delitos de lesión efectuando leves modificaciones.

Así, por ejemplo, en el caso de los delitos contra la intimidad será conveniente añadir en el artículo 154 del Código penal los medios informáticos como forma de comisión, de esta manera quedarán expresamente regulados los ataques a la intimidad provenientes del uso de computadoras, evitándose situaciones de atipicidad. En cuanto a la interceptación de correo o mensajes electrónicos, resultaría conveniente la inclusión de estos expresamente en el artículo 161 del Código penal como objeto material de las conductas descritas.

Respecto de los delitos contra el patrimonio, habrá de incorporarse dentro del artículo 197 del Código penal el supuesto de defraudación llevada a cabo por medios informáticos.

Asimismo, respecto del denominado daño o sabotaje informático previsto en el actual artículo 207-B, es suficiente el tipo penal del delito de daños del artículo 205 del Código penal, pues no existen problemas para comprender como objeto material al sistema o programa informático, desde esta perspectiva se sancionará la efectiva producción del daño, superándose los problemas actuales vinculados al principio de proporcionalidad.

No obstante, debemos advertir que en el artículo 207-A deberá comprenderse como modalidad típica la conducta de interferir una base de datos, sistema o red de computadoras, actualmente contenida en el artículo 207-B. Ello no significaría la derogación de este artículo.

Las agravantes establecidas en el artículo 207-C inciso 1 y 2 en cuanto se basa en el uso de la información privilegiada obtenida en función del cargo que desempeña el agente y a la puesta en peligro de la seguridad nacional, han de ser mantenidas como modalidades agravadas del delito de intrusismo informático.

Quizás, la orientación final del presente trabajo este muy lejos de la opinión de expertos en el tema, sin embargo, creo que los planteamientos expuestos deberán ser considerados para una revisión de la Ley N° 27309.

1.2.2 Proyecto de Ley.

Lunes, 10 de mayo del año 2001

CONGRESO DE LA REPUBLICA

Proyecto de Ley que modifica la Ley de los Delitos Informáticos

LEY N° _____

EL PRESIDENTE DE LA REPÚBLICA

POR CUANTO:

El Congreso de la República

ha dado la Ley siguiente:

EL CONGRESO DE LA REPÚBLICA;

ha dado la Ley siguiente:

LEY QUE MODIFICA LA LEY N° 27309 -LEY DE DELITOS INFORMÁTICOS-.

Artículo 1.- Modifíquese el artículo 207-A del Código penal en los siguientes términos:

Artículo 207-A. El que accede, utiliza o interfiere indebidamente a un sistema informático, base de datos, sistema o red de computadoras o cualquier parte de la misma, será reprimido con pena privativa de libertad no mayor de dos años o con prestación de servicios comunitarios de cincuentidós a ciento cuatro jornadas.

La pena será privativa de libertad no menos de cinco ni mayor de siete años, cuando:

1. El agente haga uso de información privilegiada, obtenida en función a su cargo.
2. El agente pone en peligro la seguridad nacional.

Artículo 2.- Deróguese los artículos 207-B y 207-C del Código penal.

Artículo 3.- Modifíquese los artículos 154, 161 y 197 del Código penal en los siguientes términos:

Artículo 154.- “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, medios informáticos u otros medios, será reprimido con pena privativa de libertad no mayor de dos años. (...) “

Artículo 161.- “El que abre indebidamente, una carta, un pliego, telegrama, radiograma, despacho telefónico, correo o mensaje electrónico 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.”

Artículo 197. inciso 5- “El que, con el ánimo de procurar para sí o para otro un provecho ilícito, altere o modifique la configuración de algún programa, sistema, red de computadoras, base de datos u otro medio análogo en perjuicio del titular o de un tercero.”

Comuníquese al señor Presidente de la República para su promulgación.

En Lima, 10 de mayo del año 2001.

Conclusiones

-
-
-
-
-
-

1. Es indubitable el gran desarrollo que originan cada día los sistemas informáticos. Cada vez más, la sociedad se ve inmersa en el avance tecnológico que produce la utilización de estos sistemas.
2. Así, la tecnología ha originado nuevas formas de comunicación virtual, como el Internet Relay Chat o el correo electrónico, las cuales han suplantado, en gran medida, el correo postal, favoreciendo tanto las relaciones personales como los negocios y la industria.
3. Una de las principales características del ciberespacio es el anonimato de las personas en donde pueden con gran facilidad, suplantar su personalidad por otra.

4. Debido a los contenidos ilegales en Internet y a las conductas nocivas que se originan mediante el empleo de sistemas informáticos, se hace necesario una debida regulación de tipos penales que sancionen estas conductas.
5. Así como el avance tecnológico ha traído consigo muchos adelantos, también se han generado nuevas conductas antisociales que no eran posible imaginar el siglo pasado.
6. Son muchas las conductas ilícitas que se producen cada día en la red o en sistemas informáticos. Si bien es cierto que los llamados delitos informáticos están caracterizados por la dificultad de descubrirlos, denunciarlos y probarlos, estas conductas deben ser reguladas adecuadamente para una efectiva sanción.
7. Ciñéndonos a la legislación vigente, se puede llegar a decir que el bien jurídico protegido en los denominados delitos informáticos son principalmente, la intimidad y el patrimonio. Advirtiéndose que los tipos penales actuales no les otorgan una efectiva protección.
8. Sin embargo, estos bienes jurídicos no son autónomos de la informática, por lo que es necesario la determinación de un nuevo bien jurídico que deberá de gozar de protección penal.
9. El bien jurídico en los delitos informáticos es la seguridad informática, característica propia y autónoma de la red y los sistemas informáticos.
10. La seguridad se basa principalmente en el acceso a un sistema informático y al tránsito de la información.
11. Por tanto, la configuración de los delitos informáticos deberá recoger sólo a las conductas que atenten contra el acceso y/o tránsito de sistemas informáticos.
12. El delito de intrusismo informático aparece como delito informático con autonomía e identidad propias. Por lo que se requiere la modificación de los artículos 207-A y 207-B del Código penal.
13. Se ha de incorporar como modalidades específicas de los delitos contra la intimidad, el secreto e inviolabilidad de las comunicaciones y el patrimonio modalidades que recojan el empleo de medios de información.
14. Asimismo, se ha de incorporar el inciso 5 en el artículo 197, como delito de defraudación por medios informáticos.
15. Se ha de configurar una instancia previa a la penal que regule el funcionamiento de la red y los sistemas informáticos, a efectos de una mejor comprensión de los tipos penales informáticos.
16. El legislador debe tener presente las soluciones adoptadas por los diferentes países mencionados para la adecuación de los delitos tradicionales en los delitos informáticos.

17. Es necesaria la adopción de un convenio internacional a fin de garantizar el uso de sistemas informáticos y de la red. Así como la promulgación de una ley de protección de datos personales.

Glosario de términos

En la cibercultura y sobre todo en la informática, existen varios diccionarios con gran cantidad de términos –usualmente en el idioma inglés- y significados de palabras que desde hace algún tiempo, la Real Academia de la Lengua Española se ha visto en la obligación de incluir.

Debido que el presente trabajo de investigación comprende una serie de términos acrónimos y palabras que no sabemos, en muchos casos su significado exacto y menos aún sin saber de donde provienen, consideramos que el glosario de términos es parte fundamental en la presente tesis.

En esta sección de obligada visita, se detallará el significado de cada acrónimo citado en la presente tesis, así como los principales términos usados tanto en sistemas informáticos como en Internet.

Cabe resaltar, que los referidos términos que se señalan a continuación provienen de los libros y diccionarios virtuales más usados en informática.

Agencia de Proyectos de Investigación Avanzada para la Defensa (Defense Advanced Research Projects Agency – DARPA): Organismo dependiente del Departamento de Defensa norteamericano (DOD) encargado de la investigación y desarrollo en el campo militar y que jugó un papel muy importante en el nacimiento de Internet a través de la red ARPANET.

Algoritmo criptográfico (Cryptographic algorithm): Función matemática que combina un texto o cualquier otra información inteligible con una cadena de dígitos denominados clave, para obtener una de texto de símbolos ininteligibles.

Archivo, fichero (File): Unidad significativa de información que puede ser manipulada por el sistema operativo de un ordenador. Un fichero tiene una identificación única formada por un nombre y un apellido, (apellido llámese extensión .exe, .com, etc) en el que el nombre suele ser de libre elección del usuario y el apellido suele identificar el contenido o el tipo de fichero.

Archivo: Conjunto de datos almacenados bajo un solo nombre, tal como una lista de direcciones, lista de fechas o facturas por cobrar que pueden ser procesadas por un computador.

Autenticación: Verificación de la identidad de una persona o de un proceso para acceder a un recurso o poder realizar determinada actividad. También se aplica a la verificación de identidad de origen de un mensaje.

Autoridad de Certificación (Certificate authority): Empresa u organización de confianza que acepta las claves junto con algunas pruebas de identidad y sirve como depósito de los certificados digitales. Se puede requerir la verificación de las claves a la Autoridad de Certificación.

Ayudante digital personal (Personal digital assistant): Pequeño mecanismo electrónico portátil de apoyo.

Back Up: Copia de respaldo de archivos o programas de datos que es conservada para ser usada solamente si el archivo inicial es destruido.

Bajar, descargar (download): Proceso de transferir información desde un servidor de información al propio ordenador.

Banca en casa (Home banking): Servicios bancarios que puede utilizar un cliente de una institución financiera, utilizando para ello un teléfono, la televisión, o un ordenador personal como unión con el centro de ordenadores de la institución financiera.

Bastion Host: Es un sistema identificado por el administrador del sistema como el punto más crítico en la seguridad de la red. Esta expuesto a Internet y es el punto de contacto para usuarios de redes internas.

Baud Rate: Velocidad de transmisión de caracteres en una línea conectada usualmente por impresoras, terminales y Modem. Su nombre deriva de Emil Baudot quien fuera un pionero en telegrafía impresa.

Beat (Bit): Abreviatura de dígito binario, unidad básica de información utilizado por una computadora. Unidad mínima de información digital que puede ser tratada por un ordenador. Proviene de la contracción de la expresión binary digit (dígito binario)

Bombardeo postal (Mail Bombing): Envío indeseado y masivo de mensajes de correo electrónico.

Bombardeo publicitario (Spam): Envió masivo, indisciplinado y no solicitado de publicidad a través de correo electrónico.

Browser: Hojeador, navegador, visor, visualizador. Aplicación para visualizar documentos html y navegar por Internet. En su forma más básica son aplicaciones hipertexto que facilitan la navegación por los servidores de información Internet, cuentan con funcionalidades plenamente multimediales y permiten indistintamente la navegación por servidores www, FTP, Gopher, el acceso a grupos de noticias, la gestión del correo electrónico, etc.

Bucaneros: Individuos que sólo buscan el comercio negro de los rótulos entregados por los *Copyhackers*. Los bucaneros sólo tiene cabida fuera de la red, ya que dentro de ella, los que ofrecen productos “crackeados” pasan a denominarse piratas informáticos. El bucanero es simplemente un comerciante, el cual no tiene escrúpulos a la hora de explotar un producto de cracking a nivel masivo.

Bug: error, insecto. Término aplicado a los errores descubiertos al ejecutar un programa informático. Fue usado por primera vez en el año 1945 por Grace Murria Hooper, una de las pioneras de la programación moderna, al descubrir como un insecto (bug) había dañado un circuito del ordenador Mark.

Bulo, camelo (Hoax): Término utilizado para denominar a rumores falsos, especialmente sobre virus inexistentes, que se difunden por la red, a veces con mucho éxito causando al final casi tanto daño como si se tratase de un virus real.

Byte: Conjunto significativo de ocho bits que representan un caracter. Es el menor elemento direccionable en el computador usualmente utilizado para almacenar un caracter.

Caballo de Troya (Trojan Horse): Programa informático que lleva en su interior la lógica necesaria para que el creador del programa pueda acceder al interior del sistema que lo procesa desde un lugar remoto.

Caja de conexión, módulo de conexión (Step-top Box): Dispositivo multifunción que permite la recepción y distribución en el ámbito doméstico de señales procedentes de diversos tipos de redes de comunicación (radio, televisión, teléfono, cable, satélite, Internet, etc.)

Caja registradora automática (Automated teller machine – ATM): Un dispositivo electromecánico que permite que los usuarios autorizados, habitualmente usando tarjetas de plásticos leíbles por el dispositivo, retiren efectivo de sus cuentas y/o accedan a otros servicios, tal como peticiones de saldo, transferencias o aceptación de depósitos.

Cajero automático (Cash dispenser): Un dispositivo electromecánico que permite el retiro, utilizando habitualmente tarjetas de plástico, de billetes de banco y en algunos casos monedas.

Capacidad: Cantidad de información que quiere decir que puede almacenarse en una unidad magnética (diskette) usualmente descrita el K Bytes y Kilo Bytes, donde un kilo bytes representa 1,024 bytes.

Caracter: Una letra, signo especial, dígito numérico.

Carga del Sistema Operativo: Leer el sistema operativo del área reservada al mismo en el diskette.

Certificado digital (Digital certificate): Documento electrónico emitido por una autoridad de certificación, utilizado para establecer la identidad de una empresa o persona, comprobando su clave de acceso público.

Chat: Conversación, charla, chateo, tertulia. Comunicación simultanea entre dos o más personas a través de Internet.

Chip: Circuito integrado en un soporte de silicio, formado por transistores y componentes electrónicos miniaturizados. Son uno de los elementos esenciales de un ordenador. Pequeño elemento de silicio que contiene la lógica del computador, los circuitos para el procesamiento de datos, la memoria principal, la entrada y salida de la información. Los chips están soldados sobre una plaqueta de circuito impreso para formar el computador.

Ciber (cyber): Prefijo utilizado ampliamente en la comunidad Internet para dominar conceptos relacionados con las redes (cibercultura, ciberespacio, cibernauta, etc.) Su origen es la palabra griega “cibernao”, que significa “pilotear una nave”.

Ciberpolicía (Cybercop): Funcionario policial especializado en Internet o en utilizar la red para sus investigaciones.

Cifrado, encriptación: El cifrado es el tratamiento de un conjunto de datos, contenidos o no en un paquete, a fin de impedir que nadie excepto el destinatario de los mismos pueda leerlos.

Cifrar: consiste en desordenar los datos de manera que adquieran una apariencia aleatoria pero recuperable.

Clave (key): Código de signos convenidos para la transmisión de mensajes secretos o privados.

Clave de acceso privado (Private Key): Clave utilizada para encriptar un mensaje. La clave es conocida sólo por su propietario.

Clave de acceso público (Public Key): Clave utilizada por el destinatario de un mensaje para desencriptarlo.

Clave de búsqueda, palabra clave (Keyword): Conjunto de caracteres que pueden utilizarse para buscar una información en un buscador o en un sitio web.

Clic: cliqueo, cliquear, pulsación, pulsar. Acción de tocar un mando cualquiera de un ratón una vez colocado el puntero del mismo sobre una determinada área de la pantalla con el fin de dar una orden al ordenador.

Comando: Instrucción ingresada por el usuario mediante el teclado o mouse para dirigir la acción del computador.

Compatibilidad: Habilidad de un computador para aceptar y procesar datos producidos, equipos, piezas internas por otro computador sin ninguna modificación en los discos o diskettes en los que los datos son transferidos.

Configuración: Conjunto de comandos que permiten al usuario modificar a su elección el sistema operativo.

Contraseña, palabra de paso (Password): Conjunto de caracteres alfanuméricos e incluso especiales (comandos ASCII) que permite a un usuario el acceso a un determinado recurso o la utilización de un servicio dado.

Cookie: (espía, delator, fisgón, soplón). Conjunto de caracteres que se almacenan en el disco duro o en la memoria temporal del ordenador de un usuario cuando accede a las páginas de determinados sitios web. Se utilizan para que el servidor accedido pueda conocer las preferencias del usuario. Dado que pueden ser un peligro para la intimidad de los usuarios, éstos deben saber que los navegadores permiten desactivar los cuquis.

Copyhacker: Es una nueva raza sólo conocida en el terreno del crackeo de hardware, mayoritariamente del sector de tarjetas inteligentes empleadas en sistemas de televisión de pago. Estos personajes emplean la ingeniería social para convencer y entablar amistad con los verdaderos *hackers*, les copian métodos de ruptura y después se los venden a los “bucaneros”. Los *Copyhackers* divagan entre la sombra del verdadero *Hacker* y el Lamer.

Cortafuegos (Rirewall): Sistema que se coloca entre una red local a Internet. La regla básica es asegurar que todas las comunicaciones entre dicha red e Internet e incluso entre otros periféricos, se realicen conforme a las políticas de seguridad de

la organización que lo instala. Además, estos sistemas suelen incorporar elementos de privacidad, autenticación, etc.

CPU: Unidad Central de Procesos, es el llamado cerebro del computador donde se interpretan y procesan las instrucciones y los datos a través del microprocesador.

Cracker: Sinónimo de ruptura. Es una persona que rompe la seguridad de un sistema. 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 encuentra el modo de romper una protección. Esta rotura es difundida normalmente a través de la red para conocimientos de otros.

Criptoanálisis: El arte de descifrar mensajes cifrados.

Criptografía (Cryptography): Término formado a partir del griego *kryptos*, "oculto". Arte de escribir con clave secreta o de un modo enigmático. Es criptografía cualquier procedimiento que permita a un emisor ocultar el contenido de un mensaje de modo que sólo personas en posesión de determinada clave puedan leerlo tras haberlo descifrado.

Criptografía de la clave de acceso público (Public Key Cryptography): Método de codificación que utiliza dos claves: una de acceso privado y otra de acceso público. Los mensajes codificados con cada clave pueden ser descodificados con la otra. Los criptogramas de las claves de acceso público utilizan algoritmos de encriptación asimétricos.

Criptografía: en griego, escritura secreta. Es el arte de diseñar cifradores. Se emplean para proteger la identidad de los usuarios y la confidencialidad de los datos. La regla general de la criptografía es que el criptoanalista conoce el método general de cifrado utilizado. El secreto real es la clave y su longitud es un aspecto importante del diseño. Formado por la criptografía y el criptoanálisis.

Cursor: Indica la posición activa en la pantalla de la terminal. Generalmente es una línea, en forma horizontal o vertical.

Cyberculture (Cibercultura): Conjunto de valores, conocimientos, creencias y experiencias generadas por la comunidad internauta a lo largo de la historia de la red. Al principio era una cultura elitista; más tarde, con la popularización de Internet, la cibercultura es cada vez más parecida a la cultura a secas.

Cybernauta (ciber-nauta): Persona que navega por la red.

Cyberspace (Ciberespacio): Término creado por William Gibson en su novela fantástica "*Neuromancer*" para describir el "mundo" de los ordenadores y la sociedad creada en torno a ellos.

Cybertrash (ciberbasura): Todo tipo de información almacenada o difundida por la red que es manifiestamente molesta o peligrosa para la salud mental de los internautas. Dícese también de quienes arrojan basura la red.

Cyberzapping (ciberzapeo): Acción de pasar de forma rápida y compulsiva de una página a otra dentro de un sitio web o de un sitio web a otro.

Daemon: Aplicación UNIX que está alerta permanentemente en un servidor Internet para realizar determinadas tareas como, por ejemplo, enviar un mensaje de correo electrónico o servir una página web. Daemon es una palabra latina que significa espíritu (bueno o malo) o demonio.

Datos: Los números, letras, símbolos procesados o producidos por una computadora.

Descifrado, deencriptación (De-encryption): Recuperación del contenido real de una información cifrada previamente.

Dialup (conexión por línea conmutada): Conexión temporal, en oposición a conexión dedicada o permanente, establecida entre ordenadores por línea telefónica normal. Dícese también del hecho de marcar un número de teléfono.

Dinero digital al contado (Digital cash): Alternativa electrónica para obtener dinero al contado.

Dirección IP (IP address): Dirección de 32 bits definida por el Protocolo Internet en STD 5, RFC 79 1. Se representa usualmente mediante notación decimal separada por puntos. Un ejemplo de dirección IP es 193.127.88.345

E.D.I. (Electronic Data Interchange): Se inició en la década de los sesenta. Su objetivo es el intercambio de documentación que se encuentra previamente normalizada.

E.F.T.: Responde a Electronic Funds Transfer y permite una adecuada transmisión electrónica de fondos y realización de

pagos.

En línea (On line): Es esencialmente todo aquello a lo que puedes conectarte con el ordenador y un módem. Incluye por consiguiente la web, el correo electrónico y los servicios tradicionales como *América On Line* y otros. Es comunicación directa en tiempo real a través de la red.

Entrada/Salida: Aceptación o transferencia de datos desde y hacia un computador.

Entrada: Datos ingresados en el computador mediante un periférico. (Ya sea, por teclado, scanner, modem, etc.)

Espacio de mercado (Marketspace): Término nuevo para el mercado donde se lleva a cabo el comercio electrónico. Engloba la transición de los mercados físico a los mercados basados y controlados por la información.

Estándar de Cifrado de Datos (Data Encryption Standard – DES): Algoritmo de cifrado de datos estandarizado por la administración de los Estados Unidos de Norte América.

Estrato de huecos seguros (Secure sockets layer): Este protocolo proporciona autenticidad para servidores y navegadores, así como confidencialidad e integridad de los datos para las comunicaciones entre un servidor y un navegador. Sin embargo, asegura el canal de comunicaciones actuando en baja intensidad en las estanterías de la red entre la capa o estrato de aplicación y el transporte TCP/IP y capas de la red.

Extensiones de correo en Internet sin riesgo (Secure multimedia Internet mail estensions): Propuesta nueva que utiliza algoritmos criptográficos patentados y autorizados por RSA Data Security Inc. Depende de certificados digitales y por consiguiente de las autoridades de certificación para acreditar la autenticidad.

Firewall: Es un programa que reside en una máquina que actúa como único punto de defensa, para controlar el acceso entre redes privadas y redes públicas. Establece un perímetro de seguridad, separa las redes y define el acceso y refuerza las políticas de seguridad. Es un sistema o grupo de sistemas configurados para reforzar las políticas de seguridad entre dos redes.

Firma digital (Digital signature): Información creada que identifica al autor de un documento electrónico y autentifica que es quien dice ser.

Firmas ciegas (Blind signaures): Este sistema, desarrollado por DigiCash, permite al comprador obtener dinero electrónico al contado en un banco. El banco no está autorizado a situar el nombre del comprador entre los pagos nominales que emite.

Formatear: Acción de preparar la inicialización de la estructura de un dispositivo de almacenamiento, diskettes, cd's, cintas, etc., para que pueda ser reconocido por el sistema operativo.

Free Software (Software Libre): Programas desarrollados y distribuidos según la filosofía de dar al usuario la libertad de ejecutar, copiar, distribuir, estudiar, cambiar y mejorar dichos programas. El software libre no es siempre software gratuito (equivocación bastante habitual que tiene su origen en que la palabra inglesa free es conocido como gratuito).

Freeware (programas de libre distribución, programas de dominio público): Programas informáticos que se distribuyen a través de la red de forma gratuita.

