Felipe Villavicencio Terreros(*)

Delitos Informáticos(**)(***)(****)

Cybercrimes

(...) EN ESTE TIPO DE DELITOS NO SE PUEDE ESTABLECER A LA INFORMACIÓN COMO EL ÚNICO BIEN JURÍDICO AFECTADO, POR SER EL PRINCIPAL Y EL MÁS IMPORTANTE; SINO A UN CONJUNTO DE BIENES QUE SON AFECTADOS, DEBIDO A LA CARACTERÍSTICA DE LA CONDUCTA TÍPICA EN ESTA MODALIDAD DELICTIVA QUE COLISIONA CON DIVERSOS INTERESES COLECTIVOS.

Resumen: En los últimos tiempos, producto del desarrollo de las tecnologías informáticas se ha ido desarrollando una nueva forma de criminalidad denominada *delitos informativos*. En relación a esta nueva forma delictiva, se ha emitido una Ley penal especial cuya finalidad es prevenir y sancionar las conductas ilícitas que afectan los sistemas y datos informáticos, así como el secreto de las comunicaciones, y los demás bienes jurídicos que resulten afectados con esta modalidad delictiva, como son el patrimonio, la fe pública y la libertad sexual.

Palabras Clave: Cibereducación - Ciberdelincuente - *Hackers* - *Crackers* - Sabotaje Informático - Gusanos - *Malware* - *Browser* - *Cookie* - *Dialup*

Abstract: In recent times, due to the development of information technology, a new form of crime called *informational crimes* has developed. In relation to this new type of crime, a special criminal law was issued, whose purpose is to prevent and punish illegal activities that affect computer systems and datas, secret communications, and other legal goods that are affected with this type of crime, such as equity, public faith and sexual freedom.

Keywords: Cybereducation - Cybercriminal - Hackers - Crackers - Informatics Sabotage - Worms - Malware - Browser - Cookie - Dialup

---

(*) Abogado por la Universidad Nacional Mayor de San Marcos. Doctor por la Universidad de Buenos Aires. Profesor de Derecho Penal en la Pontificia Universidad Católica del Perú y en la Universidad San Martín de Porres. Docente de Derecho Penal de la Maestría en Ciencias Penales de la Universidad Nacional Mayor de San Marcos. Experto en Derecho Penal. Socio del Estudio Villavicencio, Meza & Rivera.

(**) La Ley 30096 *Ley de delitos informativos*, fue promulgada el 21 y publicado el 22 de octubre del 2013 en El Peruano. Luego se promulgo la Ley 30171 *Ley que modifica la Ley 30096, Ley de delitos informativos*, promulgada el 9 y publicado el 10 de marzo del 2014 en *El Peruano*.

(***) Este trabajo ha sido posible con la colaboración de mi alumno Vilmer de la Cruz Paulino.

(****) Nota del Editor: el presente artículo fue recibido el 1 de febrero de 2015 y aprobada su publicación el 15 de febrero del mismo año.

1. Consideraciones Generales

1.1. Introducción

El proceso de integración cultural, económica y social a nivel mundial viene acompañado del gran desarrollo de la tecnología de la información y comunicación (en adelante TIC), y la masificación de la misma aparece jugando un papel importante en el desarrollo cultural de la sociedad. Las nuevas herramientas que ponen las TIC al servicio del hombre están relacionadas con la transmisión, procesamiento y almacenamiento digitalizado de información, así como un conjunto de procesos y productos que simplifican la comunicación, y hacen más viables la interacción entre las personas. Un invento tecnológico que reforzó el poder de las TIC es, sin lugar a dudas el internet (por ejemplo, a través del desarrollo de *messenger*, correo electrónico, *facebook*, *twitter*, *web*, etcétera). Este nuevo descubrimiento superó el paradigma real del tiempo-espacio en la interacción humana, en tanto la comunicación se podía dar en tiempo real sin importar la distancia. Por otra parte, las aplicaciones de las TIC a partir de internet (entre ellas *cibergobierno*, *cibereducación* y *cibersalud*) se consideran habilitantes para el desarrollo social, puesto que proporcionan un canal eficaz para distribuir una amplia gama de servicios básicos en zonas remotas y rurales, pues estas aplicaciones facilitan el logro de los objetivos de desarrollo prospectivo, mejoras en las condiciones sanitarias y medioambientales.

Si bien los diversos ámbitos de interacción se ven favorecidos por la fluidez que le brinda esta nueva alternativa tecnológica, no obstante, crecen los riesgos relacionados al uso de las tecnologías informáticas y de comunicación[(1)]. El desarrollo de la tecnología también ha traído consigo nuevas formas delictuales que tienen por medio y/o finalidad los sistemas informáticos e internet.