FTP (File Transfer Protocol): Comprende el conjunto de reglas que permiten la transferencia síncrona o asíncrona de archivos a través de Internet.

Fuera de línea (Off line): Es una comunicación realizada en otro medio, fuera de Internet y en otro momento.

Gurú (gurfi): Persona a la que se considera, no siempre con razón, como el sumo manantial de sabiduría sobre un determinado tema. Nicholas Negroponte es considerado el máximo guía en lo que se refiere a Internet y la llamada sociedad de la información.

Gusano (Worm): Programa informático que se autoduplica y autopropaga. En contraste con los virus, los gusanos suelen estar especialmente escritos para redes.

Hacker: Una persona que le encanta explorar los detalles de los sistemas informáticos u explotar sus capacidades, contrario a muchos usuarios que prefieren aprender sólo lo mínimo necesario. Estos personajes son expertos en sistemas avanzados. Su objetivo principal es comprender los sistemas y el funcionamiento de ellos. Normalmente son quienes alertan de un fallo en algún programa comercial y lo comunican al fabricante. El perfil del *Hacker* idóneo es aquel que se interesa por la tecnología si la intención de producir un daño. No obstante puede darse el caso.

Hardware: Se trata de la parte física del computador, sus componentes duros tales como elementos mecánicos o magnéticos.

Impresora: Periférico de complemento que permite la salida de los comandos de impresión sobre el papel de los datos enviados por el computador.

Iniciativa de pagos electrónicos comunes (Joint electronic payments initiative): Esta iniciativa liderada por World Wide Web Consortium y Commerce Net, es un intento de estandarizar las negociaciones de los pagos. Desde el punto de vista del comprador o cliente, la Iniciativa (en inglés conocida por sus siglas JEPI) sirve como un contacto que autoriza a los navegadores, y monederos electrónicos, a usar una variedad de protocolos de pago.

Instrucción: Sentencia de un programa especificando una función o tarea a realizar.

Intercambio de datos electrónicos (Electronic data interchange): El intercambio electrónico de documentos empresariales como órdenes de compra, cotizaciones, gastos de mercancías o facturas, entre las aplicaciones informáticas de empresas, de forma estándar. Los sistemas de intercambio de datos electrónicos son usados principalmente por las empresas interesadas en contactar con sus proveedores.

K: Proviene del griego Kilo que significa 1,000. Equivale a 1024 elementos. Se utiliza 1024 en lugar de 1000 debido a que es una potencia entera de dos.

Lamers: Individuos con ganas de hacer *Hacking*, pero que carecen de cualquier conocimiento. Habitualmente son individuos que apenas si saben lo que es un ordenador, pero el uso de este y las grandes oportunidades que brinda Internet, convierten al nuevo internauta en un obsesivo ser que rebusca y relee toda la información que le fascina y que se puede encontrar en Internet. Este es quizás el grupo que más peligro acontece en la red ya que ponen en practica todo el software de *hacker* que encuentran en la red. Así es fácil ver como un Lamer prueba a diestro y siniestro un "bombeador de correo electrónico" esto es, un programa que bombardea el correo electrónico ajeno con miles de mensajes repetidos hasta colapsar el sistema y después se mofa auto denominándose *hacker*. También emplean de forma habitual programas sniffers para controlar la red, interceptan tu contraseña y correo electrónico y después te envían varios mensajes, con dirección falsa amenazando tu sistema, pero en realidad no pueden hacer nada más que cometer el error de que poseen el control completo de tu disco duro, aún cuando el ordenador esta apagado.

Lenguaje HTML (Hiper Text Markup Language): Conjunto de códigos usados para definir documentos de la Web. El navegador en el ordenador del usuario se fija en el HTML para determinar la forma en que deberían ser distribuidos los textos, gráficos y otros elementos multimedia.

Lenguaje: Mecanismos de expresión y codificación de instrucciones al computador, definido y gobernado por un conjunto de reglas y convenciones. Para el funcionamiento práctico debe existir al menos un intérprete o compilador que traduzca la instrucción del lenguaje propio del computador a otro accesible.

Lista de Revocación de certificados (Certificate Revocation List): Las autoridades de certificación deben establecer una lista de certificados digitales que no tienen validez por mucho tiempo.

Localizador de recurso uniforme (Uniform Resource Locator): Medios para identificar el recurso en Internet. Un localizador URL comienza con el nombre del protocolo necesario para conseguir los datos del servidor y continúa por la identificación del texto del recurso o fuente. Por ejemplo, una página Web es una fuente localizada en Internet y requiere el uso del protocolo http.

Marketing de relación (Relationship marketing): Marketing que crea relaciones con cada cliente individual.

Menús: Mecanismo de ingreso de órdenes mediante teclado para dirigir la acción del computador. Los menús están generalmente conformados por una serie de opciones o una letra asociada a ella. A diferencia de los comandos son necesarios datos adicionales para completar la especificación de la orden.

Microcomerciantes (Micromerchants): Aquellos que ofrecen sus artículos en Internet, intercambiándolos por dinero electrónico o digital.

Micropagos (Microcash): Pagos digitales nominales de pequeña cuantía.

Microsegmentación (Microsegmentation): Utilizar referencias muy detalladas de los consumidores para establecer grupos de mercados más pequeños.

Microtransacciones (Microtransactions): Transacciones a bajo coste y tiempo real utilizando micropagos.

Modem: Contracción del modulador. Equipo de comunicación que permite la transmisión de información e interconexión entre computadoras por medio de líneas telefónicas.

Monedero electrónico (Electronic wallet): Aplicación de ayuda para un navegador utilizada para trasladar un número de tarjeta de crédito encriptados desde un comprador, a través del vendedor al servidor, perteneciente a la compañía de crédito. (por ejemplo, CyberCash o Verifore) para su aprobación y consentimiento.

Navegadores Web (Web Browser): Programa de software que permite conectar con los servidores de la red para acceder a los documentos HTML y a sus archivos asociados (páginas Web) y seguir las conexiones de documento a documento o de página a página. El servidor puede estar en una red privada o en Internet. Las aplicaciones de ayuda pueden incorporarse con el navegador para manejar archivos especiales y aplicaciones.

Newbie: Es un novato, particularmente es aquel que navega por Internet, tropieza con una página de *Hacking* y descubre que existe un área de descarga de buenos programas de hackeo. Después se baja todo lo que puede y empieza a trabajar con los programas. Los Newbies aprenden el *Hacking*, siguiendo todos los pasos para lograrlo y no se mofa de su logro, si no que aprende.

Operador del sistema (Sysop): Persona responsable del funcionamiento de un sistema o de una red.

Paquete (Packet): La unidad de datos que se envía a través de una red. En Internet la información transmitida es dividida en paquetes que se reagrupan para ser recibidos en su destino.

Pasarela (Gateway): Hoy se utiliza el término router (direccionador, encaminador, enrutador) en lugar de la definición original de gateway. Una pasarela es un programa o dispositivo de comunicaciones que transfiere datos entre redes que tienen funciones similares pero implantaciones diferentes.

Periféricos: Partes del sistema utilizados para comunicarse con información de entrada y de salida, tales como teclado, impresora, etc.

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 procesamiento de datos.

Privacidad Bastante Buena (Pretty Good Privacy (PGP): Creado por Phil Zimmermann en 1995. Es un paquete completo de seguridad de correo electrónico que proporciona confidencialidad, validación de identificación, firmas digitales y compresión de texto, todo a precio cero. Hay versiones comerciales para las personas que requieren asistencia técnica. Es una aplicación de software de alta seguridad criptográfica para MSDOs, UNIX (LINUX), VAX/VMS, y otras computadoras. PGP permite a la gente a intercambiar archivos o mensajes con privacidad, autenticación y conveniencia. Privacidad significa que únicamente a los que se les envió el mensaje, podrán leerlo. Autenticación significa que un mensaje que aparece ser enviado por una persona, únicamente pudo ser originado por esa persona. Conveniencia significa que la privacidad y autenticación son proveídos sin el manejo de llaves asociadas con el software convencional de criptografía.

Programas compartidos (Shareware): Dícese de los programas informáticos que se distribuyen a prueba, con el compromiso de pagar al autor su precio, normalmente bajo, una vez probado el programa y/o pasado cierto tiempo de uso.

Programas de Aplicación: Conjunto de instrucciones sistematizadas que permiten al computador realizar tareas específicas.

Protocolo de Internet (Internet Protocol): Este protocolo trabaja sobre la red facilitando una dirección para los trabajos de Internet, y manejando el envío de paquetes a través de la misma.

Protocolo de Transferencia de Ficheros (File Transfer Protocol – FTP): Protocolo que permite a un usuario de un sistema acceder y transferir desde otro sistema de una red. Es también habitualmente el nombre del programa que el usuario invoca para ejecutar el protocolo.

Protocolo de transferencia de textos seguros (Secure Hypertext Transfer Protocol): Diseñado específicamente para apoyar el protocolo de transferencia de textos, suministra autenticidad para servidores y navegadores así como

confidencialidad e integridad de los datos para comunicaciones entre un servidor de la web y un navegador.

Proveedores de servicios de Internet (Internet service providers): Empresas que facilitan a clientes con conexiones a la red.

Proxy: Es una aplicación o programa especializado que se ejecuta en un host. Un proxy analiza el requerimiento del usuario para servicios de Internet y se encarga de procesarlo de acuerdo a las políticas de seguridad de la empresa. Un proxy actúa como un Gateway para los servicios a nivel de aplicación.

RAM: Memoria de acceso al azar o memoria de lectura y escritura.

Riesgo sistémico (Systemic risk): El riesgo de que el fallo en el cumplimiento de sus obligaciones de uno de los participantes en un sistema de transferencias, o en mercados financieros en general, genere una imposibilidad de cumplir con sus obligaciones a otros participantes o instituciones financieras, incluyendo obligaciones contractuales. Puede generar problemas de liquidez o de crédito, generando una inestabilidad en los mercados financieros.

ROM: Memoria únicamente de lectura utilizado generalmente para programas que deben encontrarse disponibles en forma permanente.

Servidor Web (Web Server): Programa de software que maneja los datos en el sitio web, controla el acceso a los mismos y responde a cuestiones planteadas por los navegadores de la web.

Sistema anfitrión, sistema principal / albergar, dar albergue (Host): Ordenador que, mediante la utilización de los protocolos TCP/IP, permite a los usuarios comunicarse con otros sistemas anfitriones de una red. Los usuarios se comunican utilizando programas de aplicación, tales como el correo electrónico, Telnet, www y FTP. La acepción verbal (to host) describe el hecho de almacenar algún tipo de información en un servidor ajeno.

Sistema Global para comunicaciones Móviles (Global System for Mobile communication – GSM): Sistema compatible de telefonía móvil digital desarrollado en Europa con la colaboración de operadores, administraciones públicas y empresas.

Sistema Operativo: Conjunto de instrucciones que permiten la interacción entre el computador y el usuario. Controla el funcionamiento del computador, interpretando y ejecutando los comandos recibidos, dirigiendo la información a su destino.

Sociedad o Corporación Virtual (Virtual corporation): Entidad formada por trabajadores dispersos geográficamente que comparten su trabajo y se comunican con medios electrónicos, con escasos o nulos contactos físicos.

Software: Programa que controla el funcionamiento del computador y permite que el hardware realice las instrucciones dadas.

Tarjetas inteligentes (Chip card): Una tarjeta que contiene uno o varios chips o circuitos integrados para propósitos de identificación, almacenamiento de datos y otros propósitos especiales utilizado para validar número de identificación personal, autorizar compras, verificar saldos de cuenta y grabar registros personales.

Tarjetas monedero (Smart cards): Tarjetas de crédito de tamaño similar a las de plástico con un circuito integrado especial implantado en ellas. El circuito integrado almacena información en formato electrónico y controla quién usa dicha información y de qué forma.

Teclado. Conjunto de teclas que al ser oprimidas provocan la iniciación de determinadas acciones del programa a ejecutar.

Transacciones electrónicas aseguradas (Secured electronic transaction): Desarrolladas por el consorcio formada por MasterCard y VISA. Son la combinación de un protocolo previsto para ser usado por otras aplicaciones (como navegadores de la web) y una forma estándar (procedimientos recomendados) para manejar las transacciones con tarjetas de crédito en Internet.

Transferencia automática de fondos en el punto de venta (Electronic funds transfer at the point of sale ETFPOS): Este término hace referencia a la utilización de tarjetas de pago en un punto de venta minorista. La información del pago se recoge en terminales electrónicos diseñados para transmitir la información.

Unix (UNIX): Sistema portátil robusto, flexible y portable muy utilizado en los ambientes Internet.

Virus (Virus): Programa que se duplica a si mismo en un sistema informático incorporándose a otros programas que son utilizados por varios sistemas. Estos programas pueden causar problemas de diversa gravedad en los sistemas que los almacenan.

Web: Red

Web site: Conjunto de documentos en la web, que habitualmente incluyen la página inicial y otras correlacionadas.

Bibliografía

ALONSO PÉREZ, Francisco. Introducción al Estudio de la Criminología. Editorial Reus S.A. Madrid, Año 1999.

ANDRÉS DOMÍNGUEZ, Ana Cristina. El delito de daños: Consideraciones jurídico-políticas y dogmáticas. Servicio de Publicaciones: Universidad de Burgos. Valladolid, Año 1999.

ARLUCEA, Esteban. Lecciones de Teoría Jurídica del Delito. Editorial Comares. Año, 1999.

BLOSSIERS, Juan José y **CALDERÓN GARCÍA**, Sylvia. Los Delitos Informáticos en la Banca. Editora Rao. Lima, Año 2000.

BRAMONT-ARIAS, Luis Alberto y **GARCÍA CANTIZANO**, M. C. Manual de Derecho Penal. Parte Especial. Editorial San Marcos. Lima, Año 1998.

BRAMONT-ARIAS, Luis Alberto. Código Penal Anotado. Editorial San Marcos. Lima, Año 1998

- El Delito Informático en el Código penal Peruano. Biblioteca de Derecho Contemporáneo. Vol. 6. Pontificia Universidad Católica del Perú. Lima, Año 1997.

- El delito informático. En Gaceta Jurídica. Tomo 81-B. Agosto. Informe Penal. Lima, Año 2000.

BRIZ, Julián. Internet y Comercio Electrónico. Editorial Esic. Madrid, Año 2000.

BRIZZIO R., Claudia. La Informática en el Nuevo Derecho. Abeledo-Perrot. Buenos Aires, Año 2000.

BUSTOS RAMIREZ, Juan. Manual de Derecho Penal. Tercera Edición. Editorial Ariel. Barcelona, Año 1989.

-Control Social y Sistema Penal. PPU. Barcelona, Año 1987.

CARBONELL MATEU, Juan Carlos. Derecho Penal. Concepto y Principios Constitucionales. Tirant lo blanch. Valencia, Año 1996.

Código Penal Alemán y Código Procesal Penal Alemán. Marcial Pons. Ediciones Jurídicas y Sociales S.A. Madrid, Año 2000.

Código Penal Español.

Código Penal Peruano.

Código de Procedimientos Penales.

Constitución Política del Perú.

Código Civil.

CHOCLÁN MONTALVO, José Antonio. La Organización Criminal. Tratamiento Penal y Procesal. Editorial Dykinson. Madrid, Año 2000.

DAVARA RODRÍGUEZ, Miguel Angel. De las Autopistas de la información a la sociedad virtual. Arazandi. Pamplona, Año 1995.

- Manual de Derecho Informático. Arazandi. Pamplona, Año 1997.

DE MIGUEL ASECIO, Pedro. Derecho Privado de Internet. Civitas Ediciones. Madrid, Año 2000.

DIEGO, Ma. Rosario y **SÁNCHEZ**, Virginia. Hacia un Derecho Penal Sin Fronteras. Editorial Colex. Madrid, Año 2000.

ESPINOZA CÉSPEDES, José Francisco. Contratación Electrónica, Medidas de Seguridad y Derecho Informático. Editora Rao. Lima, Año 2000.

FERNÁNDEZ ESTEBAN, M. L. : Nuevas tecnologías, Internet y derechos fundamentales. Madrid, Año 1998.

FERRÉ O., Juan y ANARTE B., Enrique. Delincuencia Organizada. Aspectos penales, procesales y criminológicos. Universidad de Huelva Publicaciones. Huelva, Año 1999.

FRÍGOLA VALLINA, Joaquín y ESCUDERO MORATALLA, José Francisco. Honor, secreto profesional en los medios de comunicación. Límites y aspectos jurídicos civiles y penales. Ediciones Revista General de Derecho. Valencia, Año 1998.

GARCÍA CAVERO, Percy. La responsabilidad penal del administrador de hecho de la empresa: Criterios de imputación. J.M. Bosch Editor. Barcelona, Año 1999.

GUTIERREZ ZARZA, Ángeles. Investigación y Enjuiciamiento de los Delitos Económicos. Editorial Colex. Madrid, Año 2000.

HERNÁNDEZ, Claudio. Los clanes de la Red. Año 2000. (Libro disponible en la Web).

HERRÁN ORTÍZ, Ana Isabel. La Violación de la Intimidad en la Protección de Datos Personales. Dykinson. Madrid, Año 1998.

HUERTA MIRANDA, Marcelo y LIBANO MANSSUR, Claudio. Delitos Informáticos. Editorial Jurídica Cono Sur. Santiago de Chile, Año 1998.

JAKOBS, Günther. Derecho Penal Parte General. 2ª. Ed. Marcial Pons. Madrid, Año 1997.

- La ciencia del Derecho Penal ante las exigencias del presente. Estudios de Derecho Judicial Nº 20. Galicia, Año 1999.
- Estudios de Derecho Penal. Editorial Civitas. Madrid, Año 1997.
- Sociedad, Norma y Persona en una Teoría de un Derecho Penal Funcional. Cuadernos Civitas. Madrid, Año 1996.

JAKOBS, Günther; CANCIO MELIÁ, Manuel. El Sistema Funcionalista del Derecho Penal. Editorial Grijley. Lima, Año 2000.

JAKOBS, Günther y STRUENSEE, Eberhard. Problemas Capitales del Derecho Penal Moderno. Buenos Aires, Año 1998.

JIJENA LEIVA, Renato. Chile, La protección penal de la intimidad y el delito informático. Editorial Jurídica de Chile. Santiago de Chile, Año 1992.

JULIÁ BARCELÓ, Rosa. Comercio electrónico entre empresarios. Tirant lo blanch. Valencia, Año 2000.

LESCH, H. La Función de la Pena. Trad. de Sánchez - Vera Gómez- Trelles. Dykinson. Madrid, Año 1999.

LLANEZA GONZÁLEZ, Paloma. Internet y comunicaciones digitales. Bosch Editor. Barcelona, Año 2000.

MANGLIOLA MARKOVITCH, Claudio Paul y **LÓPEZ MEDEL**, Macarena. Delincuencia y Fraude Informático. Derecho Comparado y Ley 19.223. Editorial Jurídica de Chile. Santiago de Chile, Año 1999.

MARTÍN BANDI, P. y **HÉCTOR FRAGA**, P. En Crisis Informática del año 2000. Ediciones Abeledo-Perrot. Buenos Aires, Año 1999.

MARCHENA GÓMEZ, Manuel. Prevención de la delincuencia tecnológica. Derecho de Internet. Contratación Electrónica y Firma Digital. **MATEU DE ROS**, Rafael y **CENDOYA MENDEZ DE VIGO**, Juan Manuel. (Coordinadores) Autores Varios. Arazandi Editorial. Navarra, Año 2000.

MATELLANES RODRÍGUEZ, Nuria. Algunas notas sobre las formas de delincuencia informática en el Código penal. En Hacia un Derecho Penal sin fronteras. Colex. Madrid, Año 2000.

MAZUELOS COELLO, Julio. Derecho Penal Económico y de la Empresa. Doctrina Penal Española y Alemana. Editorial San Marcos. Lima, Año 1996.

MIR PUIG, Santiago. Derecho Penal. Parte General. Cuarta Edición PPU. Barcelona. Año, 1996.

MONTERO PASCUAL, Juan J. Competencia en las Telecomunicaciones Móviles. Tirant lo blanch. Valencia, Año 2000.

MORÓN LERMA, Esther. Internet y Derecho Penal: *Hacking* y otras conductas ilícitas en la red. Editorial Aranzadi. Pamplona, Año 1999.

MUÑOZ CONDE, Francisco y **GARCÍA ARAN**, Mercedes. Derecho Penal. Parte General. Tercera Edición. Valencia, Año 1998.

MUÑOZ MACHADO, Santiago. La Regulación de la Red. Poder y Derecho en Internet. Grupo Santillana de Ediciones. Madrid, Año 2000.

NÚÑEZ PONCE, Julio César. Software: Licencia de uso, derecho y empresa. Universidad de Lima. Lima, Año 1998.

- Derecho Informático, nueva disciplina jurídica para una sociedad moderna. Marsol. Trujillo, Año 1996.
- El Habeas Data y la Protección jurídica de la información computarizada. Universidad de Lima. En separata IUS ET PRAXIS N° 21-22. Lima, Año 1993.

PEÑARANDA RAMOS, Enrique, **SUAREZ GONZÁLEZ**, Carlos y **CANCIO MELIÁ**, Manuel. Un Nuevo Sistema del Derecho Penal. Consideraciones sobre la teoría de la imputación de Günther Jakobs. Editora Grijley. Lima, Año, 1998.

RAMOS NÚÑEZ, Carlos. Como hacer una tesis de Derecho y no envejecer en el intento. Gaceta Jurídica. Lima, Año 2000.

RIQUERT, Marcelo Alfredo. Informática y Derecho Penal Argentino. Editora Ad Hoc. Buenos Aires, Año 1999.

ROXIN, Claus. Derecho Penal. Parte General. Tomo I. La Estructura de la Teoría del Delito. Civitas Ediciones. Madrid, Año 2000.

- Política Criminal y Estructura del Delito. Elementos del Delito en base a la Política Criminal. Editorial Promociones y Publicaciones Universitarias S.A. Barcelona, Año 1992.

RODAS MONSALVE, Julio Cesar. Protección Penal del Medio Ambiente. PPU. Barcelona, Año 1993.

RUIZ CARRILLO, Antonio. Los datos de carácter personal. Bosch Editor. Barcelona, Año 1999.

SÁNCHEZ BLANCO, Angel. Internet. Sociedad, empresa y poderes públicos. Editorial Comares. Granada, Año 2000.

SANCHEZ DE DIEGO, M. Transparencia de las bases de datos como mecanismo de protección de la intimidad de las personas. Idn° 4. Año 1994.

SEGURA GARCÍA, María José. El Consentimiento del Titular del Bien Jurídico en Derecho Penal. Tirant lo blanch. Valencia, Año 2000.

SIEBER, Ulrich. The International Handbook on Computer. Jhon Wiley & Sons Ltda. Londres, Año 1986.

SILVA SÁNCHEZ, Jesús María. Aproximación al Derecho Penal Contemporáneo. Bosch Editores. Barcelona, Año 1992.

- La expansión del Derecho Penal. Aspectos de la política criminal en las sociedades postindustriales. Civitas. Madrid, Año 1999.

STERLING, Bruce. *The Hacker Crackdown. LA Caza de Hackers. Ley y Desorden en la Frontera Electrónica.* Texas, Año 1994 (Libro disponible en la Web).

STEFIK, Mark. *The Internet Edge. Social, Technical and Legal Challenges for a Network World.* Massachusetts Institute of Technology. Massachusetts, Año 2000.

TIEDEMANN, Klaus. *Derecho Penal y Nuevas Formas de Criminalidad.* Idemsa. Lima, Año 2000.

- *Temas de derecho penal económico y ambiental.* Idemsa. Lima, Año 1999.

TÉLLEZ VALDES, Julio. *Derecho informático. Segunda Edición.* McGraw Hill. México, Año 1995.

VIVES ANTÓN, Tomás S. *Fundamentos del Sistema Penal.* Editora Tirant lo Blanch. Valencia, Año 1996.

VIVES ANTÓN, T. S., **BOIX REIG**, J., **ORTS BERENGUER**, E., **CARBONELL MATEU**, J.C. Y **GONZÁLES CUSSAC**, J.L. *Derecho Penal. Parte Especial.* Tirant lo blanch. Valencia, Año 1999.

VILLAR URIBARRI, J.M. *Firma Electrónica y Seguridad Jurídica en Internet. Informática y Derecho en Internet.* Mérida, Año 2000.

Bibliografía de boletines y revistas

1. Arteaga, S. El delito informático: Algunas consideraciones jurídicas penales. *Revista de la Facultad de Ciencias Jurídicas y Políticas* Universidad Central de Venezuela. N° 68. Año 33. Caracas. 1987.
2. Bianchi, Roberto A. En *Revista La Ley*. 06 de junio del año 2000. Buenos Aires, Año 2000.
3. Boletín de Noticias N° 179 del Instituto Peruano de Comercio Electrónico. Agosto del año 2000.
4. Boletín de Noticias N° 7 del Instituto Peruano de Comercio Electrónico. Marzo del año 2000.
5. Chacón de Albuquerque. Combate a Pornografía Infanto-Juvenil en Internet. En *Revista Electrónica de Derecho Informático*. <http://publicaciones.derecho.org/redi/No.26-Septiembre2000/2>.
6. Cid Moliné, José. Garantías y Sanciones. Argumentos contra la tesis de la identidad de las garantías entre las sanciones punitivas". En *Revista de Administración Pública*. N° 140. Mayo-Junio. Año 1996.

7. Colección Informática Fácil. Los Macrovirus y Antivirus Informáticos N°32. Publicación del Instituto Nacional de Estadística e Informática. Lima. 2000.
8. Colección Seguridad de la Información N° 2. Amenazas en Internet. Publicación del Instituto Nacional de Estadística e Informática. Lima. 2000. Revista Iberoamericana de Derecho Informático. Informática y Derecho. N° 33. Edita Universidad Nacional de Educación a Distancia. Centro Regional de Extremadura en Mérida. Año 2000.
9. Cuervo Alvarez. Delitos Informáticos: Protección penal de la intimidad. En Revista Electrónica de Derecho Informático. <http://publicaciones.derecho.org/redi/No.06-enerode1999/cuervo>.
10. Del Río Fernández, L. La autoría en organizaciones complejas en Cuadernos de Derecho Judicial. Fenómenos Delictivos Complejos. Madrid, Año 1999.
11. Diario El Comercio. Sección de Internet. Lima, 4 de Junio del año 2000. Pp. E14.
12. Diario El Peruano. Sector Justicia: Aprueban el Reglamento sobre la aplicación de normas que regulan el uso de tecnologías avanzadas en materia de archivo de documentos e información a entidades públicas y privadas. Lima, 26 de Marzo del 2000. Pp. 185081.
13. Diario El Peruano. Sección de Derecho. Lima, 03 de Febrero del 2000. Pp. 10.
14. Diario El Peruano. Sección de Derecho. Lima, 18 de Febrero del 2000. Pp. 10.
15. Diario El Peruano. Sección de Derecho. Lima, 30 de Mayo del 2000. Pp. 10.
16. Diario El Peruano. Sección de Economía. Lima, 15 de enero del año 2001. Pp. 22.
17. Diario El Peruano. Sección de Economía. Lima, 4 de enero del año 2001. Pp. 21
18. Diario El Peruano. Sección de Economía. Lima, 8 de enero del año 2001. Pp. 21.
19. Diario El Peruano. Sección de Tecnología. Suplemento Especial. Lima, 04 de Abril del 2000. Pp. 2-3.
20. Diario El Peruano. Sección Jurídica. Lima, 09 de Enero del 2001. Pp. 28.
21. Diario El Peruano. Sector Justicia: Aprueban el Reglamento sobre la aplicación de normas que regulan el uso de tecnologías avanzadas en materia de archivo de documentos e información a entidades públicas y privadas. Lima, 26 de Marzo del 2000.
22. Figoli, Andrés. El Acceso no Autorizado a Sistemas Informáticos. En Revista Electrónica de Derecho Informático. http://publicaciones.derecho.org/redi/No.17_diciembre_de_2000/14.
23. Gómez Pérez, Mariana. Criminalidad Informática. Un fenómeno de fin de siglo. En Revista Electrónica de Derecho Informático. http://publicaciones.derecho.org/redi/No.10_mayo_de_1999/mariana.
24. Herrera Bravo. Reflexiones sobre los Delitos Informáticos motivadas por los desaciertos de la Ley Chilena. En Revista Electrónica de Derecho Informático. http://publicaciones.derecho.org/redi/No.05_Diciembre_de_1998/herrera.
25. Hurtado Falvy, Juan Manuel. Introducción a los Delitos Informáticos en la Legislación Peruana. En la Revista Derecho y Sociedad editada por los estudiantes de la F.D.P.U.C.P. N° 15. Año XI, 2000. Pp. 311-320.
26. Informática y Derecho 30-32. Revista Iberoamericana de Derecho Informático. Universidad Nacional de Educación a Distancia. Centro Regional de Extremadura Mérida. Año, 1999.
27. Jeangeorges. El primer fallo que ampara el E-mail en la Argentina.- Caso de violación y publicación indebida. En Revista Electrónica de Derecho Informático. http://publicaciones.derecho.org/redi/No.21_abril_de_999/1.
28. Jiménez Dan, Rafael Ricardo. Crimen Silencioso. En Revista Electrónica de Derecho Informático. http://publicaciones.derecho.org/redi/No.10_Mayo_de_1999/jimenez.
29. Líbano Manssur, Claudio. Los Delitos de *Hacking* en sus Diversas Manifestaciones. En Revista Electrónica de Derecho Informático. http://publicaciones.derecho.org/redi/No.21_abril_de_2000/4.

30. Mazuelos Coello, Julio F. Del Hommo Sapiens al Homo Digitalis: Los retos del Derecho penal. En Revista Legal del Estudio Muñiz, Forsyth, Ramirez, Pérez-Taiman y Luna-Victoria Abogados. Mayo del año 2000. Pp 10 y ss.
31. Mazuelos Coello, Julio F. Protección Jurídico Penal de la Información como valor económico de la empresa. En Revista Legal del Estudio Muñiz, Forsyth, Ramirez, Pérez-Taiman y Luna-Victoria Abogados. Marzo de 1999. Pp 38 y ss.
32. Nuñez Ponce, Julio. Los Delitos Informáticos. En Revista Electrónica de Derecho Informático.
http://publicaciones.derecho.org/redi/No.15_octubre_de_1999/6.
33. Revista de Derecho de Daños. Tomo II. La prueba del daño. Editorial Rubinzal-Culzoni. Buenos Aires, Año 1999.
34. Reyna Alfaro, Luis Miguel. El bien jurídico en el delito informático 2001. Revista Jurídica del Perú. N° 21. Lima, Año 2001.
35. Reyna Alfaro, Luis Miguel. VIII Congreso Iberoamericano de Derecho e Informática. Tema: Los Delitos Informáticos en el Código penal Peruano: Análisis del tipo de injusto de los Art. 207a, 207b y 207c del C.P. peruano y propuestas de política criminal. En revista Memorias. México 21 a 25 de Noviembre del 2000.
36. Sánchez Almeida, Carlos. El *Hacking* ante el Derecho Penal. Una visión libertaria. En Revista Electrónica de Derecho Informático. http://publicaciones.derecho.org/redi/No.13_agosto_de_1999/ponencia.
37. Vega Lozada, Fredrick. VIII Congreso Iberoamericano de Derecho e Informática. Tema: Hostigamiento sexual virtual: Perspectivas del ordenamiento jurídico de Estados Unidos de Norteamérica. En revista Memorias. México 21 a 25 de Noviembre del 2000.
38. Ventura Monfort. La estafa cometida mediante la utilización de medios informáticos. En Revista Electrónica de Derecho Informático. http://publicaciones.derecho.org/redi/No.06_enero_de_1999/ventura.
39. Viega Rodríguez, María José. Delitos Informáticos. En Revista Electrónica de Derecho Informático.
http://publicaciones.derecho.org/redi/No.09_abril_1999/viega.
40. Viega Rodríguez, María José. La Piratería del Software ¿es un delito? Análisis de las respuestas dictadas en fallos de Uruguay y Argentina. En Revista Electrónica de Derecho Informático.
http://publicaciones.derecho.org/redi/No.05_diciembre_de_1998/viega.
41. Villalba Díaz. Los delitos y contravenciones informáticas. Los *Hackers* y el Código Contravencional de la Ciudad de Buenos Aires. En Revista Electrónica de Derecho Informático. http://publicaciones.derecho.org/redi/No.23_junio_de_2000/5.

-

Tesis consultadas

-

Título : El contrato de licencia de uso de software en la empresa:

Regulación Jurídica adecuada.

Autor : Julio César Núñez Ponce.

Título : Los seguros sobre bienes informáticos.

Autor : Beepe Gualino Noce.

Título : Responsabilidad civil en la informática.

Autor : Juan Carlos Peralta Castellano.

Título : Contratación Electrónica, Medidas de Seguridad y Derecho Informático

Autor : José Francisco Espinoza Céspedes.

Título : Proceso de elaboración de la ley penal.

Autor : César Augusto Nakasaki Servigon.

-

-

-

Diccionarios consultados

-

-

-

-

-

-

1. Calvo Beca, Rafael. Diccionario Inglés – Español Informático, Electrónico y General. Segunda Edición. Madrid, Año 1994.

2. Diccionario de la Lengua Española. Real Academia Española. Vigésima Primera Edición. Editorial Espasa Calpe S.A. Madrid, Año 1997.

3. Diccionario Enciclopédico Práctico. Norma Editorial. Lima, Año 1995.

4. Köbler. Rechtsspanisch. Deutsch-spanisches und spanisch-deutsches. Von Gerhard Köbler. München, Año 1997.

Páginas web consultadas

1. <http://www.informatica-juridica.com/jurisprudencia.asp>
2. <http://www.icann.org/udrp/proceedings-stat.htm>
3. <http://www.cybercrime.gov/>
4. <http://www.cybercrime.gov/compcrime.html>
5. <http://www.cybercrime.gov/compcrime.html#VIIIc>
6. <http://www.cybercrime.gov/compcrime.html#VIIId>
7. http://publicaciones.derecho.org/redi/Index_General_/16
8. <http://v2.vlex.com/vlex2/front/asp/default.asp>
9. <http://www.delitosinformaticos.com/>
10. <http://www.delitosinformaticos.com/legislacion/europea/>
11. <http://vlex.com/pe/canales/Derecho%20Penal/>
12. <http://www.delitosinformaticos.com/noticias/index.shtml>
13. <http://www.delitosinformaticos.com/casos/>
14. <http://www.ruta66.org/>
15. <http://www.europa.eu.int/en/record/green/gp9610/protec.html>
16. <http://www.metacrawler.com>
17. <http://webopedia.com>
18. <http://www.whatis.com>
19. http://gahtan.com/cyberlaw/criminal_law
20. <http://cybercrimes.net/index/>
21. http://derecho_informaticos.com/delitos%20informaticos.html
22. <http://mailer.fsu.edu/carrwelcome.html>
23. http://stlr.stanford.edu/stlr/cove_page/index.html
24. <http://richmond.edu/jolt/v7i3/index.html>
25. <http://cybercrimex.net>
26. [http://www.ecommercetimes.com/printer/.](http://www.ecommercetimes.com/printer/)
27. <http://www.bitniks.es>
28. [http://www.infoweek.com.mx.](http://www.infoweek.com.mx)

29. <http://www.kriptopolis.com/tlib/20000507.html>
30. <http://conventions.coe.int/treaty/en/projets/cybercrime.htm>
31. <http://ecija.com>
32. <http://www.hispasec.com/unaaldia.asp?id=553>
33. <http://www.gmx.net>
34. <http://www.delitosinformaticos.com/articulos/protempleo.htm>.
35. <http://www.newbytes.com/pubnews/00/145086.html>
36. <http://www.delitosinformaticos.com/articulos/freenet.htm>
37. <http://www.bufetalmeida.com/intro.htm>
38. <http://web2.airmail.net/walraven/romance.htm>
39. <http://ww2.grn.es/merce/ciberamor.html>
40. <http://www.webpersonals.com>
41. <http://www.match.com>
42. <http://www.lovingyou.com>
43. <http://www.delitosinformaticos.com/articulos/freenet.htm>
44. <http://www.diarioti.com/noticias/2000/may2000/15193090.htm>
45. <http://www.youvebeenhack.com>
46. http://publicaciones.derecho.org/redi/No._06_Enero_de_1999/cuervo
47. http://publicaciones.derecho.org/redi/No._09_-_Abril_de_1999/viega
48. <http://cnnenespanol.com/2001/tec/02/27/museo/index.html>
49. <http://iecl.iuscomp.org/gla/statutes/BDSG.html>
50. <http://www.kronegger.at/recht/b5.htm>
51. http://europa.eu.int/comm/internal_market/en/media/dataprot/law/impl.html
52. <http://comunidad.derecho.org/congreso/ponencia29.html>
53. <http://www.geocities.com/CapeCanaveral/2566/>
54. <http://www.geocities.com/CapeCanaveral/2566/seguri/seguri.html>
55. <http://www.kriptopolis.com/>
56. <http://www.geocities.com/CapeCanaveral/2566/intro/mecanism.html>
57. <http://delitosinformaticos.com/noticias/98395846971449.htm>
58. <http://publicaciones.derecho.org/redp>
59. <http://www.mgap.gub.uy>
60. <http://www.mtss.gub.uy>

61. <http://www2.compendium.com.ar/juridico/depablo.html>
62. http://publicaciones.derecho.org/redi/No.13_agosto_de_1999/ponencia
63. <http://www.delitosinformaticos.com/noticias/98353057377944.htm>
64. <http://delitosinformaticos.com/noticias/98404275043664.htm>
65. <http://delitosinformaticos.com/noticias/98378704517479.htm>
66. <http://www.latinlex.com/cl/contenido/leg4.asp>.
67. http://publicaciones.derecho.org/redi/No._20_marzo_del_2000/14
68. http://publicaciones.derecho.org/redi/No.05_Diciembre_de_1998/herrera
69. http://europa.eu.int/eur-lex/es/lif/dat/1999/es_499X0364.html

Índice

PORTADA.....	I
DEDICATORIA	II
AGRADECIMIENTOS.....	III
SUMARIO.....	IV
ÍNDICE DE LAS ABREVIATURAS.....	V
INTRODUCCIÓN.....	VI

Primera Parte

APROXIMACIÓN AL TEMA

CAPÍTULO I: ANÁLISIS DE LA REALIDAD

INTRODUCCIÓN.....	1
1.1 Incidencia Social de las Computadoras.....	2
1.2 Informática y Proceso de Comunicación de las Personas en la Red.	6
1.2.1 Breve Reseña Histórica.	6
1.2.2 Nuevas Formas de Comunicación...	7
1.2.2.1 Internet Relay Chat	7
1.2.2.2 El Correo Electrónico	8
1.3 Principales Características de la Red.	11
1.3.1 El Ciberespacio	11
1.3.2 El Anonimato	13
1.4 Los sujetos en la Red	15
1.4.1 Cinco Categorías.....	15
1.5 Necesidad de Regulación de Internet	17
1.5.1 Origen de Internet..	17
1.5.2 Contenidos Ilegales en Internet..	19
1.5.3 La Free Net	22
1.5.4 Amenazas en Internet .	23

CAPÍTULO II: ALGUNAS PRECISIONES ACERCA DE LA CRIMINALIDAD INFORMÁTICA COMO NUEVA FORMA DE CRIMINALIDAD

La Criminalidad Informática....	29
1.1 Aspectos generales de la criminalidad informática.....	29
1.2 Conductas nocivas que se cometen a través de sistemas informáticos y de Internet.....	36
1.2.1 Introducción de datos falsos o “Data Diddling”.	37
1.2.2 El Caballo de Troya o “Trojan Horse”.	38
1.2.3 El Salame, Redondeo de Cuentas o “Rounding Down”	40
1.2.4 Uso Indevido de Programas o “Superzapping”	41
1.2.5 Puertas Falsas o “Traps Doors”	44
1.2.6 Bomba Lógicas o “Logic Bombs”	45
1.2.7 Ataques Asincrónicos o “Asynchronic Attacks”	47
1.2.8 Recojo de Información Residual o “Scavenging”	49
1.2.9 Divulgación No Autorizada de Datos o “Data Leakage”	51

1.2.10	Acceso a Áreas No Autorizadas o “Piggyn Baking”	51
1.2.11	Suplantación de la personalidad o “Impersonation”	52
1.2.12	Interferencia de Líneas Telefónicas o “Wiretapping”	53
1.2.13	Hurto de Tiempo	53
1.2.14	Simulación e Imitación de Modelos o “Simulation and Modeling”	53
1.3	Conductas nocivas e ilícitas según la Organización de las Naciones Unidas...	54
1.4	Otras conductas no previstas.....	55

Segunda Parte

LOS DELITOS INFORMÁTICOS: MARCO LEGAL

CAPÍTULO I : DELIMITACIÓN CONCEPTUAL DEL DELITO INFORMÁTICO

1.1	Concepto de Delito.	58
1.2	El Concepto de Delito Informático.....	61
1.3	Delimitación de Bien Jurídico protegido de los Delitos Informáticos.....	68
1.3.1	Función del Derecho Penal....	68
1.3.2	La Función de Tutela de Bienes Jurídicos	69
1.3.3	La Función de Tutela de la Vigencia de las Normas	73
1.3.4	Posición personal respecto de la función del Derecho Penal....	76
1.4	El contenido del bien jurídico protegido en los Delitos Informáticos.....	79
1.4.1	La Intimidad como bien jurídico protegido	80
1.4.2	El Patrimonio como bien jurídico protegido	91
1.4.3	El Honor como bien jurídico protegido	94
1.4.4	La Libertad Informática... 105	
1.4.4.1	La Libertad Informática en el Derecho Comparado	111
1.4.5	La Seguridad Informática... 115	
1.4.6	La Información... 124	
1.5	Posición personal respecto del bien jurídico en los Delitos Informáticos...	132
1.5.1	Fundamentación Constitucional	133
1.5.2	Fundamentación Jurídico - Penal	138

CAPÍTULO II : POSICIÓN PERSONAL RESPECTO DEL CONCEPTO DE DELITO INFORMÁTICO.

- 1.1 Posición personal respecto del concepto de Delito Informático..... 144
- 1.2 Clasificación de los Delitos Informáticos..... 148
- 1.3 Principales manifestaciones de Delincuentes Informáticos..... 151
 - 1.3.1 Piratas o *Hackers* 151
 - 1.3.2 *Crackers*..... 152
 - 1.3.3 *Phreakers* 152
- 1.4 Tipología del “Delincuente Informático”..... 154

CAPÍTULO III: LOS DELITOS INFORMÁTICOS EN EL CODIGO PENAL PERUANO

- 1.1 Introducción 160
- 1.2 Ubicación Sistemática 165
- 1.3 Análisis de la Ley N° 27309 – “Ley de Delitos Informáticos”.... 167
- 1.4 El Delito de Intrusismo Informático - Art. 207-A 168
- 1.5 El Delito de Daño Informático - Art. 207-B 175
- 1.6 El Delito Informático Agravado - Art. 207-C..... 178
- 1.7 Aspectos problemáticos de la tipificación de los delitos informáticos en la legislación penal peruana. 180
 - 1.7.1 Exceso del uso de elementos subjetivos en los tipos penales informáticos 181
 - 1.7.2 El Principio de Territorialidad 186
 - 1.7.3 La inexistencia de peritos informáticos en el Perú 190
 - 1.7.4 Ausencia de proporcionalidad de las penas establecidas 191
 - 1.7.5 Principio de *Ultima Ratio* 192

CAPÍTULO IV : LOS DELITOS INFORMÁTICOS EN LA LEGISLACIÓN COMPARADA

Introducción 194

- 1.1 Alemania 194
- 1.2 España. 204
- 1.3 Estados Unidos de Norte América..... 212
- 1.4 Chile.... 220

Tercera Parte

PROPUESTA DE *LEGE FERENDA*

CAPÍTULO I : FUNDAMENTOS DE LA REGULACIÓN ADMINISTRATIVA

1.1 Necesidad de un ente regulador.....	232
1.2 Propuesta	235
1.2.1. Reformulación de los tipos penales del Delito Informático.....	235
1.2.2. Proyecto de Ley.....	238

CONCLUSIONES..... 242

GLOSARIO DE TÉRMINOS. 246

BIBLIOGRAFÍA..... 270

BIBLIOGRAFÍA DE BOLETINES Y REVISTAS..... 276

TESIS CONSULTADAS..... 280

DICCIONARIOS CONSULTADOS..... 281

PÁGINAS WEB CONSULTADAS..... 282

ÍNDICE..... 285

[1] MATELLANES RODRÍGUEZ, Nuria. Algunas notas sobre delincuencia informática en el Código penal. Hacia un derecho penal sin fronteras. Colex. Madrid, Año 2000. Pp. 129.

[2] Al respecto, un punto importante sobre la incidencia que tiene la informática en la banca, es la opinión de la Organización de Cooperación de Desarrollo Económico (OCDE), que cree que la banca por Internet eleva el riesgo de lavado de dinero negro con relación a la banca convencional, según un informe realizado por su Grupo de Trabajo sobre el Blanqueo de Capitales, que agrupa a expertos sobre este tema de los países desarrollados. El informe sobre modalidades de blanqueo de dinero 2000-2001, de fecha 1 de febrero del año 2001, señala que aunque la banca *online* puede ser una modalidad financiera segura, ésta tiende a agravar ciertos riesgos convencionales de blanqueo de dinero. Igualmente, vinculan a 10 bancos de los Estados Unidos a lavado de dinero. El BTCB logró abrir cuentas en varios bancos de Estados Unidos y canalizó a través de ellos más de US\$ 85 millones, incluyendo millones resultantes del lavado de dinero, fraude financiero y apuestas ilegales en Internet. En sus recomendaciones, el informe preconiza "impedir a los bancos de Estados Unidos abrir cuentas de correspondencia a bancos ficticios" y aplicar al pie de la letra las medidas de lucha contra el lavado de dinero. En <http://www.delitosinformaticos.com/articulos/freenet.htm>. Fecha de acceso: 10 de Febrero del año 2001.