Las principales características de vulnerabilidad que presenta el mundo informático son las siguientes:

a) La falta de jerarquía en la red, que permite establecer sistemas de control, lo que dificulta la verificación de la información que circula por este medio.

b) El creciente número de usuarios, y la facilidad de acceso al medio tecnológico.

c) El anonimato de los cibernautas que dificulta su persecución tras la comisión de un delito a través de este medio.

d) La facilidad de acceso a la información para alterar datos, destruir sistemas informáticos.

Otro factor determinante es la rápida difusión de información a través de este medio tecnológico a muy bajo costo que permite a las organizaciones delictivas perpetrar delitos con mayor facilidad[(2)].

Es necesario mencionar que el hecho de criminalizar algunas conductas desplegadas en el mundo informático no implica desconocer las ventajas y facilidades brindadas por estos sistemas. Son evidentes los beneficios de los adelantos tecnológicos que trae para la sociedad el uso de la tecnología informática y comunicación. Sin embargo, conforme al informe del doceavo Congreso de las Naciones Unidas sobre Prevención del Delito y Justicia Penal[(3)], estos adelantos tecnológicos posibilitan una nueva modalidad de cometer los delitos tradicionales como el fraude y la distribución de pornografía infantil, y a su vez facilita la comisión de nuevos delitos como la penetración en redes informáticas, el envío de correo basura, la pesca de los datos *pishing*, la piratería digital, la propagación maliciosa de virus y otros ataques contra las infraestructuras de información esenciales.

(1) AROCENA, Gustavo. *La regulación de los delitos informativos en el Código Penal argentino. Introducción a la ley nacional 26388*. En: *Boletín Mexicano de Derecho Comparado, nueva serie*. Año XLV. No. 135. México, 2012; pp. 945-988.

(2) *Véase:* CARNEVALI RODRÍGUEZ, Raúl. *La criminalidad organizada. Una aproximación al derecho penal italiano, en particular la responsabilidad de las personas jurídicas y la confiscación*. En: *Ius Et Praxis*. No. 2. Volumen 16. Talca, 2010; p. 273.

(3) *Véase: Informe del 12vo. Congreso de las Naciones Unidas sobre Prevención del Delito y Justicia Penal*; p. 61.

Desde el ángulo del derecho penal internacional, el impacto de la sociedad de la información es triple: "primero, la sociedad de la información genera una amenaza transnacional para ciertos bienes jurídicos, si bien otros quedan sin resultar afectados por ella. En segundo lugar, la sociedad de la información crea, por otra parte, una herramienta para la justicia penal. El tercer impacto de importancia tiene que ver con la pérdida de soberanía. La sociedad de la información ha hecho disminuir gravemente (y hasta eliminado) el valor e importancia de la territorialidad. Como la localización es difícil, imposible o en desplazamiento permanente, esta es la cuestión clave del ciberespacio. En todos los espacios el ciberespacio no presenta suficiente permanencia para permitir a los Estados reclamar por su soberanía sobre todo lo que sucede"(4).

Antes de empezar a analizar la Ley de Delitos Informáticos es necesario mencionar que esta ley tiene como fuente directa la COMJIB (Bases para la elaboración de un instrumento internacional en materia de cibercriminalidad)(5) y el Convenio sobre la ciberdelincuencia de Budapest.

1.2. Los delitos informáticos: concepto y modalidades

Los delitos informáticos(6) se vinculan con la idea de la comisión del crimen a través del empleo de la computadora, internet, etcétera; sin embargo, esta forma de criminalidad no solo se comete a través de estos medios, pues éstos solo son instrumentos que facilitan pero no determinan la comisión de estos delitos. Esta denominación es poco usada en las legislaciones penales; no obstante, bajo ella se describe una nueva forma de criminalidad desarrollada a partir del elevado uso de la tecnología informática(7).

Para Mühlen el delito informático ha de comprender todo comportamiento delictivo en el que la computadora es el instrumento o el objetivo del hecho(8). En similar sentido, Dannecker concibe el delito informativo como aquella forma de criminalidad que se encuentra directa o indirectamente en relación con el procesamiento electrónico de datos y se comete con la presencia de un equipo de procesamiento electrónico de datos.

Por nuestra parte, entendemos a la criminalidad informática como aquellas conductas dirigidas a burlar los sistemas de dispositivos de seguridad, esto es, invasiones a computadoras, correos o sistemas de datas mediante una clave de acceso; conductas típicas que únicamente pueden ser cometidas a través de la tecnología. En un sentido amplio, comprende a todas aquellas conductas en las que las TIC son el objetivo, el medio o el lugar de ejecución, aunque afecten a bienes jurídicos diversos; y que plantea problemas criminológicos y penales, originados por las características propias del lugar de comisión(9).