[3] MARTÍN BANDI, P. y HÉCTOR FRAGA, P. Crisis Informática del año 2000. Ediciones Abeledo-Perrot. Buenos Aires,

Año 1999. Pp. 11.

[4] SÁNCHEZ BLANCO, Ángel. Internet. Sociedad, empresa y poderes públicos. Editorial Comares. Granada, Año 2000. Pp. 26, en donde se señala que “la madre de un investigador del Instituto Tecnológico de Massachussets que rechazo de su hijo el regalo de un ordenador cuando tenía setenta años y que, cumplidos los ochenta años, le pidió que le comprara el ordenador que inicialmente rechazó. En diez años la madre había sufrido los efectos de la artritis y de pérdida de vista y, aunque no podía utilizar una pluma o un bolígrafo con la mano artrítica, sí podía teclear en el ordenador y ampliar lo escrito mediante el *zoom* y, de este modo, mantener su correspondencia mediante el correo electrónico. Con este dato, es apreciable el interés de Internet como medio para una tercera edad integrada en la comunidad social y familiar.”

[5] SÁNCHEZ BLANCO, Ángel. *Op. Cit.* Pp. 27. E.g. en lo casos de invidentes, el conversor de texto-habla y el cumplimiento del protocolo www.c permite a las personas privadas de la vista poder escuchar los textos y descripciones incorporadas a las páginas web, la dislexia y las dificultades para la disciplina secuencial de la lectura, tiene la precisa alternativa de la utilización de Internet en los procesos educativos y la normal utilización de las páginas web con su técnica de hipertexto.

[6] El bit es considerado como la unidad mínima de información digital que puede ser tratada por un ordenador, proviene de la contracción de la expresión binary digit (dígito binario).

[7] Un ejemplo de ello resultan los portales de búsqueda de empleo, los mismos que presentan una serie de irregularidades como el no mostrar en la página de inicio alguna información sobre su política de privacidad, no informar cual es la finalidad de la recogida de datos ni destinatarios del mismo, etc. En <http://www.delitosinformaticos.com/articulos/protempleo.htm>. Fecha de acceso: 12 de diciembre del año 2000. De igual manera en Boletín de Noticias N°7. del Instituto Peruano de Comercio Electrónico. 7 de marzo del año 2000. Pp. 3, en donde se señala que la Red no es el mejor camino para encontrar un trabajo, dado la encuesta de Drake Bearn Morin, la mayor agencia de empleo a nivel mundial y subsidiaria del gigante de la publicidad, Harcourt, Inc., encontró que mientras el mercado favorece a los empleados, el buscador de un trabajo en la Internet no lo hace. <http://www.newbytes.com/pubnews/00/145086.html>

[8] En este sentido, VILLAR URIBARRI, J. M. Firma Electrónica y Seguridad Jurídica en Internet. Informática y Derecho en Internet. Mérida, Año 2000. Pp. 118, en donde se establece que el desarrollo tecnológico no sólo es necesario para desempeñar actividades empresariales o profesionales, sino incluso también numerosas actividades personales.

[9] SILVA SÁNCHEZ, Jesús María. La Expansión del Derecho Penal. Aspectos de la política criminal en las sociedades postindustriales. Civitas Ediciones. Madrid, Año 1999. Pp. 68.

[10] Diario El Peruano. Lima, 31 de enero del año 2001. En Internet y el Perú. Tribunal Libre / Opinión. Pp. 12.

[11] *Ibidem.*

[12] Diario Gestión. Sección Negocios. Lima, 26 de Enero del año 2001. Pp. 26.

[13] Diario El Peruano. 26 de enero del año 2001. En Inversión publicitaria en Internet crecería 300% este año. Sección Economía. Pp. 21.

[14] Para poder acceder a un servidor IRC es necesario contar con un programa que nos permita la conexión y dialogar con los restantes usuarios. En cada servidor IRC hay decenas de canales de discusión. Los canales disponibles son de 4 tipos: canales públicos y abiertos a todos los participantes, los canales secretos, los canales ocultos y los canales comprimidos. Luego, una vez establecido el contacto con el servidor a través del programa, es necesario elegir un apodo (*nickname*) que será el nombre con que uno se identificará, protegiendo de esta forma la identidad. Finalmente, los participantes de un mismo canal se presentan a lo largo de una lista. A partir de este momento, lo que uno escribe en el teclado es visto por los demás participantes del canal, pero también es posible mantener conversaciones privadas con alguno de ellos. Para ello se debe clicar sobre su *nickname*, con lo que aparecerá una especie de caja donde uno puede escribir su mensaje, enviar fotos archivos de texto, etc. Asimismo, cuando algún otro miembro del canal nos quiere enviar un mensaje privado, aparecerá en la pantalla un icono con su *nickname*, el cual, al ser clicado, nos mostrará el mensaje. Otro elemento importante que apareció a medida que se fue desarrollando la cultura del IRC, es la utilización de los emoticones, es decir, dos o más caracteres que simbolizan un sentimiento o estado de animo. Se sugiere observarlos girando la cabeza hacia la izquierda y con un poco de imaginación; a modo de ejemplo: :-) representa una sonrisa, una formulación sarcástica o una broma, :(al usuario no le ha gustado una frase

o está deprimido. En <http://www.guias.se/~oscar/adiccion/comunicacion.html>. Fecha de acceso: 21 de Febrero del año 2001.

[15] E.g., en Estados Unidos ya han surgido *sites* de ayuda a los adictos a los *Chats*, a Internet, al correo electrónico, etc. La ayuda consiste en comunicarse vía e-mail o a través de algún canal de Chat y recibir consejos. Pero la paradoja de ello reside en que para poder salir de una adicción, uno sigue recreándola a través de los medios que ofrecen para la cura. Un conciso análisis en <http://www.guias.se/~oscar/adiccion/comunicacion.html> Fecha de acceso: 21 de febrero del año 2001.

[16] Pese a todos los beneficios existentes gracias al correo electrónico, existe también un aspecto negativo y es el caso de dos adolescentes japonesas, que se conocieron a través de la Red. Las jóvenes fueron encontradas medio desangradas y gravemente heridas en la calle fuera de un edificio en Iizuka, en la provincia de Fukuoka (sureste de Tokio). Según la policía, parecía un intento de suicidio. Los investigadores de la Policía sospechan que las dos chicas, una de 14 años y la otra de 17, saltaron desde la cuarta planta del edificio deshabitado. Otra agencia japonesa, Jiji Press, informó que la joven de 14 años le había dicho hacía poco a una compañera de clase que iba a suicidarse "por lo que le ha pasado a mi amiga con la que me escribo por e-mail". En <http://delitosinformaticos.com-/noticias/98370553075358.htm> Fecha de acceso: 05 de marzo del año 2001.

[17] En este sentido, MORÓN LERMA, Esther. Derecho y Proceso Penal. Internet y Derecho Penal: Hacking y otras Conductas Ilícitas en la Red. Editorial Arazandi. Navarra, Año 1999, Pp. 92.

[18] Sobre Contratación Electrónica. Vid. ESPINOZA CÉSPEDES, José Francisco. Contratación Electrónica, Medidas de Seguridad y Derecho Informático. Editora Rao. Lima, Año 2000.

[19] DE MIGUEL ASECIO, Pedro A. Derecho Privado de Internet. Civitas Ediciones. Madrid, Año 2000. Pp. 335. También conocida como la firma electrónica. El empleo efectivo de muchas de las posibilidades de comunicación de Internet aparece subordinado a la presencia de mecanismos que permitan comprobar el origen y la integridad de los datos comunicados, así como acreditar la identidad del transmitente y, en ocasiones, manifestar su voluntad de formular la declaración contenida en la información.

[20] Un interesante caso es el de "Chase Manhattan contra Jiménez" por usurpación de una marca en Internet. El presente caso sienta precedente en España y empieza así: Buenas, llamo para ver si podía conseguir un pasaporte falso y montar una empresa en el Caribe para evadir impuestos. En 1998 comenzaron las llamadas de este tipo a las oficinas en España de Chase Manhattan, uno de los primeros bancos del mundo. Los clientes interesados en este tipo de servicios decían que lo habían visto en Internet y en anuncios de los periódicos y pedían presupuesto. Los empleados de Chase perjuraban que la entidad no ofrecía esos productos. Lo que ocurría era una usurpación de marca en Internet. Esta usurpación de marca en Internet que ha provocado la primera sentencia en España con pena de cárcel por este delito. El Juzgado número 23 de Madrid hizo pública la sentencia que condena al español José Francisco Jiménez Criado, residente en Madrid, a 15 meses de cárcel por nada menos que utilizar la marca del gigante bancario estadounidense para captar clientela. Jiménez, que dice pertenecer a una empresa llamada Amerinvest -con sede en Delaware (EEUU)- representa en España la dirección de Internet *chase-manhattan-group.com*, en la que ofrece todo tipo de servicios para evadir impuestos. En <http://www.delitosinformaticos.com-/articulos/freenet.htm>. Fecha de acceso: 12 de febrero del año 2001.

[21] SILVA SÁNCHEZ, José María. *Op. Cit.* Pp. 69.

[22] ESPINOZA CÉSPEDES, José Francisco. Contratación Electrónica, Medidas de Seguridad y Derecho Informático. *Op. Cit.* Pp. 29.

[23] SÁNCHEZ BLANCO, Ángel. *Op. Cit.* Pp. 8.

[24] STERLING, Bruce. La Caza de Hackers. En Ley y Desorden en la Frontera Electrónica. Año 2000. Publicación completa en Internet en <http://www.bufetalmeida.com/intro.htm>. Fecha de acceso: 20 de noviembre del año 2000.

[25] Un dilema de esta nueva forma de relación es si el llamado ciberamor es lo mismo que el amor. El tema tiene defensores y detractores entusiastas, que se dedican a hablar de ello en cada vez más foros y páginas web como la de Cyber-Romance 101 (<http://web2.airmail.net/walraven/romance.htm>), un gran centro repleto de información y artículos sesudos que versan sobre esta maravillosa novedad en el mundo de los sentidos. Más información en <http://ww2.grn.es/merce/ciberamor.html> Fecha de acceso:, 4 de enero del año 2001.

[26] *Ibidem*. Algunos individuos negociantes están aprovechando el ciberamor para montar negocios: grandes bases de datos que funcionan como agencias matrimoniales electrónicas, como <http://www.webpersonals.com> y <http://www.match.com>; <http://www.lovingyou.com>. Las más sofisticadas dan la posibilidad de incluir una foto y archivos de voz o de vídeo a la ficha de quien busca mujer o marido. Los robots de búsqueda permiten afinar más en la caza de la pareja: se puede buscar por localización geográfica, por religión, por apariencia física e incluso por preferencias sexuales. Así, "Men are from cyberspace: The single woman's guide to flirting, dating and finding love on-line". Lisa Skriloff y Jodie Gould. Ed. St. Martin's Griffin. New York, 1997, en donde se puede obtener desde consejos para saber si te encuentras ciberenamorado hasta para saber que hacer si tu pareja tiene un ciberamante (con consejos al respecto).

[27] STERLING, Bruce. *Op. Cit.* Fecha de acceso: 20 de noviembre del año 2000.

[28] LLANEZA GONZÁLEZ, Paloma. Internet y Comunicaciones Digitales. Bosch. Barcelona, Año 2000. Pp. 37.

[29] ESPINOZA CÉSPEDES, José Francisco. *Op. Cit.* Pp. 31.

[30] En este sentido, MORÓN LERMA, Esther. *Op. Cit.* Pp. 93.

[31] Así, los correos electrónicos gratuitos en la red permiten que el usuario pueda cambiar de sexo, raza, edad, país, etc., adoptando una personalidad distinta a la que realmente tiene.

[32] Nunca podremos estar seguros acerca de la persona que se esconde detrás de su sobrenombre o de su *nickname*.

[33] En este sentido, SILVA SÁNCHEZ, José María. *Op. Cit.* Pp. 69, en donde señala que "los fenómenos de la globalización económica y la integración supranacional tienen un doble efecto sobre la delincuencia. ...conductas tradicionalmente contempladas como delictivas, deban de dejar de serlo, pues lo contrario se convertiría en un obstáculo a las propias finalidades perseguidas con la globalización y la integración supranacional.

[34] En este sentido, BUENO ARÚS, F. El delito informático en Actualidad Jurídica Arazandí, N° 11, Abril de 1994, Pp. 1, citado por Matellanes Rodríguez, Nuria. *Op. Cit.* Pp. 129.

[35] DE MIGUEL ASENCIO, Pedro. *Op. Cit.* Pp. 35 y ss.

[36] Esto es que la computadora del usuario se enlaza a un sistema conectado directa o indirectamente a Internet, por medio de un proveedor de acceso.

[37] Por lo general, los proveedores no disponen de conexión directa con Internet, sino que la realizan a través de una de las grandes redes de acceso por medio de un operador telefónico.

[38] DE MIGUEL ASENCIO, Pedro. *Op. Cit.* Pp. 211. "Los sitios web –o conjuntos de páginas web- están integrados por una serie de elementos relacionados entre sí, muchos de los cuales son creaciones originales, de distintas categorías: textos, fotografías, logotipos, gráficos, imágenes, sonidos, videos, animaciones. Cabe señalar que estas páginas web son susceptibles de ser objeto de propiedad intelectual."

[39] *Vid.* LLANEZA GONZÁLEZ, Paloma. *Op. Cit.* Pp. 37.

[40] LLANEZA GONZÁLEZ, Paloma. *Op. Cit.* Pp. 35.

[41] Para el entendimiento de las computadoras entre sí, es necesario del Número IP (Internet Protocol). Este número contiene la identificación de cada máquina conectada a Internet. El IP utiliza un número binario (de ceros y unos) de 32 bits para crear una dirección (la dirección IP). Este sistema comenzó a ser administrado por la *National Science Foundation* (NSF).

[42] FERNÁNDEZ ESTEBAN, M. L. : Nuevas tecnologías, Internet y derechos fundamentales. Madrid, Año 1998. Pp. 25.

[43] En este sentido, MORÓN LERMA, E.: *Op. Cit.* Pp. 91.

[44] LLANEZA GONZÁLEZ, Paloma. *Op. Cit.* Pp. 52. La autora señala que "la idea de sociedad de la información engloba un conjunto de actividades industriales y económicas, comportamientos sociales, actitudes individuales y formas de organización política y administrativa, relacionadas con o producto del uso de las tecnologías de la información y la comunicación." En igual sentido, VILLAR URIBARRI, J.M. Firma Electrónica y Seguridad Jurídica en Internet. Informática y

Derecho en Internet. Mérida, Año 2000. Pp. 117, en donde señala que la “sociedad de la información se ha convertido en una de las grandes prioridades políticas de ámbito mundial.”

[45] SÁNCHEZ BLANCO, Ángel. *Op. Cit.* Pp. 4. El autor compara a Internet con la Gran Enciclopedia, por su intermediación para estructurar los desbordantes contenidos de la sociedad de la información, con efectos sobre los ámbitos en los que se proyecta de modo directo o inducido.

[46] Esto, debido a que las conexiones de Internet se implementaron sin políticas de seguridad.

[47] LLANEZA GONZÁLEZ, Paloma. *Op. Cit.* Pp. 41. “Existe y funciona como resultado del hecho que cientos de miles de operadores de ordenadores o de redes de ordenadores individuales decidieron cada uno de ello de manera independiente utilizar protocolos comunes de transferencia de datos para intercambiar comunicaciones e informaciones entre sí. No existe una entidad de almacenamiento centralizado, ni un punto de control o un solo canal de comunicación para Internet y no sería técnicamente factible para una entidad individual controlar toda la información de Internet.”

[48] Página Web del Boletín de Noticias de Delitos Informáticos. Sección: Artículos. Fecha de acceso: 19 de febrero del año 2000. Recientemente, la Comisión Europea ha recogido esta preocupación en un comunicado en el que destacaba la necesidad de "mejorar la seguridad de las infraestructuras de información y lucha contra la delincuencia informática". El comunicado establece "que existe una clara necesidad de un instrumento de la Unión Europea que garantice que los Estados miembros dispongan de sanciones efectivas para luchar contra la pornografía infantil en Internet".

[49] En este sentido, MORÓN LERMA, Esther. *Op. Cit.* Pp. 92 y ss.

[50] *Cfr.* el trabajo de MUÑOZ MACHADO, Santiago. La Regulación de la Red. Poder y Derecho en Internet. Grupo Santillana de Ediciones S.A. Madrid, Año 2000; en donde el propósito del libro es analizar como se regula y gobierna Internet.

[51] En español, “netiquetas”. LLANEZA GONZÁLEZ, Paloma. *Op. Cit.* Pp. 70. Arlene Rinaldi en un intento por hacer posible la convivencia en la red, redactó la guía *The Net: User Guidelines and Netiquette*. La referida guía establece un buen uso y comportamiento para los usuarios en la red de ordenadores de la Universidad del Atlántico de Florida, siendo obligatorias estas normas para los usuarios de esa red y voluntarias para los demás. Considera que el uso de la red es un privilegio y no un derecho, privilegio que puede ser revocado en cualquier momento de manera temporal a causa de una conducta abusiva del usuario. El Texto de Rinaldi acaba con una referencia a “Los Diez Mandamientos para el Uso Ético de un Ordenador”:

1. No usarán un ordenador para dañar a otros
2. No entrarás en colisión ni interferirás con el trabajo digital ajeno
3. No violarás los archivos ajenos
4. No usarás un ordenador para robar
5. No usarás un ordenador para mentir
6. No usarás o copiarás software por el que no has pagado
7. No usarás los recursos de un ordenador ajeno sin autorización
8. No te apropiarás del trabajo intelectual ajeno
9. Habrás de considerar las consecuencias sociales del programa que “escribes”
10. Usarás un ordenador de manera tal que muestres consideración y respeto.

Sobre las “netiquettes” también en DE MIGUEL ASECIO, P. A. *Op. Cit.* Pp. 72.

[52] Por conductas antisociales en la red, entendemos aquellas conductas que no se ajustan a los parámetros de un debido ingreso y una correcta estadía en la red, perjudicando así al resto de usuarios que hacen uso del Internet.

[53] *I.e.* no se basa en el sistema tradicional de cliente / servidor.

[54] En <http://www.delitosinformaticos.com/articulos/freenet.htm>. Fecha de acceso: 12 de diciembre del año 2000.

[55] Instituto Nacional de Estadística e Informática. Colección Seguridad de la Información. Lima, Marzo del año 2000. Pp. 8.

[56] E.g., destruir un disco duro, cortar una línea de comunicación o deshabilitar un sistema de consulta.

[57] Ejemplos de este tipo de ataques son interceptar una línea para obtener información y copiar ilegalmente archivos o programas que circulan por la red, o bien la lectura de las cabeceras de mensajes para descubrir la identidad de uno o más de los usuarios involucrados en una comunicación que es interceptada ilegalmente.

[58] E.g., el cambio de valores en un archivo de datos, alterar un programa para que funcione de forma diferente y modificar el contenido de mensajes que están siendo transferidos por la red.

[59] Ejemplos de este ataque son insertar mensajes no deseados en una red o añadir registros a un archivo.

[60] E.g., secuencias de autenticación pueden ser capturadas y repetidas, permitiendo a una entidad no autorizada acceder a una serie de recursos privilegiados suplantando a la entidad que posee esos privilegios, como al robar la contraseña de acceso a una cuenta.

[61] Como ingresar dinero repetidas veces en una cuenta dada.

[62] E.g., el mensaje "ingresa diez mil dólares en la cuenta A" podría ser modificado para decir "ingresa diez mil dólares en la cuenta B".

[63] El intruso podría suprimir todos los mensajes dirigidos a una determinada entidad o se podría interrumpir el servicio de una red inundándola con mensajes no deseados. Entre estos ataques se encuentran los de denegación de servicio, consistentes en paralizar temporalmente el servicio de un servidos de correo, Web, FTP, etc.

[64] DE MIGUEL ASENCIO, Pedro. *Op. Cit.* Pp. 69.

[65] Un ejemplo de nuevas formas de delinquir en *USA Today*. Martes, 6 de febrero del año 2001. Líderes terroristas usan la Internet para planificar sus atentados. OSAMA BIN LADEN y otros extremistas musulmanes están usando Internet para planificar actividades terroristas contra los Estados Unidos y sus aliados. Igualmente en <http://www.delitosinformaticos.com/articulos/freenet.htm>. Fecha de acceso: 12 de Febrero del año 2001. Después de varias entrevistas, agentes de policía y expertos en el tema revelaron detalles de cómo los extremistas musulmanes ocultan mapas y fotografías de objetivos terroristas en salas de conversación de deportes, sitios pornográficos y en otros lugares de la Internet.

[66] Muchas empresas que en un principio no querían conectarse a Internet por los posibles problemas de seguridad sin embargo, ahora no quieren quedarse atrás, ya sea porque se ha convertido en una cuestión de pura necesidad o de imagen, y ahora se conectan a marchas forzadas, lo que hace que muchas no tomen las precauciones necesarias y se conviertan automáticamente en jugosos y fáciles objetivos.

[67] En Revista Tecnología. Suplemento Especial. Lima, 4 de Abril del año 2000. Pp. 3.

[68] Según las informaciones procedentes de Atlanta sobre el ataque de "bloqueo de servicio", los *hackers* saturaron un sitio en la red con mensajes inútiles que atoraron sus computadoras lo que produjo la alteración en las operaciones del sitios noticioso durante varias horas.

[69] Un comité clave del Parlamento Europeo aprobó el proyecto final de una norma europea para combatir la piratería en Internet. La votación del comité de asuntos legales del Parlamento Europeo, órgano legislativo de la Unión Europea, había sido esperada ansiosamente por las industrias de la música y el cine, que cada año pierden millones a causa de la piratería digital. "El texto ha sido aprobado. Hemos defendido una posición que está con el interés de los autores", dijo a REUTERS ENRICO BOSELLI, miembro del comité parlamentario. La mencionada norma dará a los propietarios de la música y las obras de cine el derecho a utilizar tecnología avanzada, como codificación especial, para bloquear las copias ilícitas de trabajos registrados y limitar la captura ilegal de archivos de audio y video desde la Internet. La redacción del proyecto final resultó una gran tarea para la comisión del Parlamento Europeo, a causa del choque de intereses de grupos de presión. Mientras los autores y las compañías de música querían la inclusión de reglas muy duras contra las copias ilegales, las asociaciones de consumidores se quejaron de que tales disposiciones podrían limitar las libertades individuales.

<http://www.delitosinformaticos.com-articulos/freenet.htm>. Fecha de acceso: 12 de febrero del año 2001.

[70] En Boletín de Noticias N° 179 del Instituto Peruano de Comercio Electrónico. 7 de agosto del año 2000. Pp. 2.

[71] El primer virus del mundo fue creado en 1982, denominado "*Elk Cloner*" y su autoría corresponde a Rich Skrenta, quien en ese entonces era un muchacho de sólo 14 años de edad. El virus fue escrito para las máquinas Apple II, que al infectarse mostraban el siguiente mensaje en pantalla por cada cincuenta veces que se encendiese la computadora: *Elk Cloner: The program with a personality, It will get on all your disks, It will infiltrate your chips, Yes it's Cloner! It will stick to you like glue, it will modify RAM too, send in the Cloner!* Al tratarse de un período en que Internet era un sistema limitado a los círculos académicos, la propagación de *Elk Cloner* se producía mediante disquetes. El primer virus que llamó la atención mediática a nivel mundial fue "Jerusalén", que luego de propagarse silenciosamente liberaba su carga destructiva cada viernes 13, eliminando archivos en las máquinas infectadas. <http://www.diarioti.com/noticias/2000/may2000/15193090.htm>. Fecha de acceso: 23 de febrero del año 2001. El último virus aparecido hasta el 05 de Marzo del año 2001 es el virus conocido como ROJ_MYBABYPIC.A. El mismo consigue distribuirse automáticamente por Internet a través de archivos ejecutables adjuntos a mensajes de correo electrónico con el asunto "*My Babypic*". Adicionalmente incluye rutinas maliciosas que pueden dañar información de los sistemas afectados. Este virus se propaga por e-mail (MS Outlook) llegando al usuario como un archivo adjunto a un mensaje con asunto "*My Babypic*". Cuando el archivo .EXE es ejecutado, una ventana con la foto de un niño es desplegada. Una vez que la ventana se cierra, el troyano crea varias copias de sí mismo en la carpeta *Windows\System* con los siguientes nombres de archivos: El asunto del mensaje del virus es "*My Babypic*"; el cuerpo del mensaje dice: "*Its my animated baby picture!!!*" y además llega un archivo adjunto bajo el nombre "*MYBABYPIC.EXE*". En sistemas Windows NT, el archivo CMD.EXE citado anteriormente sobrescribe el archivo original del sistema operativo. El troyano cambia las entradas en el registro para lograr ser ejecutado cada vez que se reinicia el sistema. Una vez ejecutado intenta acceder a un sitio web específico (<http://www.youvebeenhack.com>) y activar algunas rutinas maliciosas que van desde sobrescribir archivos con ciertas extensiones hasta borrarlos. En particular el troyano sobrescribe con su propio código los archivos con las siguientes extensiones: C, CPP, CSS, H, HTA, JPG, JPEG, JS, JSE, PAS, PBL, SCT, y WSH, agregando la extensión .EXE. Su rutina de borrado se ejecuta con archivos del tipo .VBS y .VBE. Adicionalmente crea copias de sí mismo usando los nombres de los archivos .MP2, .MP3 y .M3U existentes. Los archivos originales permanecen ocultos y las copias infectadas quedan como archivos ejecutables. El virus abruptamente puede habilitar y deshabilitar las teclas *Numlock*, *ScrollLock* y *CapsLock*.

[72] Hasta el surgimiento del nefasto *ILOVEYOU*, el virus más costoso de la historia había sido Melissa, creado por el estadounidense David Smith, y que ocasionó pérdidas mundiales del orden de los 80 millones de dólares. Tal cifra es modesta comparada con los 15 mil millones de dólares en que se calculan los daños causados por *ILOVEYOU*, cuya presunta autoría se atribuye al filipino Onel Guzmán.

[73] MUÑOZ MACHADO, Santiago. *Op. Cit.* Pp. 152.

[74] Página www.rpp.com.pe. Fecha de acceso: el 02 de enero del 2001.

[75] DEL RÍO, FERNÁNDEZ, L. La autoría en organizaciones complejas en Cuadernos de Derecho Judicial. Fenómenos Delictivos Complejos. Madrid, Año 1999. Pp. 198.

[76] En http://publicaciones.derecho.org/redi/No._06_Enero_de_1999/cuervo. Fecha de acceso: 10 de marzo del año 2001.

[77] Igualmente en http://publicaciones.derecho.org/redi/No._06_Enero_de_1999/cuervo. Fecha de acceso: 10 de marzo del año 2001.

[78] En este sentido, BRAMONT-ARIAS, Luis Alberto. El Delito informático en el Código penal Peruano en Biblioteca de Derecho Contemporáneo. Editorial Desa. Lima, Año 1997, Pp. 5. "De esta manera, el mundo de la informática se convierte, por un lado, en un campo amplio y lleno de posibilidades para el futuro progreso, medio de avance en el desarrollo de la sociedad moderna; pero, por otro lado, se convierte en un factor de "riesgo", en cuanto fuente de nuevas formas de criminalidad, entre las que cabe citar la manipulación de computadoras, la destrucción o alteración de datos, la alteración de programas, etc."

[79] TIEDEMANN, Klaus. Derecho Penal y Nuevas Formas de Criminalidad. Idemsa. Lima, Año 2000. Pp. 85. "Ya que, hasta el momento no se ha demostrado tal internacionalización del fraude informático –aparte del abuso turístico de cajeros automáticos de bancos y del empleo que hagan bandas criminales de las tarjetas (de crédito) robadas en el extranjero- y también la interconexión internacional de los sistemas, que, sin duda, será más fuerte en el futuro y es mencionada."

[80] En este sentido, TIEDEMANN, Klaus. *Op. Cit.* Pp. 85 y ss. En donde explica la relación entre la criminalidad informática y el derecho penal. Así, el autor pronostica que debido al creciente empleo de sistemas procesadores de datos ... en el futuro... la cuota de autores externos (debería) incrementarse; como consecuencia de la constitución de formas delictivas técnicamente cada vez más refinadas, al mismo tiempo sería probable un desplazamiento de círculo de víctimas, así como la aparición de una criminalidad informática transnacional.

[81] En este mismo sentido, FERRÉ O., Juan y ANARTE B., Enrique. *Delincuencia Organizada. Aspectos penales, procesales y criminológicos.* Universidad de Huelva Publicaciones. Huelva, Año 1999. Pp. 17 y ss. En donde señala que es cierto que en los últimos tiempos, la criminalidad organizada se ha convertido en centro de atención de algunos legisladores, con el fin de combatir a este tipo de criminalidad. Así, leyes como las de terrorismo, leyes tributarias y otras tratan de limitar estas acciones criminales tan bien organizadas por grandes grupos de poder económico. Se ha podido observar a lo largo de los últimos años, que la criminalidad organizada no se limita a determinadas zonas geográficas, en donde las actividades pueden tener como base a un país determinado como no determinado, o a diferencias culturales, máxime pareciera ser que aún la globalización favorece -y lo seguirá haciendo- a la criminalidad organizada.

[82] ALONSO PÉREZ, Francisco. *Op. Cit.* Pp. 218, 310 y ss.

[83] FERRÉ OLIVÉ, J.C. y ANARTE BORRALLA, E. *Op. Cit.* Huelva, Año 1999. Pp. 59. El autor señala que para determinar si un delito pertenece a esa categoría, se exigen como mínimo seis características de las enunciadas, de las cuales, al menos serán obligatorias las que figuran con los números 1, 5 y 11.

[84] TIEDEMANN, Klaus. *Op. Cit.* Pp. 85. Como el caso de la TELEKOM, empresa alemana que prefiere no hacer de público conocimiento las falsificaciones de tarjetas telefónicas o la fabricación de simuladores de tarjetas telefónicas o el caso de los bancos, cuando desmienten la posibilidad de que los número de PIN (*personal identification number*) puedan ser forzados por vía de cálculo.

[85] TIEDEMANN, Klaus. *Op. Cit.* Pp. 87.

[86] *Vid.* BRAMONT-ARIAS, Luis. *Op. Cit.* Pp. 18.

[87] Al respecto, ARTEAGA, S. El delito informático: Algunas consideraciones jurídicas penales. *Revista de la Facultad de Ciencias Jurídicas y Políticas* Universidad Central de Venezuela. N° 68. Año 33. Caracas. 1987. Pp. 125 y ss.

[88] MATELLANES RODRÍGUEZ, Nuria. *Op. Cit.* Pp. 130.

[89] Nos parece interesante la clasificación sobre las diversas formas de conductas que pueden producirse en la red y en sistemas informáticos, por lo que hacemos un breve resumen sobre estas conductas de JIJENA LEIVA, Renato. Chile, La protección penal de la intimidad y el delito informático. Editorial Jurídica de Chile. Santiago de Chile, Año 1992. Pp. 95 y ss. Así como de BLOSSIERS MAZZINI y CALDERON GARCÍA. *Los Delitos Informáticos en la Banca.* Editora Rao. Lima, Año 2000. Pp. 39 y ss. Igualmente en http://publicaciones.derecho.org/redi/No.06-Enero_de_1999/cuervo y en http://publicaciones.derecho.org/redi/No.09-Abril_de_1999/viega. Fecha de acceso: 10 de marzo del año 2001. Asimismo un análisis de estas conductas en: HUERTA MIRANDA, Marcelo y LIBANO MANSSUR, Claudio. *Delitos Informáticos.* Editorial Jurídica Cono Sur. Santiago de Chile, Año 1998. Pp. 124 y ss.

[90] Un antecedente muy publicitado es el Caso Blair, conocido por un delito cometido en Maryland en mayo de 1980. Janeth Blair, empleada de las oficinas de seguridad social, ingresaba desde su terminal informático, que se encontraba conectado con su computador central, transacciones falsas para producir la emisión de cheques fraudulentos, consiguiendo por este procedimientos apropiarse de cerca de Ciento Doce Mil Dólares. Este delito fue descubierto de manera casual por el empleado del banco a cuyo nombre eran girados los cheques quien sospechó al verificar la existencia de gran cantidad de cheques con el mismo número de afiliación a la seguridad social pero expedido a diferentes titulares. La Sra. Janeth Blair fue acusada de 43 cargos de falsificación y desfalco y fue condenada a ocho años de prisión con una multa de Quinientos Dólares.

[91] Inspirado en las épicas hazañas contadas por Homero en su obra "La Iliada" que narra toma de Ciudad de Troya. Ulises mandó construir un enorme caballo de madera vacío que obsequió a los troyanos en señal de paz, sin embargo, en su interior ocultaba gran cantidad de soldados y pertrechos militares de la época, los cuales permanecieron ocultos hasta que se diera la orden a fin de sitiar la ciudad. Los habitantes de Troya al creer que habían ganado la guerra, introdujeron al caballo en la ciudad y celebraron el triunfo con una gran fiesta, pero durante la noche, cuando todos dormían confiados bajos los efectos del

alcohol, los soldados de Ulises salieron del caballo y abrieron las puertas de la ciudad ingresando los soldados enemigos tomando la ciudad sin que los troyanos opusieran mayor resistencia. Por esta razón, la denominación “Caballo de Troya” se aplica a algo que en apariencia es inofensivo para tranquilidad de la víctima, pero cuando desencadena su daño potencial causa verdaderos estragos. En [http://publicaciones.derecho.org/redi/No. 09 - Abril de 1999/viega](http://publicaciones.derecho.org/redi/No.09-Abril-de-1999/viega) Fecha de acceso: 11 de marzo del año 2001.

[92] Un procedimiento usualmente utilizado en la banca es, *E.g.*, introducir una modificación al programa del tratamiento de cuentas corrientes para que siempre que se consulte un saldo se multiplique por diez, por cien, por mil, por cien mil, etc. con lo que es posible autorizar pagos, transferencias superiores a lo real.

[93] Un claro ejemplo de este método es un caso real sucedido en una entidad de crédito al cual no se le dio publicidad y del que se desconoce incluso el nombre del autor. Este caso ocurrió a fines de 1984 y el procedimiento utilizado por el autor, aparentemente un ex - empleado del centro de cómputo de la entidad, fue el introducir una rutina en el programa de tratamiento de cuentas corrientes para que un determinado día, aproximadamente seis meses después de haber dejado su trabajo, y a una hora nocturna predeterminada se autorizase el pago a un talón de una cuenta corriente sin consultar el saldo. Posteriormente la misma rutina borraba parte del programa modificado con lo cual se eliminaba el rastro de la comisión del delito. Otro caso similar sucedió en 1985 en una importante entidad bancaria cuando en una oportunidad tres personas, supuestamente antiguos empleados de la institución, manipularon el sistema informático abriendo dos cuentas en diferentes oficinas de la ciudad con nombres distintos y falsos, lo que les permitió disponer de talonarios de cheques al mismo tiempo que las cuentas ingresaran al sistema del banco. Pues bien, después de unos días de funcionamiento normal y sin que se haya explicación alguna, en las cuentas se hicieron asientos falsos por un total de 24 millones de dólares. Los malos elementos fueron detenidos al ser descubiertos después de haber cobrado cinco cheques y en posesión de documentos falsos que identificaban a las personas en cuyo nombre estaban abiertas las cuentas.

[94] Un caso real se dio en los Estados Unidos donde un programador tenía bajo su responsabilidad el sistema mecanizado de personal en el cual introdujo pequeñas modificaciones en los cálculos del plan de inversiones corporativas. La empresa había acordado con sus trabajadores que les retendría una pequeña cantidad de sus salarios para invertirlos en valor. Lo que realizó el programador fue retirar pequeñas cantidades de lo descontado a cada empleado para transferirlo a su propia cuenta.

[95] Un conocido caso con el método del *superzapping* ocurrió *New Jersey* en donde el autor comenzó a desviar fondos desde las cuentas de diferentes clientes hacia la de unos amigos sin que quedara en el sistema ninguna evidencia de las modificaciones efectuadas en los saldos de cuenta corriente. El delito se descubrió por los reclamos efectuados por uno de los afectados, lo cual motivó una investigación que culminó con la detención del sujeto.

[96] Tal es el caso de unos ingenieros en una fábrica de automóviles en Detroit que descubrieron una puerta falsa en una red de servicios público de *time-sharing* de Florida. Después de una serie de intentos consiguieron ingresar con una llave de ingreso de alto nivel, según parece la del propio presidente ejecutivo de la compañía y utilizándola pudieron apoderarse de diferentes programas clasificados de carácter reservado y archivados en el computador bajo la denominación de secreto comercial, al mismo tiempo que utilizaban la red sin cargo económico alguno.

[97] Un conocido caso de bomba lógica se presentó en Septiembre de 1981 y tuvo como protagonista un programador de computadoras de 26 años de edad que trabajaba para el departamento de defensa en Washington D.C. en los Estados Unidos de Norteamérica. Resulta que el programador se sintió frustrado y discriminado al no recibir una promoción que supuestamente le correspondía, por lo que decidió vengarse. El trabajo de este empleado consistía en el mantenimiento de las nóminas del sistema de personal lo que le permitía tener acceso a todos los programas y a la información contenida en la base de datos de dicho sistema. Decidido a vengarse escribió unas rutinas para incluir en los programas que a cierta señal se borren y destruyan gran parte de la información que él procesaba en los sistemas. Posteriormente comenzó a buscar otro trabajo para lo cual solicitó vacaciones en su empleo siendo así que consiguió un nuevo trabajo. Unos días después que recibió la confirmación de su nuevo empleo, y en ese mismo momento aprovechando la hora del almuerzo, introdujo la rutina que tenía programada, incluyendo un control que se activaría seis meses desde la fecha de su salida de su anterior empleo. En efecto, seis meses después de haber abandonado a su anterior trabajo cuando se estaban procesando las nóminas de personal la rutina introducida por él funcionó como había previsto su autor, borrando la mayor parte de información de los registros de personas. Dado que el programa había estado funcionando largo tiempo y nadie dudaba de su funcionamiento se volvieron a probar con las copias de seguridad las que también resultaron dañadas. El descubrir el motivo de los daños al sistema y recomponer la información requirió gran esfuerzo de personal y de tiempo, lo que puede dar una idea del costo que se supuso, pero no fue posible probar

la autoría del hecho, aunque las sospechas recayeron sobre su verdadero autor, el que nunca fue acusado formalmente, ni juzgado ni castigado.

[98] Una importante obra sobre contratos de Licencia de uso de Software en la empresa y legislación comparada en NÚÑEZ PONCE, Julio. El contrato de licencia de uso de software en la empresa: Regulación Jurídica Adecuada. Lima. Año, 1997.

[99] El caso más célebre de scavenging ocurrió en Los Ángeles por un estudiante de ingeniería eléctrica. El estudiante simultáneamente trabajaba como vendedor de equipos de comunicaciones lo cual le permitió adquirir un conocimiento bastante profundo de cómo operaban los sistemas mecanizados de la empresa. Al haber recogido cada mañana los papeles que depositaban en el exterior del centro de procesamiento de datos de la compañía. El estudiante simulando ser un publicista convenció a los directivos de la empresa para lanzar un boletín que reforzaría considerablemente la imagen de la compañía. Esto le permitió recopilar información, añadida a al compra de una camioneta en una subasta de la propia compañía. El estudiante pidió telefónicamente mercadería para una empresa que había seleccionado previamente. Para ser despachada por la noche por la cantidad de 30mil dólares, lo que hizo fue recoger la mercadería y distribuirla a diferentes compradores. El estudiante fue descubierto al ser denunciado por su ayudante a quien se negó a aumentar el dinero que le pagaba por sus servicios especiales. El estudiante fue acusado de varios delitos y el 5 de julio de 1972 fue condenado por el Juez M. Deal a dos meses en una correccional, 500 dólares de multa y tres años de libertad vigilada.

[100] Otro caso célebre es el que hicieron los estudiantes de una universidad norteamericana al mandar una carta en papel oficial a todos los usuarios de computadoras de la universidad advirtiéndoles que el número de conexión al sistema había sido cambiado, solicitándoles su número anterior. Posteriormente y debido a que lo primero que solicita el sistema al conectarse era la clave de identificación, los estudiantes recogieron la clave e indicaron que hasta nueva orden volvieran a usar su número antiguo, obteniendo así el número clave de todos los usuarios del sistema, descubriendo todos los secretos de los estudiantes de la universidad. Una vez descubierto el procedimiento todas las claves fueron cambiadas.

[101] Ad Cops, un consorcio que lucha contra las estafas en el comercio electrónico en representación de sus miembros, recientemente inauguró lo que, sostienen, es el único museo sobre fraude. Actualmente el museo contiene 13 muestras, pero se proponen agregar otras a medida que se descubran nuevas formas delictivas. Entre las muestras se encuentra un mensaje de correo electrónico, supuestamente proveniente de América Online, diseñado para recolectar contraseñas de los usuarios y luego sus números de tarjeta de crédito. Existe un programa que genera números de tarjeta de crédito apócrifos, de acuerdo con las pautas de cada firma. Y hasta se incluye una supuesta página de Microsoft para "reclamar premios" que captura contraseñas. Uno de los apartados más llamativos del museo trata sobre el fraude mediante tarjetas de crédito. Las instrucciones son tan detalladas que hasta los no entendidos en la materia quedarían impresionados. Entre otras cosas, se dan explicaciones sobre cómo utilizar números robados para encargar productos y hacerlos enviar a direcciones falsas aprovechando puertas traseras, jardines e intermediarios desprevenidos. Los datos sorprendentes abundan. ¿Sabía usted que por unos 1.000 dólares puede comprar todo el equipo necesario para fabricar sus propias tarjetas de crédito? El propósito de este museo es mantener a los miembros de Ad Cops (tales como comercios y bancos que operan en la red) al día en materia de fraudes, explica Daniel Clements, presidente de Ad Cops. El enseñarles los mensajes de correo apócrifos, las páginas de Internet engañosas y los programas utilizados por los criminales ayuda a los comerciantes a protegerse. Sin embargo, el paseo por el museo virtual del fraude plantea la siguiente duda: ¿que impide a un aspirante a estafador utilizar la información del Museo del Fraude para obtener ideas? Clements dice que los 99 dólares que cuesta la suscripción son suficientes para alejarlos. Además, agrega: "Este material está disponible en Internet, de todas formas", y los interesados saben cómo y dónde encontrarlo. Las secciones de acceso libre del sitio de Ad Cops ofrece datos menos concretos pero igualmente escalofrantes, tales como una lista de sujetos buscados junto con la descripción de sus delitos, y un artículo que describe las distintas clases de fraude y su difusión. Hasta existe una sección de "consejos" anónimos. El material expuesto en el Museo del Fraude proviene de los propios estafadores. Clements, ex gerente de una empresa de anuncios en Internet, conoció a un grupo que había creado un software capaz de registrar visitas inexistentes a los sitios anunciados. "Cuando atrapamos a estos tipos les pedimos que nos mostraran cómo lo hacían", dice. Y así nació el Museo del Fraude. En <http://cnnenespanol.com/2001/tec/02/27/museo/index.html> Fecha de acceso: 05 de marzo del año 2001.

[102] Este fenómeno, ligado al crimen organizado internacional, es un lastre que frena el desarrollo de Internet en Europa y que provocó en el 2000 pérdidas anuales de 600 millones de euros. El 50% más que en 1999. Europa, por su parte -mediante la Comisión Europea- recomienda a las empresas del sector a poner en práctica, antes de julio de 2002, un sistema que garantice un nivel alto de seguridad del dinero electrónico. El Ejecutivo comunitario señala dos tipos de fraude: el originado

por el robo o pérdida de tarjetas bancarias y el que tiene relación con las compras por Internet o por teléfono. Este último es el que más ha aumentado en los últimos años. El problema es que hay quince respuestas distintas para un problema que no conoce fronteras.