De la concepción de los delitos informáticos, se entiende que no todo delito puede ser clasificado como delito informático por el solo hecho de haber empleado la computadora u otro instrumento tecnológico. Es necesario

(4) KLIP, André. *Sociedad de la Información y derecho penal*. Relación general en: *Revista Internacional de Derecho Penal*, *Asociación Internacional de Derecho Penal AIDP*. Francia, 2014; p. 479.

(5) COMJIB. *Conferencia de Ministros de Justicia de los Países Iberoamericanos*.

(6) Debido al desarrollo de la tecnología, entre ellas la computadora, y dado la nueva forma de comisión de delitos a través de las tecnologías es que se ha optado por denominar indistintamente a este tipo de delitos como *delitos de abuso de computadoras*, *delitos bajo la influencia de la computadora, criminalidad de la información y la comunicación*, *criminalidad de internet*, *criminalidad multimedia*. En el Perú se los denomina *delitos informáticos*. Todas estas denominaciones identifican de manera general la problemática de la delincuencia mediante las computadoras y el empleo de las comunicaciones; sin embargo, para efectos didácticos en la doctrina se prefiere la denominación de *delitos informáticos* para identificar la criminalidad vinculada a la tecnología. *Véase*: MAZUELOS COELLO, Julio. *Modelos de imputación en el derecho penal informático*; p. 40.

(7) MAZUELOS COELLO, Julio. *Óp. cit.*; p. 40.

(8) MÜHLEN, citado por MAZUELOS COELLO, Julio. *Modelos de imputación en el derecho penal informático*. *Óp. cit.*; p. 41.

(9) MIRÓ LINARES, Francisco. *El cibercrimen. fenomenología y criminología de la delincuencia en el ciberespacio*, Madrid: Marcial Pons, 2012; p. 44.

determinar que conductas pueden ser clasificadas como delitos informáticos y cuales no, a pesar de su vinculación con una computadora, un procesador de datos o la red de información. Al respecto, uno de los criterios a utilizar seria que un delito, para ser clasificado dentro de los delitos informáticos, no sea posible de realizarse sin la intervención de la informática, porque es el medio informático lo que va caracterizar este delito[10]; por ejemplo el difamar a una persona a través de los medios de comunicación (sea por correo electrónico, *facebook* o twitter), no puede constituirse como un delito informático por el solo hecho de emplear la tecnología informática como medio, pues este delito puede realizarse a través de otros medios como son verbal, escrito, etcétera. Sin embargo, los delitos de ingresar sin autorización a un sistema de datos o sabotear una base de datos sí se clasifican dentro de los delitos informativos, porque no es posible la comisión de estos delitos sin la intervención de la informática.

Respecto de los delitos informativos, Krutisch, identifica tres tipos de categorías: manipulación informática, sabotaje informático y acceso no autorizado a datos o sistema computarizados[11] pero no son categorías de delitos, sino modos de cometer los delitos informativos.

1.3. Antecedentes de los delitos informáticos

El delito informático en un inicio se encontraba tipificado en el artículo 186, inciso 3, segundo párrafo del Código Penal de 1991. Esta regulación no era propia de un delito autónomo, sino como una agravante del delito de hurto[12] En la actualidad, los delitos informáticos están previstos en el Capítulo X[13] del Código Penal: los artículos 207-A (interferencia, acceso o copia ilícita contenida en base de datos), 207-B (alteración, daño o destrucción de base de datos), 207-C (circunstancias cualificantes agravantes), 207-D (tráfico ilegal de datos), y en las leyes penales especiales.

Entre estas leyes penales especiales, se encuentra la Ley 30096[14] (*Ley de Delitos Informáticos*). Esta Ley de Delitos Informáticos está conformada por siete capítulos que se estructuran de la siguiente manera: finalidad y objeto de la ley (Capítulo I), delitos contra datos y sistemas informáticos (Capítulo II), delitos informáticos contra la indemnidad y libertad sexual (Capítulo III), delitos informáticos contra la intimidad y el secreto de las comunicaciones (Capítulo IV), delitos informáticos contra el patrimonio (Capítulo V), delitos informáticos contra la fe pública (Capítulo VI) y las disposiciones comunes (Capítulo VII).

Posteriormente se promulgó la Ley 30171[15] (*Ley que modifica la Ley 30096, Ley de Delitos Informáticos*). La finalidad de esta ley fue adecuar la Ley 30096 a los estándares legales del convenio sobre la *cibercriminalidad* (en adelante Convenio de Budapest), al incorporar en la redacción típica de los artículos 2, 3, 4, 7, 8 y 10 de la referida Ley la posibilidad de cometer el delito deliberada e ilegítimamente. Las modificaciones de la Ley 30171, con respecto a los delitos informáticos, son las siguientes:

- Artículo 1; Modificación de los artículos 2, 3, 4, 5, 7, 8 y 10 de la Ley 30096 *Ley de Delitos Informáticos*.