- [103] ARLUCEA, Esteban. Lecciones de teoría jurídica del delito. Editorial Comares. Granada, Año 1999. Pp. 2.
- [104] MUÑOZ CONDE, Francisco y GARCÍA ARAN, Mercedes. Derecho Penal. Parte General. Tercera Edición. Valencia, Año 1998. Pp. 224.
- [105] BRAMONT-ARIAS, Luis Alberto y BRAMONT-ARIAS TORRES, Luis Alberto. Código penal Anotado. Editorial San Marcos. Lima, Año 1988. Pp. 29.
- [106] MUÑOZ CONDE, Francisco y GARCÍA ARAN, Mercedes. *Op. Cit.* Pp. 220. Para los referidos autores, consideran este concepto como puramente formal, que nada dice sobre los elementos que debe tener esa conducta para ser castigada por la ley con una pena.
- [107] Se trata del sistema tripartito del delito, dominante en la doctrina alemana; sin embargo, debemos señalar que la doctrina ha realizado propuestas conducentes a una bipartición, acentuando los conceptos básicos de antijuricidad y culpabilidad, y relegando a un segundo plano a la tipificación; sobre esta discusión puede verse en SILVA SANCHEZ, Jesús María. Aproximación al Derecho Penal. Bosch. Barcelona, Año 1992. Pp. 374 y ss.
- [108] Las causas de justificación se encuentran en el artículo 20, incisos 3,4 y 8.
- [109] MUÑOZ CONDE, Francisco y GARCÍA ARÁN, Mercedes. *Op. Cit.* Pp. 223.
- [110] Un hecho típico no es antijurídico si existe una causa de justificación que lo permita. Luego, una vez comprobado que el hecho es típico y antijurídico, debemos analizar si el autor es culpable o no.
- [111] ARLUCEA, Esteban. *Op. Cit.* Pp. 7.
- [112] “Según los especialistas, siempre se da una especie de ecuación en la que se combinan errores de programación o negligencias por parte del fabricante del software con las habilidades de los *hackers*”. En Tecnología. Suplemento especial. Lima, 4 de abril del año 2000. Pp. 2
- [113] ROMEO CASABONA, C. M.: Poder informático y Seguridad Jurídica, Fundesco, Madrid, Año 1997. Pp. 41, citado por Matellanes Rodríguez, Nuria. *Op. Cit.* Pp. 130.
- [114] En este sentido, BRAMONT-ARIAS, Luis Alberto. *Op. Cit.* Pp. 58.
- [115] Para GÓMEZ PERALS. La delincuencia informática es un conjunto de comportamiento dignos de reproche penal que tienen por instrumento o por objeto a los sistemas o elementos de técnica informática, o que están en relación significativa con ésta, pudiendo presentar múltiples formas de lesión de variados bienes jurídicos. Ver en http://publicaciones.derecho.org/redi/No._06_Enero_de_1999/cuervo.
- [116] MATELLANES RODRÍGUEZ, Nuria. *Op. Cit.* Pp. 131, en donde señala que “lo realmente específico de la delincuencia informática lo constituyen las funciones de procesamiento, transmisión y ejecución de programas propios del ordenador, con independencia de que la manipulación de estas funciones sea el medio o el objeto de la agresión ilegítima. Con esto, se elimina del ámbito de la delincuencia informática todas aquellas conductas que no afecten a alguna de las funciones citadas.”
- [117] En este mismo sentido, MATELLANES RODRÍGUEZ, Nuria. *Op. Cit.* Pp. 129, en donde señala que “la utilización de un sistema de detonación de explosivos que funciona por control remoto para causar la muerte de alguien; o la entrega de una suma de dinero para adquirir un equipo de informática personal por correo a una empresa que resulta ser inexistente, o el mismo hecho de las agresiones al soporte físico de los equipos de procesamiento, debe quedar fuera de la noción de delitos informáticos.”
- [118] Sin embargo, distingue dentro de la manipulación mediante la informática dos vertientes diferentes: a) Acceso y manipulación de datos y b) Manipulación de los programas. En http://publicaciones.derecho.org/redi/No._06_-_Enero_de_1999/cuervo Fecha de acceso: 10 de marzo del año 2001.

- [119] HUERTA MIRANDA, Marcelo y LIBANO MANSSUR, Claudio. *Op. Cit.* Pp. 114.
- [120] Citado por BLOSSIERS, Juan José y CALDERÓN GARCÍA, Sylvia. *Op. Cit.* Pp. 32.
- [121] Citado por BLOSSIERS, Juan José y CALDERÓN GARCÍA, Sylvia. *Op. Cit.* Pp. 33.
- [122] En [http://publicaciones.derecho.org/redi/No. 09 - Abril de 1999/viega](http://publicaciones.derecho.org/redi/No.09-Abril-de-1999/viega) Fecha de acceso: 11 de marzo del año 2001.
- [123] A modo de ejemplo, la empresa Telefónica Móviles desmiente la existencia de virus o fraude en las tarjetas SIM que puedan afectar a sus terminales, informó la compañía, saliendo al paso así de diversas informaciones difundidas por correo electrónico. La compañía considera que estas informaciones "carecen de cualquier fundamento técnico" y, por lo tanto, "no existe ningún riesgo" en la utilización de los servicios, ya sean de *MoviStar* o de *Moviline*, "ni para el usuario ni tampoco para los terminales". Telefónica Móviles insiste en que no ha recibido "ninguna reclamación" de sus clientes por estas supuestas incidencias y que ningún fabricante de terminales ha confirmado "los rumores difundidos" a través de Internet. <http://www.delitosinformaticos.com/articulos/freenet.htm>. Fecha de acceso: 15 de febrero del año 2000.
- [124] En mi actividad profesional, fui testigo de un caso similar en donde un Banco conocido se rehusaba a denunciar el acceso indebido a sus sistemas por un ex empleado, debido a la pérdida de imagen que tendría dicho Banco. Por tanto, creemos que la cifra negra es consecuencia de estas conductas.
- [125] También denominada por gran parte de la doctrina como *cifra oculta*, en cuanto se trata de conductas que no son comprendidas en las investigaciones que realizan los policías o las diversas instancias de control.
- [126] En [http://publicaciones.derecho.org/redi/No. 09 - Abril de 1999/viega](http://publicaciones.derecho.org/redi/No.09-Abril-de-1999/viega) Fecha de acceso: 11 de marzo del año 2001. En donde señala que es difícil descubrir este tipo de delitos en razón del poder económico de quienes lo cometen. Se habla de pérdidas anuales por delitos informáticos y otros tecno-crímenes, que van desde los US\$ 100 millones de dólares hasta los US\$ 5,000 millones de acuerdo a un estudio realizado en 1990.
- [127] Al respecto, SILVA SÁNCHEZ, Jesús María. "Aproximación al Derecho Penal contemporáneo". *Op. Cit.* Pp. 268.
- [128] Este autor, representa la máxima expresión del funcionalismo y se orienta a la normativización de la sociedad.
- [129] BUSTOS RAMIREZ, J. Manuel de Derecho Penal. Tercera Edición. Barcelona. Año 1989. Pp. 45.
- [130] Al respecto, MIR PUIG, Santiago. Derecho Penal Parte General. Barcelona, Año 1996. Pp. 90 y ss.
- [131] BUSTOS RAMIREZ, Juan. Manual de Derecho Penal. *Op. Cit.* Pp. 50- 51.
- [132] ROXIN, Claus. Derecho Penal. Parte General. Tomo I. Pp. 55 y 56.
- [133] BUSTOS RAMIREZ, J. Manual de Derecho Penal. *Op. Cit.* Pp. 54 y 55.
- [134] MUÑOZ CONDE, Francisco y GARCÍA ARÁN, Mercedes. *Op. Cit.* Pp. 64.
- [135] MIR PUIG, Santiago. *Op. Cit.* Pp. 91.
- [136] MUÑOZ CONDE, Francisco y GARCÍA ARÁN, Mercedes. *Op. Cit.* Pp. 65.
- [137] MUÑOZ CONDE, Francisco y GARCÍA ARÁN, Mercedes. *Op. Cit.* Pp. 88.
- [138] *E.g.*, sabemos que intereses morales no podrían estar considerados como intereses merecedores de una protección del derecho penal.
- [139] En este sentido, MIR PUIG, Santiago. *Op. Cit.* Pp. 91 y ss.
- [140] Al respecto, debemos indicar que para que determinados bienes jurídicos deban ser objeto de protección penal, es necesario que estos bienes tengan una importancia fundamental, es decir; que los bienes jurídicos sean condiciones de la vida en un determinado sistema social, máxime de un Estado democrático.
- [141] En sentido contrario, JAKOBS, el mismo que refiere respecto a esta teoría que el derecho penal interviene cuando ya

se afectó el bien jurídico. Sin embargo, creemos, que para eso el legislador ha optado por los delitos de peligro abstracto, aunque no estemos totalmente de acuerdo con que la puesta en peligro de determinados bienes, sean objeto de tipificación en nuestro Código penal.

[142] Cfr. en este sentido, SILVA SÁNCHEZ, Jesús María. *Op. Cit.* Pp. 267.

[143] JAKOBS, Gunther. *Sociedad, Norma y Persona en una Teoría de un Derecho Penal Funcional*. Cuadernos Civitas. Madrid, Año 1996. Págs. 11.

[144] *Ibidem*. Creemos, que el autor de dicha teoría deberá referirse a que entiende por el término norma. Si es que se trata de una norma legal, es decir, tipificada o por el contrario se trata de una norma social, como gran parte de sus seguidores opinan; mientras que sus detractores afirman que hace referencia a las normas jurídicas. Esta discusión pareciera responder a un tema de traducción, ya que el término “Norm” usado por Jakobs en sus trabajos no hace referencia expresa a la norma jurídica, por lo que puede ser entendido como norma social, norma ética, religiosa, ya que el autor menciona, eventualmente, el término “Gesetz” (ley) para hacer referencia a la norma jurídica.

[145] JAKOBS, Günther. *Op. Cit.* Pp. 15.

[146] Cfr. LESCH, H. *La Función de la Pena*. Trad. de Sánchez - Vera Gómez- Trelles. Ed. Dykinson. Madrid. 1999. Pp. 47.

[147] Cfr. JAKOBS, Günther. *Op. Cit.* Pp. 9.

[148] Cfr. en este sentido , JAKOBS, Günther. *Op. Cit.* Pp. 10.

[149] JAKOBS, Günther. *Imputación jurídico penal. Desarrollo del sistema a partir de las condiciones de vigencia de la norma*. Hammurabi. Buenos Aires, Año 1998. Pp. 33 y ss.

[150] Cfr. al respecto, GARCÍA CAVERO, Percy. *La responsabilidad penal del administrador de hecho de la empresa: Criterios de imputación*. Bosch. Barcelona, Año 1999. Pp. 51-52.

[151] BRAMONT-ARIAS, Luis Alberto y GARCÍA CANTIZANO, María del Carmen. *Manual de Derecho Penal*. Editorial San Marcos. Lima, Año 1998. Pp. 28.

[152] *Ibidem*.

[153] BRAMONT-ARIAS, Luis Alberto y BRAMONT-ARIAS TORRES, Luis Alberto. *Op. Cit.* Pp. 29 y ss. “Es decir, si se considera que el bien jurídico como síntesis normativa concreta de una relación social determinada, en forma alguna se agota en la vinculación social, sino que además es necesario determinada perturbación de la relación social misma, ósea, determinada afección del bien jurídico mismo traducida en una situación de peligro o en una lesión, con lo que se pone de manifiesto que, junto al desvalor del acto, es necesario apreciar el desvalor del resultado.”

[154] En este sentido Cfr., CARBONELL MATEU, Juan Carlos. *Derecho Penal. Concepto y Principios Constitucionales*. Tirant lo blanch. Valencia, Año 1996.

[155] BRAMONT-ARIAS, Luis Alberto. *El Delito informático en el Código penal Peruano*. *Op. Cit.* Pp. 51.

[156] En <http://publicaciones.derecho.org/redi/No.06-Enerode1999/cuervo> Fecha de acceso: 10 de marzo del año 2001.

[157] Quien debiera ser considerado con todo merecimiento como uno de los pensadores más relevantes en la construcción jurídica de la intimidad es LOCKE, apreciado por sus reflexiones en torno a lo que él denominó “libertad negativa”. Considera el citado autor que es preciso reconocer al individuo una esfera mínima de libertad personal, que no pueda ser invadida por nadie –“libertad negativa”-, y de donde se deduce la delimitación de una frontera entre el ámbito de la vida privada y el de la actividad pública. En este sentido, HERRÁN ORTIZ, Ana Isabel. *La Violación de la Intimidad en la Protección de Datos Personales*. Editorial Dykinson. Madrid, Año 1998. Pp. 8.

[158] En este sentido, HERRÁN ORTIZ, Ana Isabel. *Op. Cit.* Pp. 4.

[159] VILLAR URIBARRI, J. M. *Op. Cit.* Pp. 64.

- [160] DAVARA RODRÍGUEZ, M. A. citado por VILLAR URIBARRI, J. M. *Op. Cit.* Pp. 65 y 66.
- [161] MUÑOZ CONDE, Francisco. Citado por VIVES ANTÓN, T. y otros en Derecho Penal Parte Especial. Tirant lo Blanch. Valencia, Año 1999. Pp. 285.
- [162] En igual sentido, BRAMONT-ARIAS, Luis Alberto y GARCÍA CANTIZANO, María del Carmen. *Op. Cit.* Pp. 197.
- [163] En http://publicaciones.derecho.org/redi/No._06_-_Enero_de_1999/cuervo Fecha de acceso: 10 de marzo del año 2001.
- [164] El artículo 200 del Código penal español establece lo siguiente: “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.”
- [165] GARCÍA CAVERO, Percy. *Op. Cit.* Pp. 58-59.
- [166] En http://publicaciones.derecho.org/redi/No._06_-_Enero_de_1999/cuervo Fecha de acceso: 10 de marzo del año 2001.
- [167] Esta es la definición que señala SANCHEZ DE DIEGO, M. Transparencia de las bases de datos como mecanismo de protección de la intimidad de las personas. *Idn*° 4. Año 1994. Pp. 146.
- [168] Al respecto, MUÑOZ MACHADO, Santiago. *Op. Cit.* Pp. 152.
- [169] *Ibidem*. “Pasear por el ciberespacio, navegar o hacer *websurfing* no es lo mismo que pasear por la calle de una gran ciudad, curioseando las librerías, los anuncios de los cines o entrando en alguna exposición. En Internet siempre es posible, sin un coste importante, averiguar y almacenar todos los datos de quien sale a pasear: su domicilio, la duración de la salida, los sitios que ha visitado, las ofertas que le han interesado, sus gustos personales... De modo que, tras cada salida, se pierden más datos íntimos que aprovechan luego los comerciantes establecidos en la red (por lo menos ellos, si no también otros con intereses menos razonables que la venta de bienes y servicios) para tratar de acorralar al internauta con mensajes o con ofertas, incomodando, en todo caso, sus próximas salidas al espacio virtual.
- [170] En este sentido, HERRÁN ORTIZ, Ana Isabel. *Op. Cit.* Pp. 9.
- [171] JIJENA LEIVA, Renato. *Op. Cit.* Pp. 45.
- [172] VILLAR URIBARRI, J. M. *Op. Cit.* Pp. 62 y 63.
- [173] DE MIGUEL ASENCIO, Pedro. *Op. Cit.* Pp. 488.
- [174] En igual sentido, MUÑOZ MACHADO, Santiago. En la Regulación de la Red. *Op. Cit.* Pp. 153.
- [175] Creemos que la protección de datos personales debe ser prioritario en un portal de Internet, sobre todo cuando se trata de portales donde se recogen datos relevantes sobre los usuarios.
- [176] Art. 4º.1 de la LOPD.
- [177] Si bien la LOPD no hace una mención expresa a este principio, éste se deriva del derecho a la información en la recogida de datos (Art. 5º) y del derecho a conocer la existencia de ficheros automatizados de datos de carácter personal (Art. 13º).
- [178] Art. 9º.1 de la LOPD.
- [179] Art. 6º.1 de la LOPD.
- [180] Se puede encontrar la Ley Federal Alemana sobre la Protección de Datos de Carácter Personal (Bundesdatenschutzgesetz, BDSG) y otras leyes alemanas en <http://iecl.iuscomp.org/gla/statutes/BDSG.htm> o en <http://www.kronegger.at/recht/b5.htm> y en http://europa.eu.int/comm/internal_market/en/media/dataprot/law/impl.htm. Fecha de acceso: 2 de mayo del año 2001.

- [181] El artículo 2, inciso 5 establece lo siguiente: A solicitar sin expresión de causa, la información que requiera y a recibirla de cualquier entidad pública, en el plazo legal, con el costo que supongo el pedido. Se exceptúan las informaciones que afecten la intimidad personal y las que expresamente se excluyan por ley o por razones de seguridad nacional."
- [182] BRAMONT-ARIAS, Luis Alberto y GARCÍA-CANTIZANO, María del Carmen. *Op. Cit.* Pp. 197.
- [183] CARBONELL, J.C. y GONZÁLEZ, J.L. en VIVES ANTÓN, T. y otros. *Op. Cit.* Pp. 290.
- [184] BRAMONT-ARIAS, Luis Alberto y GARCÍA-CANTIZANO, María del Carmen. *Op. Cit.* Pp. 285.
- [185] *Ibidem.*
- [186] TIEDEMANN, Klaus. *Op. Cit.* Pp. 88-89.
- [187] HERRÁN ORTIZ, Ana Isabel. *Op. Cit.* Pp. 38.
- [188] VIVES ANTÓN, T. y otros. *Op. Cit.* Pp. 310. En donde se elabora un amplio resumen sobre el honor, en su concepto interno, externo, así como un análisis histórico.
- [189] DE MIGUEL ASENCIO, Pedro. *Op. Cit.* Pp. 468.
- [190] En este sentido, HERRÁN ORTIZ, Ana Isabel. *Op. Cit.* Pp. 40.
- [191] DE MIGUEL ASENCIO, Pedro. *Op. Cit.* Pp. 491 y ss.
- [192] DE MIGUEL ASENCIO, Pedro. *Op. Cit.* Pp. 491-492.
- [193] En EE.UU., frente a la tendencia jurisprudencial apuntada en el asunto *Stratton Oakmont v. Prodigy* se optó por una amplia exclusión legal de la responsabilidad de los proveedores de servicios, incorporada en el artículo 230 (c) (1) de la *Telecommunications Act* de 1996. Conforme a esta normativa, ningún proveedor o usuario de un servicio informático interactivo será considerado editor (Publisher) o autor de información proporcionada por un tercero, excluyendo así que los proveedores de servicio se hallen sometidos a la responsabilidad por difamación (en los términos en los que impone a los *publishers*) que pueda derivarse de contenidos no creados por ellos, si bien cabe exigirle responsabilidad cuando tuviera conocimiento del carácter ilícito del contenido”
- [194] En igual sentido, BRAMONT-ARIAS, Luis Alberto y GARCÍA CANTIZANO, María del Carmen. *Op. Cit.* Pp. 136.
- [195] FRÍGOLA VALLINA, Joaquín y ESCUDERO MORATALLA, José Fco. Honor, secreto profesional y cláusulas de conciencia en los medios de comunicación. Límites y aspectos jurídicos civiles y penales. Ediciones Revista General de Derecho. Valencia, Año 1998. Pp. 53.
- [196] Así lo establece la STC 139/1996, del 26 de setiembre (Sala 1) Ponente Sr. Manuel Jiménez de Parga y Cabrera. En donde se señala que “... Aunque el honor es un valor referible a personas individualmente consideradas, el derecho a la propia estimación o al buen nombre o reputación en que consiste, no es patrimonio exclusivo de las mismas... En consecuencia, dada la propia sistemática constitucional, el significado del derecho al honor ni puede ni debe excluir de su ámbito de protección a las personas jurídicas.Resulta evidente pues, que, a través de los fines para los que cada persona jurídica privada ha sido creada, puede establecerse un ámbito de protección de su propia identidad cuando desarrolla sus fines para proteger su identidad cuando desarrolla sus fines para proteger las condiciones de ejercicio de su identidad, bajo las que recaería el derecho al honor. En tanto que ello es así, la persona jurídica también puede ver lesionado su derecho al honor a través de la divulgación de hecho concernientes a su entidad, cuando la difame o la haga desmerecer en la consideración ajena. Igualmente en la STS del 9 de octubre del año 1997 (Sala1) en donde se señala que “... el honor, fama o prestigio de una persona jurídica es indudable e indiscutible; no se puede ofender a una persona física, ni tampoco a una jurídica; una persona jurídica que es atacada en su buena fama, su prestigio o su honor, tiene indudablemente acción para su protección....” En posición contraria la STC 107/1988 en donde se expresa que “el honor es un valor referible a personas individualmente consideradas, lo cual hace inadecuado hablar de las instituciones públicas o de clases determinadas del Estado....”. En el mismo sentido la STS, de 6de junio de 1992. En FRÍGOLA VALLINA, Joaquín y ESCUDERO MORATALLA, José Fco. *Op. Cit.* Pp. 53-55.
- [197] FRÍGOLA VALLINA, Joaquín y ESCUDERO MORATALLA, José Fco. *Op. Cit.* Pp. 54.

[198] El artículo 240 del Código penal establece lo siguiente: “Será reprimido con pena privativa de libertad no mayor de dos años o con ciento ochenta a trescientos sesenta y cinco días-multa, el que en beneficio propio o de terceros:

- 1.- Se aprovecha indebidamente de las ventajas de una reputación industrial o comercial adquirida por el esfuerzo de otro.
- 2.- Realiza actividades, revela o divulga informaciones que perjudiquen la reputación económica de una empresa, o que produzca descrédito injustificado de los productos o servicios ajenos.

En los delitos previstos en este artículo sólo se procederá por acción privada.

[199] El artículo 314 del Código de procedimientos penales establece que: Los jueces instructores sustanciarán los procesos por delitos de calumnia, difamación e injurias, perpetrados por medio de impresos o publicaciones, o prensa, o con escritos, vendidos o exhibidos, o por carteles expuestos al público, o el cinema, la radio, la televisión y otro medio análogo de publicidad, realizando en el término de ocho días, una sumaria investigación y fallarán dentro del término de cinco días, bajo responsabilidad.

[200] Diccionario de la Lengua Española. Real Academia Española. Vigésima Primera Edición. Editorial Espasa Calpe S.A. Madrid, Año 1997.

[201] *Ibidem*.

[202] HERRÁN ORTIZ, Ana Isabel. *Op. Cit.* Pp. 72. Debemos recordar que debido a la necesidad de asegurar a la persona una esfera de autonomía y la no intromisión por parte de los poderes públicos en la esfera íntima de cada individuo, surgen la “Primera Generación de Derechos.” Posteriormente, surge una “Segunda Generación de Derechos” para garantizar los llamados derechos económicos, sociales y culturales. También denominados como “derechos de participación”. En los derechos de “Tercera Generación” también se incluyen el derecho a la paz, los derechos de los consumidores, el derecho a un medio ambiente sano y el derecho a una calidad de vida, derechos éstos dirigidos a potenciar la esfera de libertades del individuo en la era tecnológica. En <http://comunidad.derecho.org/congreso/ponencia29.html>. Fecha de acceso: 07 de marzo del año 2001.

[203] VILLAR URIBARRI, J. M. *Op. Cit.* Pp. 63. El término de “autodeterminación informativa” es utilizado por primera vez en 1983 por el Tribunal Constitucional Alemán de Karlsruhe el 15 de diciembre de 1983 basándose en el derecho a la personalidad de la Ley Fundamental de Bonn. Igualmente, “...la libertad informática también puede ser entendida de acuerdo con lo que el Tribunal Constitucional Alemán ha calificado del “derecho a la autodeterminación informativa”, en su célebre sentencia del 15 de diciembre de 1983, que declaró inconstitucionales algunas disposiciones de la Ley del Censo de la República Federal Alemana. En tal sentido, el mencionado Tribunal señaló que dicho derecho supone la facultad del individuo de disponer y revelar datos referentes a su vida privada.” En <http://comunidad.derecho.org/congreso/ponencia29.html>. Fecha de acceso: 07 de marzo del año 2001.

[204] ÁLVAREZ-CIENFUEGOS, José M. La defensa de la Intimidad de los Ciudadanos y la Tecnología Informática. Arazandi 1999, citado por LLANEZA GONZÁLEZ, Paloma. *Op. Cit.* Pp. 259.

[205] PÉREZ LUÑO, 1989: 140 En <http://comunidad.derecho.org/congreso/ponencia29.html> Fecha de acceso: 06 de marzo del año 2001.

[206] HERRÁN ORTIZ, Ana Isabel. *Op. Cit.* Pp. 76 y ss.

[207] Otro partidario de este término es José Cuervo Álvarez. En Delitos Informáticos: protección penal de la intimidad. En http://publicaciones.derecho.org/redi/No._06_-_Enero_de_1999/cuervo Fecha de acceso: 10 de marzo del año 2001.

[208] *Ibidem*.

[209] *Ibidem*.

[210] Conferencia dada en el Congreso "Nuevas Tendencias del Tercer Milenio: Nuevas Perspectivas del Derecho Penal y Procesal Penal" Universidad de Lima. Año 2000. De igual manera, sobre la responsabilidad de las personas jurídicas en MUÑOZ CONDE, Francisco y GARCÍA ARAN, Mercedes. *Op. Cit.* Pp. 248 y ss.

[211] Al respecto PÉREZ LUÑO opina que el artículo 200 del Código penal español extiende a las personas jurídicas la

tutela penal de la intimidad, cuando se descubren o revelan datos reservados de personas jurídicas sin el consentimiento de sus representantes legales. En este punto, el nuevo Código penal español corrige uno de los aspectos más insatisfactorios de la LORTAD. A medida que el proceso de datos se proyecta a las empresas, a las instituciones y asociaciones, se hace cada vez más evidente la conveniencia de no excluir a las personas jurídicas del régimen de protección que impida o repare los daños causados por la utilización indebida de informaciones que les conciernen. En efecto, la defensa de la intimidad y los demás derechos fundamentales no es privativa de los individuos, sino que debe proyectarse a las formaciones sociales en las que los seres humanos desarrollan plenamente su personalidad. *Vid.* HERRÁN ORTIZ, Ana Isabel. *Op. Cit.* Pp. 233 y ss., en donde se establece la titularidad del derecho a la autodeterminación informativa y la problemática en torno a las personas jurídicas.

[212] En <http://comunidad.derecho.org/congreso/ponencia29.html> Fecha de acceso: 06 de marzo del año 2001.

[213] Diccionario de la Real Academia de la Lengua Española. Vigésima Primera edición. Editorial Espasa Calpe S.A. Madrid, 1997.

[214] ALTMARK, Daniel citado por MAGLIONA MARKOVICTH, Claudio Paul y LOPEZ MENDEL, Macarena. Delincuencia y Fraude Informático. Editorial Jurídica de Chile. Santiago de Chile, Año 1999. Pp. 19.

[215] MARTINEZ NADAL. Citado por LLANEZA GONZALES, Paloma. *Op. Cit.* Pp. 295.

[216] LLANEZA GONZALES, Paloma. *Op. Cit.* Pp. 295-296.

[217] Sobre medidas de seguridad *Vid.* ESPINOZA CÉSPEDES, José Francisco. Contratación Electrónica, Medidas de Seguridad y Derecho Informático. *Op. Cit.* Pp. 79 y ss.

[218] Interesantes páginas web sobre este tema son: <http://www.geocities.com/CapeCanaveral/2566/>, <http://www.geocities.com/CapeCanaveral/2566/seguri/seguri.html> y <http://www.kriptopolis.com/>.

[219] Los más importantes son los siguientes:

- Intercambio de autenticación: corrobora que una entidad, ya sea origen o destino de la información, es la deseada, *E.g.*, A envía un número aleatorio cifrado con la clave pública de B, B lo descifra con su clave privada y se lo reenvía a A, demostrando así que es quien pretende ser. Por supuesto, hay que ser cuidadoso a la hora de diseñar estos protocolos, ya que existen ataques para desbaratarlos.
- Cifrado: garantiza que la información no es inteligible para individuos, entidades o procesos no autorizados (confidencialidad). Consiste en transformar un texto en claro mediante un proceso de cifrado en un texto cifrado, gracias a una información secreta o clave de cifrado. Cuando se emplea la misma clave en las operaciones de cifrado y descifrado, se dice que el criptosistema es simétrico. Estos sistemas son mucho más rápidos que los de clave pública, resultando apropiados para funciones de cifrado de grandes volúmenes de datos. Se pueden dividir en dos categorías: cifradores de bloque, que cifran los datos en bloques de tamaño fijo (típicamente bloques de 64 bits), y cifradores en flujo, que trabajan sobre flujos continuos de bits. Cuando se utiliza una pareja de claves para separar los procesos de cifrado y descifrado, se dice que el criptosistema es asimétrico o de clave pública. Una clave, la privada, se mantiene secreta, mientras que la segunda clave, la pública, puede ser conocida por todos. De forma general, las claves públicas se utilizan para cifrar y las privadas, para descifrar. El sistema tiene la propiedad de que a partir del conocimiento de la clave pública no es posible determinar la clave privada. Los criptosistemas de clave pública, aunque más lentos que los simétricos, resultan adecuados para las funciones de autenticación, distribución de claves y firmas digitales.
- Integridad de datos: este mecanismo implica el cifrado de una cadena comprimida de datos a transmitir, llamada generalmente valor de comprobación de integridad (*Integrity Check Value* o ICV). Este mensaje se envía al receptor junto con los datos ordinarios. El receptor repite la compresión y el cifrado posterior de los datos y compara el resultado obtenido con el que le llega, para verificar que los datos no han sido modificados.
- Firma digital: este mecanismo implica el cifrado, por medio de la clave secreta del emisor, de una cadena comprimida de datos que se va a transferir. La firma digital se envía junto con los datos ordinarios. Este mensaje se procesa en el receptor, para verificar su integridad. Juega un papel esencial en el servicio de no repudio.
- Control de acceso: esfuerzo para que sólo aquellos usuarios autorizados accedan a los recursos del sistema o a la red, como *E.g.* mediante las contraseñas de acceso.

- Tráfico de relleno: consiste en enviar tráfico espurio junto con los datos válidos para que el atacante no sepa si se está enviando información, ni qué cantidad de datos útiles se está transmitiendo.
- Control de encaminamiento: permite enviar determinada información por determinadas zonas consideradas clasificadas. Asimismo posibilita solicitar otras rutas, en caso que se detecten persistentes violaciones de integridad en una ruta determinada.
- Unicidad: consiste en añadir a los datos un número de secuencia, la fecha y hora, un número aleatorio, o alguna combinación de los anteriores, que se incluyen en la firma digital o integridad de datos. De esta forma se evitan amenazas como la reactuación o resecuenciación de mensajes.

Los mecanismos básicos pueden agruparse de varias formas para proporcionar los servicios previamente mencionados. Conviene resaltar que los mecanismos poseen tres componentes principales:

- Una información secreta, como claves y contraseñas, conocidas por las entidades autorizadas.
- Un conjunto de algoritmos, para llevar a cabo el cifrado, descifrado, hash y generación de números aleatorios.
- Un conjunto de procedimientos, que definen cómo se usarán los algoritmos, quién envía qué a quién y cuándo.

Asimismo es importante notar que los sistemas de seguridad requieren una gestión de seguridad. La gestión comprende dos campos bien amplios:

- Seguridad en la generación, localización y distribución de la información secreta, de modo que sólo pueda ser accedida por aquellas entidades autorizadas.
- La política de los servicios y mecanismos de seguridad para detectar infracciones de seguridad y emprender acciones correctivas. En <http://www.geocities.com/CapeCanaveral/2566/intro/mecanism.html>. Fecha de acceso: 23 de febrero del año 2000.

[220] Cfr. al respecto SILVA SÁNCHEZ, Jesús María. La Expansión del Derecho Penal. *Op. Cit.* Pp. 24.

[221] SILVA SÁNCHEZ, Jesús María. Expansión del Derecho Penal. *Op. Cit.* Pp. 26.

[222] Un caso importante es el del servicio de Internet Bibliofind.com, propiedad de Amazon.com que ha reiniciado de nuevo esta semana su servicio de venta de libros por Internet, después de que un ataque por parte de unos *hackers* acabase en la desconexión de la web y más de 98.000 fichas de usuarios que se hicieron públicas. El principal atractivo de Bibliofind.com consiste en que facilita a todos los usuarios el poder conseguir esos libros que son realmente complejos de conseguir, bien porque hace tiempo que no se imprimen o porque se imprimieron muy pocas unidades. Al parecer un *hacker* obtuvo acceso a la web el pasado mes de octubre y había conservado el acceso no autorizado desde entonces. El *hacker* se dedicó a descargar del servidor las fichas de algunos clientes, en las que se incluían los nombres, direcciones y números de tarjeta de crédito entre otros datos. La primera reacción de la compañía al enterarse consistió en paralizar el servicio y borrar todos los datos comprometidos del servidor, informando al FBI poco después. Tal como lo expresó la propia compañía en un mensaje de e-mail dirigido a todos sus clientes: "Bibliofind ha tenido reciente conocimiento de una violación en la seguridad de su web que ha puesto en peligro la información de las tarjetas de crédito que existían en nuestro servidor. Estamos trabajando para reanudar el servicio. Sentimos los inconvenientes que esto haya podido causar". Lo siguiente fue advertir a las compañías de tarjetas de crédito, que no saben hasta el momento si dichos números se han llegado a usar de forma fraudulenta. Varios expertos en seguridad informática aseguran que lo más peligroso es que con ese prolongado tiempo sin ser descubierto el *hacker* podría haber encontrado alguna forma de acceder de forma ilegal a Amazon.com. La propia Amazon ha declarado al respecto que no han sufrido el ataque en sus servidores centrales y que la información de sus clientes no se ha visto comprometida. <http://delitosinformaticos.com-/noticias/98395846971449.htm>. Fecha de acceso: 10 de marzo del año 2001.

[223] SILVA SÁNCHEZ, Jesús María. La Expansión del Derecho Penal. *Op. Cit.* Pp. 29. El referido autor señala que no se trata de la seguridad en un sentido amplio, como podría pensarse acerca de la seguridad ciudadana que requeriría, sin lugar a dudas, una intervención policial y del Derecho penal, sino de las necesidades de regulación de la participación de los sujetos en la red, a mayor regulación mayor seguridad.

[224] GUTIÉRREZ FRANCÉS, Mariluz. Notas sobre la delincuencia informática: atentados contra la "información" como valor económico de empresa, en: Mazuelos Coello, Julio (comp.). Derecho Penal Económico y de la Empresa. Editorial San

Marcos. Lima. Año 1997. Pp. 383 y ss.

[225] MAZUELOS COELLO, Julio F. Protección Jurídico Penal de la Información como valor económico de la empresa. En Revista Legal del Estudio Muñiz, Forsyth, Ramírez, Pérez-Taimán y Luna-Victoria Abogados. Marzo de 1999. Pp. 38.

[226] JIJENA LEIVA, Renato. *Op. Cit.* Pp. 149.

[227] ÁLVAREZ-CIENFUEGOS, José M. La defensa de la Intimidad de los Ciudadanos y la Tecnología Informática. Arazandi 1999, citado por LLANEZA GONZÁLEZ, Paloma. *Op. Cit.* Pp. 259.

[228] En <http://comunidad.derecho.org/congreso/ponencia29.html>. Fecha de acceso: 07 de marzo del año 2001.

[229] JIJENA LEIVA, Renato. *Op. Cit.* Pp. 93.

[230] Sobre el valor económico de la información y la actividad de la empresa en RIQUERT, Marcelo. Informática y Derecho penal argentino. Ad-Hoc. Buenos Aires, Año 1999. Pp. 74 y ss.

[231] MAZUELOS COELLO, Julio F. Protección Jurídico Penal de la Información como valor económico de la empresa. *Op. Cit.* Pp. 40.

[232] *Ibidem.*

[233] Vid. RIQUERT, Marcelo. *Op. Cit.* Pp. 61.

[234] RIQUERT, Marcelo. *Op. Cit.* Pp. 62.

[235] Al respecto, MAZUELOS COELLO, Julio F. Protección Jurídico Penal de la Información como valor económico de la empresa. *Op. Cit.* Pp. 40.

[236] En igual sentido, REYNA ALFARO, Luis Miguel. En <http://publicaciones.derecho.org/redp>. Fecha de acceso: 18 de abril del año 2001.

[237] RODAS MONSALVE, Julio C. Protección penal y medio ambiente. PPU. Barcelona. Año 1993. Pp. 74.

[238] BUSTOS RAMIREZ, Juan. Control Social y Sistema Penal. PPU. Barcelona. Año 1987. Pp. 197.

[239] *Ibidem.*

[240] MUÑOZ CONDE, Francisco y GARCÍA ARAN, Mercedes. *Op. Cit.* Pp. 89.

[241] En <http://publicaciones.derecho.org/redi/No.06-Enero-de-1999/cuervo> Fecha de acceso: 10 de marzo del año 2001.

[242] HUERTA MIRANDA, Marcelo y LIBANO MANSSUR, Claudio. *Op. Cit.* Pp. 114.

[243] TÉLLEZ VALDÉS, citado por CUERVO ALVAREZ en <http://publicaciones.derecho.org/redi/No.06-Enero-de-1999/cuervo> De igual manera en <http://publicaciones.derecho.org/redi/No.09-Abril-de-1999/viega> Fecha de acceso: 10 de marzo del año 2000.

[244] SÁNCHEZ ALMEIDA, Carlos. El Hacking ante el Derecho Penal. Una visión libertaria. En Revista Electrónica de Derecho Informático. <http://publicaciones.derecho.org/redi/No.13-agosto-de-1999/ponencia> Fecha de acceso: 11 de marzo del año 2001. Para el referido autor, el *hacker* es el alquimista de nuestros días, la persona que busca el conocimiento absoluto. Así, considera al *hacker* como cualquier heterodoxo, que ya desde niño quiere ir más allá del libro de instrucciones.

[245] Existen muchos softwares que hacen posible la comunicación por computadora a un teléfono como el “Net2Phone!” creado por IDT Corporation que permite realizar llamadas internacionales desde una computadora personal a un teléfono fijo o celular a cualquier parte del mundo. El sistema se basa en la transmisión de la voz vía Internet. El software o programa digitaliza la voz para que viaje a través de la red. Esta nueva modalidad de comunicarse por teléfono se ha desatado con fuerza en los países donde la tecnología se encuentra en mayor desarrollo esta posibilidad estará disponible en mayor volumen en la medida que la tecnología derivada se extienda a otros, lo que permite comunicarse de una PC hacia un teléfono o de una PC

hacia otra PC. Los usuarios no necesitan coordinar con su interlocutor la hora y el día para estar en línea en el momento de la llamada. Quien efectúa la llamada sólo necesita una PC con conexión a Internet para comunicarse con otra persona.

[246] MARCHENA GÓMEZ, Manuel. Prevención de la delincuencia tecnológica. Derecho de Internet. Contratación Electrónica y Firma Digital. MATEU DE ROS, Rafael y CENDOYA MENDEZ DE VIGO, Juan Manuel. (Coordinadores) Autores Varios. Arazandi Editorial. Navarra, Año 2000. Pp. 442.

[247] Título de una exposición celebrada en Madrid el 18 de junio de 1998, por la FUNDESCO, en donde se puso de manifiesto que Internet populariza nuevos delitos surgidos a través de la red, sin embargo, también fomenta delitos tradicionales en GUTIERREZ ZARZA, Ángeles. Investigación y Enjuiciamiento de los Delitos Económicos. Editorial Colex. Madrid, 2000. Pp. 53.

[248] En sentido contrario AVÁLOS CISNEROS, María. En Diario El Peruano. Lima, 18 de febrero del año 2000. En donde señala que la sociedad ha confeccionado su propio estereotipo del autor de la delincuencia informática; se trataría de adolescentes de clase social media, inofensivos, con ausencia de toda conciencia de estar obrando mal, inteligentes y casi siempre varones. Una persona con coeficiente intelectual próximo a la genialidad y con gran dominio del complejo mundo de las computadoras.

[249] TIEDEMANN, Klaus. *Op. Cit.* Pp. 90.

[250] BRAMONT-ARIAS TORRES, Luis Alberto. El delito Informático en el Código penal Peruano. *Op. Cit.* Pp. 71.

[251] Un ejemplo de esta afirmación en la noticia siguiente: El joven holandés "On the Fly", que propagó el virus "Kournikova", y el quinceañero canadiense "Mafiaboy", que paralizó parte de Internet a principios del 2000, comparten una característica: no tienen grandes conocimientos informáticos. La elite mundial de los piratas informáticos les califica de "niños de la programación", un término adoptado también por las empresas de seguridad informática para describir a quienes no son capaces de escribir el código de sus propios programas y utilizan productos de otros piratas para sus fechorías. En el caso de "On the Fly", el joven holandés se sirvió de un programa en Visual Basic -lenguaje para crear "scripts" o programas de Microsoft-, escrito por un pirata argentino conocido como "Kalamar", para crear el virus "Kournikova". "'On the Fly' no hizo nada más que apretar un par de botones y distribuir el virus" explicó David Perry, director de Educación Global de la empresa de seguridad informática Trend Micro, una de las primeras compañías que detectó la procedencia holandesa de "Kournikova" e identificó a "Kalamar" como origen del programa utilizado para crear el virus.

[252] De la misma opinión Viega Rodríguez, María J. En [http://publicaciones.derecho.org/redi/No. 09 -Abril de 1999/viega](http://publicaciones.derecho.org/redi/No.09-Abril de 1999/viega) En donde señala que el delincuente informático se puede tratar de personas muy diferentes, ya que no es lo mismo el joven que entra a un sistema de seguridad como desafío personal, que el empleado de una institución financiera que desvía fondos de las cuentas de sus clientes. Fecha de acceso: 23 de marzo del año 2000.

[253] Entre ellos, los *Hackers*, *Crackers*, *Bocaneros*, etc.

[254] Un ejemplo en cuanto a los gobiernos, como sujetos pasivos, fue el gobierno de Uruguay, en donde piratas se hicieron con el control de www.mgap.gub.uy, donde realizaron inscripciones y símbolos anarquistas, incluyendo la proclama "Anarquía por siempre". Esta no es la primera vez que una web gubernamental del país latino americano sufre ataques. Recientemente, en el sitio del ministerio de Trabajo y Seguridad Social, www.mtss.gub.uy, aparecieron frases protestando por el desempleo que afecta al país (14 por ciento de la fuerza laboral). Según el portavoz del ministerio de Ganadería, las páginas del gobierno no tiene la tecnología adecuada para evitar estos ataques. Para mayor información en <http://www.delitosinformaticos.com/noticias/9835302575453.htm> Fecha de acceso: 05 de marzo del año 2001.

[255] DE PABLO ORTIZ, José M. Artículo publicado en la red, en donde realiza una breve exposición sobre el tema. Interesantes (y discutibles) sus consideraciones respecto la clasificación de delitos y delincuentes. <http://www2.compendium.com.ar/juridico/depablo.html>. Fecha de acceso: 17 octubre del año 2000.

[256] MAZUELOS COELLO, Julio. (Comp.) Derecho Penal Económico y de la Empresa. *Op. Cit.* Pp. 387.

[257] BRAMONT-ARIAS, Luis Alberto y BRAMONT-ARIAS TORRES, Luis Alberto. Código penal Anotado. *Op. Cit.* Pp. 55

[258] REYNA ALFARO, Luis Miguel. Los delitos informáticos en el Código penal Peruano: Análisis del tipo de injusto de los artículos 207-A, 207-B y 207-C del Código penal peruano y propuestas de política criminal. Pp. 59.

[259] MUÑOZ CONDE, Francisco citado por BRAMONT-ARIAS, Luis Alberto. El delito informático en el Código penal peruano. *Op. Cit.* Pp. 63-64.

[260] El artículo 886 del C.c. establece lo siguiente: Son muebles:

1. Los vehículos terrestres de cualquier clase.
2. Las fuerzas naturales susceptibles de apropiación.
3. Las construcciones en terreno ajeno, hechos para un fin temporal.
4. Los materiales de construcción o procedentes de una demolición si no están unidos al suelo.
5. Los títulos valores de cualquier clase o los instrumentos donde conste la adquisición de créditos o derechos personales.
6. Los derechos patrimoniales de autor, de inventor, de patentes, nombres, marcas y otros similares.
7. Las rentas o pensiones de cualquier clase.
8. Las acciones o participaciones que cada socio tenga en sociedades o asociaciones, aunque a éstas pertenezca bienes inmuebles.
9. Los demás bienes que puedan llevarse de un lugar a otro.
10. Los demás bienes no comprendidos en el artículo 885.

[261] Diario El Peruano. 18 de febrero del año 2000. Pp. 10.

[262] *Ibidem.* “El presidente de la Sociedad Nacional de Industria se dejó un agresivo llamado a favor de la tarifa plana en Argentina y en el Infopuc se insertó un sarcástico texto burlándose de la falta de seguridad de los servidores web de esa institución.”

[263] *Ibidem.* Sistemas informáticos de la Casa Blanca, el Pentágono y el Congreso de Estados Unidos, así como de organismos gubernamentales en Chile, fueron objeto de ingresos indebidos por delincuentes informáticos.

[264] *Ibidem.* “El ingreso de un ciberpirata o *hacker* a la página web de la Oficina Nacional de Procesos Electorales (ONPE) ha puesto sobre el tapete el tema de los delitos informáticos y, con esto, la necesidad de incluir éste ilícito en el Código penal peruano.”

[265] *Ibidem.* “... Raúl Chanamé Orbe, especialista en Derecho Constitucional, mencionó que resulta necesario proponer una legislación internacional ad hoc para frenar a estas personas que infiltran, alteran y dañan las redes de cómputo de diversas instituciones en todo el mundo.

[266] Los proyectos N° 5071/99, presentados por el congresista Jorge Muñoz Ziches, y el N° 5132/99 elaborado por la congresista Ivonne Susana Díaz Díaz y el dictamen favorable de la Comisión de Reforma del Código penal del Congreso de la República fueron determinante para la promulgación de la ley que incorpora los delitos informáticos al Código penal Peruano.

[267] Diario El Peruano. Lima, 30 de mayo del año 2000. Pp. 10.

[268] *Ibidem.*

[269] Diario El Comercio. Lima, 4 de junio del año 2000. Pp. E14.

[270] Sobre los Delitos de Hacking en sus diversas manifestaciones en: HUERTA MIRANDA, Marcelo y LIBANO MANSSUR, Claudio. Delitos Informáticos. *Op. Cit.* Pp. 168 y ss.

- [271] En este mismo sentido, BRAMONT-ARIAS, Luis Alberto. El delito informático en el Código penal Peruano. *Op. Cit.* Pp. 72.
- [272] MAQUEDA AGREU, María. La idea de peligro en el Derecho penal moderno. Algunas reflexiones a propósito del proyecto del Código Penal de 1992. *Actualidad Penal. Volumen I.* Pp. 492.
- [273] Real Academia Española. Diccionario de la Lengua Española. T. II. 21 Madrid, Año 1992. Pp. 1156.
- [274] CABANELLAS, G. "Diccionario Enciclopédico de Derecho Usual". T. IV. 24 Editorial Heliasta. Buenos Aires, Año 1996. Pp. 383. Indebidamente: Sin ser debido. Contra deber. De modo ilícito. indebido: Lo que no es obligatorio. Inexigible. Injusto. Ilícito. Ilegal. Antirreglamentario.
- [275] BRAMONT-ARIAS, Luis Alberto. El delito informático en el Código penal Peruano. *Op. Cit.* Pp. 72.
- [276] A esta conclusión llega: BRAMONT-ARIAS, Luis Alberto. El delito informático en el Código penal Peruano. *Op. Cit.* Pp. 71.
- [277] BRAMONT-ARIAS, Luis Alberto. El delito informático en el Código penal Peruano. *Op. Cit.* Pp. 74.
- [278] BRAMONT-ARIAS, Luis Alberto. El delito informático en el Código penal Peruano. *Op. Cit.* Pp. 73.
- [279] BRAMONT-ARIAS, Luis Alberto. El delito informático en el Código penal Peruano. *Op. Cit.* Pp. 74.
- [280] REYNA ALFARO, Luis Miguel. *Op. Cit.* Pp. 61.
- [281] El artículo 39 de nuestro C.p. establece lo siguiente: "La inhabilitación se impondrá como pena accesoria cuando el hecho punible cometido por el condenado constituye abuso de autoridad, de cargo, de profesión, oficio, poder o violación de un deber inherente a la función pública, comercio, industria, patria potestad, tutela, curatela, o actividad regulada por ley. Se extiende por igual tiempo que la pena principal."
- [282] En el mismo sentido, BRAMONT-ARIAS, Luis Alberto. El delito informático en el Código penal Peruano. *Op. Cit.* Pp. 74. El artículo 251-A señala lo siguiente: "El que obtiene un beneficio o se evita un perjuicio de carácter económico en forma directa o a través de terceros, mediante el uso de información privilegiada, será reprimido con pena privativa de libertad no menor de uno ni mayor de cinco años. Si el delito a que se refiere en el párrafo anterior es cometido por un director, funcionario, o empleado de una Bolsa de Valores, de un agente de intermediación, de las entidades supervisoras de los emisores, de las clasificadoras de riesgo, de las administradoras de fondos mutuos de inversión en valores, de las administradoras de fondos de inversión, de las administradoras de pensiones, así como de las empresas bancarias, financieras o de seguros, la pena no será menor de cinco ni mayor de siete años."
- [283] SÁNCHEZ ALMEIDA, Carlos. El Hacking ante el Derecho Penal. Una visión Libertaria. Redi, número 13-Agosto de 1999, citado por LLANEZA GONZÁLES, Paloma. Internet y Comunicaciones Digitales. *Op. Cit.* Pp. 244. Igualmente en Sánchez Almeida, Carlos. En Revista Electrónica de Derecho Informático. Para mayor información en http://publicaciones.derecho.org/redi/No.13_agosto_de_1999/ponencia un interesante artículo a favor de la exclusión del hacking como delito en el derecho penal español. Fecha de acceso: 30 de marzo del año 2001.
- [284] En el mismo sentido, RIQUEERT, Marcelo. *Op. Cit.* Pp. 75.
- [285] RIQUEERT, Marcelo. *Op. Cit.* Pp. 74 y ss.
- [286] LLANEZA GONZÁLES, Paloma. *Op. Cit.* Pp. 247.
- [287] SÁNCHEZ ALMEIDA, Carlos. El Hacking ante el Derecho Penal. Una visión libertaria. En Revista Electrónica de Derecho Informático. http://publicaciones.derecho.org/redi/No.13_agosto_de_1999/ponencia. Fecha de acceso: 16 de marzo del año 2001.
- [288] El artículo 1 establece a su tenor lo siguiente: La Ley Penal peruana se aplica a todo el que comete un hecho punible en el territorio de la República, salvo las excepciones contenidas en el Derecho Internacional. También se aplica a los hechos punibles cometidos en: 1.- Las naves o aeronaves nacionales públicas, en donde se encuentren; y, 2.- Las naves o aeronaves nacionales privadas, que se encuentren en alta mar o en espacio aéreo donde ningún Estado ejerza soberanía.

- [289] MUÑOZ CONDE, Francisco y GARCÍA ARAN, Mercedes. *Op. Cit.* Pp. 167.
- [290] BRAMONT-ARIAS, Luis Alberto y GARCÍA CANTIZANO, María del Carmen. *Op. Cit.* Pp. 149. "... cuyo precursor fue BINGING, según la cual, el delito debe reputarse cometido tanto donde se ejecuta la acción como allí donde se produce el resultado, ya que el Derecho penal ha de tomar en cuenta tanto el desvalor de acto como de resultado y además sólo así se evitan impunidades injustas".
- [291] MUÑOZ CONDE, Francisco y GARCÍA ARAN, Mercedes. *Op. Cit.* Pp. 171.
- [292] El artículo 5 del C.p. establece lo siguiente: "El lugar de comisión de un delito es aquél en el cual el autor o partícipe ha actuado u omitido la obligación de actuar o en el que se producen sus efectos".
- [293] El texto integro de esta Posición Común se puede ver en http://europa.eu.int/eurlex/es/lif/dat/1999/es_499X0364.-html.
- [294] Entre los aspectos que recogerá dicho convenio serán el acceso ilegal a sistemas informáticos, la interceptación ilegal de transmisiones de datos, la interferencia de datos y de sistemas, tanto si se hace con el fin de obtener un beneficio económico o no. Entre otros proyectos, la futura ley preverá un artículo dedicado a la pornografía infantil y a los derechos de autor. El proyecto de Convención es el resultado de cuatro años de trabajo de los expertos del Consejo de Europa. Tiene por objetivo, declarado en su preámbulo, "llevar a cabo una política penal común destinada a proteger a la sociedad de la criminalidad en el ciberespacio, singularmente mediante la adopción de una legislación apropiada y mediante la cooperación internacional". En <http://www.delitosinformaticos.com-/noticias/98353057377944.htm> Fecha de acceso: 05 de marzo del año 2001. Este convenio permitirá a la policía -siempre bajo mandato judicial- el embargo de datos y material informático, la recogida de informaciones *online* e, incluso, interceptar contenidos mediante la captación de comunicaciones vocales o escritas entre ordenadores. Asimismo, para luchar contra estos delitos, el proyecto de convenio permite a la policía de los estados una serie de poderes sobre la red -muy criticados por los grupos defensores de la libertad de expresión y los proveedores de servicios de Internet- y otorgará a los diferentes organismos y fuerzas de seguridad la potestad para obligar a empresas y servidores a conservar datos de divulgación, tráfico y conexión, para poder rastrear, *E.g.*, el origen de un ataque informático. El convenio dará a luz un texto vinculante ya -para todos los países que lo suscriban-, que pretende armonizar los marcos legales de los 41 países miembros del Consejo de Europa, además de Estados Unidos, Canadá, Japón y Sudáfrica, para luchar contra los delitos que se cometen en la red y en los sistemas informáticos, desde la difusión de contenidos ilegales hasta los ataques de piratas informáticos, "ciberterroristas". <http://delitosinformaticos.com/noticias/98404275043664.htm> Fecha de acceso: 10 de marzo del año 2001. El proyecto sobre el Convenio se encuentra disponible en Internet en la siguiente dirección: <http://conventions.coe.int/treaty/en/projets/cybercrime.htm> Fecha de acceso: 4 de mayo del año 2001.
- [295] Al respecto, MARCHENA GÓMEZ, Manuel. Prevención de la delincuencia tecnológica. *Op. Cit.* Pp. 447-448.
- [296] MIR PUIG, Santiago. Derecho Penal. Parte General. Cuarta Edición PPU. Barcelona. Año, 1996. Pp. 89.
- [297] MIR PUIG, Santiago. Derecho Penal. *Op. Cit.* Pp. 89.
- [298] JIJENA LEIVA, Renato. *Op. Cit.* Pp. 63.
- [299] El Parágrafo 202 a tipifica el delito de espionaje de datos en los siguientes términos: "202 a I. Quien consiga sin autorización, para sí o para otro, datos que no le competan y que estén especialmente protegidos contra el acceso ilegítimo, será castigado con pena privativa de libertad de hasta tres años o con multa. II. Datos, a efectos del apartado I, serán sólo aquellos que no sean almacenados, transmitidos electrónica, magnéticamente, o de forma inmediatamente accesible."
- [300] *Cfr.:* EIRANOVA, Emilio. (Coord.) "Código penal alemán StGB. Código procesal penal alemán StPO". Marcial Pons. Madrid – Barcelona, Año 2000.
- [301] El delito de estafa se sanciona en el StGB en los siguientes términos: "263 I. Quien, con la intención de procurar para sí o para un tercero una ventaja patrimonial ilícita, perjudique el patrimonio de otro causando un error o manteniéndolo, por medio de la apariencia de hechos falsos o de la desfiguración o supresión de hechos verdaderos, será castigado con pena de privación de libertad de hasta cinco años o con multa.
- II. La tentativa será punible.
- III. En casos de especial gravedad la pena será de privación de libertad de uno a diez años.

IV. Procederá aplicar los 243, apartado II, así como el 247 y 248 a.

V. El tribunal podrá ordenar la vigilancia orientadora (68, apartado I)".

[302] El apartado III del Parágrafo 267 establece que en los casos especialmente graves la pena será de privación de libertad no inferior a un año.

[303] CUERVO ALVAREZ, J. Delitos Informáticos: protección penal de la intimidad. Ver en http://publicaciones.derecho.org/redi/No.06_Enero_de_1999/cuervo. Fecha de acceso: 10 de marzo del año 2001.

[304] Hasta la propia [Dirección General de Policía](#) en España, al igual que muchos otros países, ha tenido que crear un Grupo dedicado en exclusiva a combatir los delitos informáticos.

[305] Un caso importante es el que define la Audiencia Provincial de Valladolid: "El acusado, que prestaba sus servicios para la entidad denunciante asociación de parapléjicos y grandes minusválidos físicos, como conserje, merced a un acuerdo con los servicios de asistencia social de la prisión en la que se encontraba cumpliendo condena, en régimen abierto, sin disponer de autorización alguna, o en todo caso, sin la de los responsables de prestarla, se apoderó de datos de carácter reservado, de índole personal y familiar, registrados en soporte informático, de la asociación, mediante la toma de los disquetes que se encontraban en las oficinas, para copiar sus datos y transferirlos a su ordenador personal –en disco duro- o, en otras ocasiones, mediante el acceso o lectura de referidos datos en su propio equipo informático, con un claro perjuicio, para los propios interesados o titulares de los datos muy variados: domicilios, teléfonos, cuentas bancarias, estado y condiciones de salud física y mental, informes psicológicos, gastos, presupuestos, etc.- y para la propia asociación, al acceder igualmente a su información reservada de administración y al verse quebrada la confianza y reserva puesta en ella por lo socios; tales hechos son legalmente constitutivos de un delito de revelación de secretos, previsto y penado en el Art. 197 CP." En LLANEZA GONZÁLES, Paloma. *Op. Cit.* Pp. 252. El mismo ejemplo en Sánchez Almeida, Carlos. El Hacking ante el Derecho Penal. Una visión libertaria. En Revista Electrónica de Derecho Informático. Para más información, http://publicaciones.derecho.org/redi/No.13_agosto_de_1999/ponencia

[306] En este precepto se convierten en delito actividades que antes sólo tenían sanción administrativa, al tipificar un elenco de conductas que implican abusos informáticos contra la "privacy" o libertad informática.

[307] En este sentido, MATELLANES RODRÍGUEZ, Nuria. *Op. Cit.* Pp. 136-137.

[308] Existe actualmente la concepción que el secreto ya no sólo pueden estar comprendidos en papeles ni cartas, o comunicaciones telefónicas, sino más bien, en correos electrónicos o sistemas informáticos.

[309] LLANEZA GONZÁLES, Paloma. *Op. Cit.* Pp. 249.

[310] La Sala VI de la Cámara del Crimen Argentina, en un fallo en el que se condenaba a un periodista por publicar un correo que no le había sido remitido, señaló, en igual sentido que la legislación penal española que la "comunicación electrónica es un verdadero correo en versión actualizada y, en tal sentido, la correspondencia y todo lo que por su conducto pueda ser transmitido o receptado, goza de la misma protección que las cartas". En LLANEZA GONZÁLES, Paloma. *Op. Cit.* Pp. 249.

[311] Así, el artículo 198 del C.p.e. establece lo siguiente:

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.

[312] Que Internet es asimilable a cualquier otro medio lo afirma una sentencia de un Juzgado de Barcelona que castiga por una falta de vejación injusta del artículo 620.2 del C.p. a un estudiante que se hizo pasar por una compañera de clase en un chat haciendo ofertas de contenido sexual más que explícitas. La condena se produjo por la concatenación de diversos hechos que llevaron a la confesión del imputado. El estudiante usaba los ordenadores de la biblioteca de su Universidad desde donde accedía a los canales del IRC y los chats de contenido sexual. En, al menos, uno de ellos dijo ser su compañera, facilitando su

nombre y apellidos, dirección y teléfono, y haciendo, como si de ella se tratara, ofertas sexuales explícitas a diversos “cibervarones”. A consecuencia de una de esas tórridas “charlas”, uno de los contertulios se puso en contacto telefónico con la verdadera estudiante mostrándose interesado por el ofrecimiento sexual que ésta última había “realizado” a través de Internet. El contertulio leyó, ante el espanto de la estudiante, parte del “log” en el que había guardado las conversaciones mantenidas. Al mismo tiempo que hablaba por teléfono, el estudiante se encontraba chateando con el interlocutor bajo la apariencia de su compañera. Gracias a ello, y a la colaboración del “pretendiente” que localizó la máquina desde donde se enviaban las ofertas obscenas- el ordenador de la biblioteca de la Universidad- fue posible comprobar in situ que la única persona conectada en ese momento era el estudiante condenado, que confesó los hechos, manifestando, eso sí, que bromeaba. Probablemente si no se hubiese cogido in situ al estudiante, éste no habría admitido su actuación. Obviamente, el “pretendiente” que facilitó copia de los “logs” de las conversaciones rehusó identificarse, con lo que difícilmente hubiera sido posible castigar la actuación vejatoria. Ni que decir tiene que otro elemento esencial para lograr la condena, a parte de que no hubo que recurrir a complicadas periciales técnicas, fue que los hechos se produjeron en el territorio nacional y en un círculo restringido y localizable. Es evidente que estos hechos realizados desde otro país o sin la concurrencia de todos estos factores, habría quedado impune. En el terreno de las expresiones injuriosas, cabría considerar el uso de determinados “emoticones” (demostraciones de estados de ánimo y sentimientos), en todas sus gradaciones, como elementos vejatorios o injuriosos si suponen la representación iconográfica de un insulto.

[313] MATELLANES, Nuria. *Op. Cit.* Pp. 139. En palabras de Matellanes, “la nueva disposición suprime cualquier referencia al engaño, elemento cuya apreciación se rechazaba porque no era posible engañar a una máquina y en su lugar, se alude a manipulación fraudulenta o artificio semejante, por lo mismo renuncia al error y reduce el elenco de posibles actos de disposición del tipo básico a la transferencia de cualquier activo patrimonial en perjuicio de tercer. Con ello se elimina los más destacados obstáculos que a juicio de muchos autores impedían aplicar el delito de estafa a las defraudaciones mediante ordenador.”

[314] LLANEZA GONZALES, Paloma. *Op. Cit.* Pp. 247.

[315] Un caso relevante para la jurisprudencia penal española es la sentencia en el caso Hispahack. En abril de 1998, la Guardia Civil procedió a la detención de varios miembros de Hispahack, por varios hechos, tales como la presencia de un hacker en el sistema informático de la UPC, la inserción de un graffiti en la página principal del Congreso de los Diputados y el acceso ilegal a diversas Universidades y proveedores de Internet, incluida la NASA. El Juzgado de lo Penal número 2 de Barcelona, considera probado que el 11 de septiembre de 1997 se produjo un acceso no autorizado, a través de Internet, en los ordenadores ubicados en las dependencias de la UPC, desde un ordenador situado en un campus universitario, llegando a obtener los privilegios del administrador del sistema en, al menos, dieciséis máquinas servidoras e instalando programas “Sniffers” destinados a capturar información. Concretamente, se intentaba interceptar identificadores y claves de acceso de otros usuarios, enviando los datos obtenidos a un ordenador ubicado en un cibercafé, almacenándolos en el directorio denominado “jfs” correspondiente al usuario “Hispahack”. Sin embargo, a la vista del informe pericial, el Juzgado entiende que no se puede acreditar que el acusado JFS participase en esa entrada ilegal, ni en la obtención y transferencia de datos informáticos, por lo que procede a su absolución. El perito mantiene que los hechos relativos a la entrada en los servidores de la UPC encajan dentro de la definición de Hacking blanco, ya que no se observa la destrucción de ningún tipo de información. La sustracción de ficheros de passwords no supone, en opinión del perito, daño alguno, y lo justifica manifestando que los mismos son cambiados periódicamente y que la notificación de su sustracción se efectúa de un modo sencillo, mediante el envío de un correo electrónico. El informe pericial determina, además, que eran múltiples los usuarios que podían acceder a la información contenida en la cuenta HISPACHACK del ordenador ftp.laredcafe.com. Por ello, no sólo el imputado tuvo acceso a dicha cuenta de correo, sino que cualquier usuario pudo haber depositado la información en ese ordenador. De la información de ficheros de passwords encontrada en el ordenador del imputado sólo se deriva que la obtuvo de algún ordenador, que podría ser el que tiene por nombre ftp.laredcafe.com u otro distinto, pero este hecho prueba que fuera él quien obtuviese dichos datos de las fuentes originarias, y que, por ello, fuera el quien accedió manera in consentida a los sistemas vulnerados.

[316] LLANEZA GONZÁLEZ, Paloma. *Op. Cit.* Pp. 251.

[317] Ver crítica en [http://publicaciones.derecho.org/redi/No.06 - Enero de 1999/cuervo](http://publicaciones.derecho.org/redi/No.06-Enero-de-1999/cuervo). Fecha de acceso: 10 de marzo del año 2001.

[318] Un caso reciente es que la Comisión de Valores y Mercados de Estados Unidos acusó a 23 compañías e individuos de usar Internet fraudulentamente para hacer subir los precios de una serie de acciones en más de \$300 millones y recaudar \$2.5 millones entre los inversores. En su quinta “batida” nacional contra las estafas informáticas, el ente regulador de los mercados

financieros de Estados Unidos, conocido por sus siglas inglesas SEC, dijo que los acusados usaron "spam" o mensajes electrónicos en masa, boletines electrónicos, sitios web, hiperenlaces, tabloneros de edictos y otros medios de Internet en casos que involucran tanto inversiones cotizadas en bolsa como empresas de capital privado. Los inversores en Internet deben tener presente que no hay frontera claramente delineada entre información confiable y no confiable", dijo el jefe de aplicación de normas de la SEC. Por tanto, los inversores deben ser extremadamente cautelosos cuando reciben exhortaciones online", agregó. Con las medidas de ayer, la cantidad total de casos de Internet presentados por la SEC pasa de 200. En <http://delitosinformaticos.com/noticias/98378704517479.htm> Fecha de acceso: 5 de marzo del año 2001.

[319] En www.delitosinformaticos.com. Artículo publicado por Richard Power del Computer Security Institute. Fecha de acceso 30 de setiembre del año 2000.

[320] Como *E.g.*, en casos de robo de passwords o código de acceso.

[321] El delito debe ser cometido conscientemente y con voluntad de estafar. Igualmente para el resto de categorías.

[322] Esto incluiría el uso de "Red Boxes", "Blue Boxes" y teléfonos celulares reprogramados cuando el usuario legítimo del teléfono que se haya reprogramado no esté de acuerdo con esa acción.

[323] Esto también incluye los scanners que mucha gente usa para interceptar llamadas de teléfonos celulares. Se produjo un gran escándalo cuando los medios de comunicación tuvieron noticia una llamada de un celular interceptado, la llamada correspondía al Portavoz de los Representantes de la Casa Blanca, New Gingrich.

[324] 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 [324] 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. Un ordenador de los dos o más que hayan sido usados para cometer el ataque, no estando todos ellos en el mismo estado.

[325] Esto puede ser aplicado a los synfloods y killer-pings así como también a otra clase de ataques que afecten el servicio ofrecido por los ordenadores-víctimas, así como también se incluye acceder a un ordenador saltándose las barreras de seguridad y jugar con él.

[326] Existen dos situaciones diferentes: cuando 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 cuando 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. La manera más común en que alguien se mete en problemas con esta parte del decreto es cuando intenta cubrir sus huellas tras haber traspasado las barreras de seguridad y accedido al sistema. Al editar, o, todavía peor, borrar varios archivos, el intruso puede accidentalmente borrar algo importante. O algún comando que él o ella teclee puede hacer que se cuelgue el sistema. Un simple ataque de "mail-bomb", "killer-ping", flood-ping, syn flood o ese gran número de exploits existentes para Windows NT en los que simplemente mandando un sólo comando a muchos puertos a la vez causa que un cuelgue, puede quebrantar esta ley. La otra situación es cuando la persona que realiza la transmisión no intenta hacer ningún daño pero actúa imprudentemente despreciando el riesgo que existe de que la transmisión causará daño a los propietarios u operadores de los ordenadores, y provoca \$1000 o más de pérdidas, o modifica o altera, o potencialmente modifica o altera un examen o tratamiento médico. Esto significa que incluso si se prueba que dañaste el ordenador por accidente, se puede ir a prisión.

[327] *Cfr.*, <http://publicaciones.derecho.org/redi/No. 09 - Abril de 1999/viega> Fecha de acceso: 11 de marzo del año 2001.

- [328] En <http://www.latinlex.com/cl/contenido/leg4.asp>. Fecha de acceso: 20 de febrero del año 2001.
- [329] *I.e.* desde 541 días hasta 5 años de cárcel.
- [330] Desde 61 días hasta 3 años de cárcel.
- [331] Desde 541 días hasta 3 años de presidio.
- [332] Desde 541 días hasta 3 años de cárcel. Si la persona es responsable del sistema, podría alcanzar hasta 5 años.
- [333] En el mismo sentido, HERRERA BRAVO. Reflexiones sobre los Delitos Informáticos motivadas por los desaciertos de la Ley Chilena. En Revista Electrónica de Derecho Informático. Para una mejor revisión en http://publicaciones.derecho.org/redi/No.05_Diciembre_de_1998/herrera. Fecha de acceso: 11 de marzo del año 2001.
- [334] HUERTA MIRANDA, Marcelo. Chile: Figuras delictivo-informáticos tipificadas en Chile. Revista Electrónica de Derecho Informático. http://publicaciones.derecho.org/redi/No.20_marzo_del_2000/14. Fecha de acceso: 11 de marzo del año 2001.
- [335] *Ibídem.*
- [336] HERRERA BRAVO. Reflexiones sobre los Delitos Informáticos motivadas por los desaciertos de la Ley Chilena. En Revista Electrónica de Derecho Informático. Para más información en http://publicaciones.derecho.org/redi/No.05_Diciembre_de_1998/herrera. Fecha de acceso: 11 de marzo del año 2001.
- [337] En igual sentido, JIJENA LEIVA, Renato. *Op. Cit.* Pp. 30.
- [338] JIJENA LEIVA, Renato. *Op. Cit.* Pp. 33.