- Artículo 2; Modificación de la tercera, cuarta y undécima disposiciones complementarias finales de la Ley 30096 *Ley de Delitos Informáticos*.

(10) *Véase* MAZUELOS COELLO, Julio. *Delitos informativos: una aproximación a la regulación del Código Penal peruano*. En: *RPDJP*. No. 2. Lima, 2001; p. 253 y siguientes.
(11) KRUTISCH citado por MAZUELOS COELLO, Julio. *Óp. cit*.; p. 40.
(12) BRAMONT- ARIAS TORRES, Luis. *Delitos informáticos*. En: *Revista Peruana de Derecho de la Empresa, Derecho informático Y Teleinformática Jurídica*. No. 51. Lima: Asesor Andina, 2000.
(13) Capitulo incorporado por la Ley 27309, publicado el 17/07/2000.
(14) Publicado el 22 octubre 2013. Esta ley tiene su origen en el Proyecto de Ley No. 34/ 2011- CR, presentado al congreso el 11 de agosto del 2011.
(15) Publicado el 10 de marzo 2014. Esta Ley tiene su origen en el Proyecto de Ley No. 2991/ 2013- CR, presentado al congreso el 25 de noviembre del 2011.

- Artículo 3; Incorporación del artículo 12 a la Ley 30096 *Ley de Delitos Informáticos*.

- Artículo 4; Modificación de los artículos 158, 162 y 323 del Código Penal.

- Artículo 5; Incorporación de los artículos 154-A y 183-B del Código Penal.

- Única Disposición Complementaria Derogatoria; Deroga el artículo 6 de la Ley 30096 *Ley de Delitos Informáticos*.

1.4. Finalidad y objeto de la ley

El artículo 1 de la *Ley de delitos informáticos* establece que la finalidad de la ley es prevenir y sancionar las conductas ilícitas que afectan los sistemas, las datas informáticos, el secreto de las comunicaciones; y otros bienes jurídicos de relevancia penal (como el patrimonio, la fe pública, la libertad sexual, etcétera) que puedan ser afectados mediante la utilización de las TIC, con la finalidad de garantizar las condiciones mínimas para que las personas gocen del derecho a la libertad y al desarrollo. Con esta ley se intenta garantizar la lucha eficaz contra la ciberdelincuencia.

Esta Ley no responde solo a la necesidad de ejercer la función punitiva del Estado enfocada en la protección de la información; sino que tiene como principal objetivo la estandarización de la ley penal peruana con el ordenamiento penal internacional, principalmente por la Convenio contra la *cibercriminalidad* del Consejo Europeo (CETS 185), denominado Convenio de Budapest[16].

1.5. Bien jurídico tutelado

El bien jurídico tutelado en los delitos informáticos se concibe en los planos de manera conjunta y concatenada; en el primero se encuentra la *información* de manera general (información almacenada, tratada y transmitida mediante los sistemas de tratamiento automatizado de datos), y en el segundo plano, los demás bienes afectados a través de este tipo de delitos como son la indemnidad sexual, intimidad, etcétera. Respecto de la información deber ser entendido como el contenido de las bases y/o banco de datos o el producto de los procesos informáticos automatizados; por lo tanto se constituye en un bien autónomo de valor económico. Y es la importancia del *valor económico* de la información lo que ha hecho que se incorpore como bien jurídico tutelado[17].

Sin embargo, creemos que la información se debe considerar de diferentes formas, y no solo como un valor económico, sino como un valor intrínseco de la persona por la fluidez y el trafico jurídico, y por los sistemas que lo procesan o automatizan, los mismos que se equiparan a los bienes protegidos tradicionalmente, tales como el patrimonio (fraude informático), la reserva, la intimidad y confidencialidad de los datos (agresiones informáticas a la esfera de la intimidad), la seguridad o fiabilidad del trafico jurídico probatorio (falsificación de datos o documentos probatorios), etcétera.

Por tanto, en este tipo de delitos no se puede establecer a la información como el único bien jurídico afectado, por ser el principal y el más importante; sino a un conjunto de bienes que son afectados[18], debido a la característica de la conducta típica en esta modalidad delictiva que colisiona con diversos intereses colectivos. En es ese sentido que coincidimos

(16) *Véase* Ley 30096, *Ley de delitos informáticos*, octava disposición complementaria: "El Estado peruano promoverá la firma y ratificación de convenios multilaterales que garanticen la cooperación mutua con otros Estados para la persecución de los delitos informáticos".

(17) Cfr. GUTIERREZ FRANCÉS, María Luz. *Atentados contra la información como valor económico de empresa*. MAZUELOS COELLO y REYNA ALFARO. *Delitos informáticos*. DURAND VALLADARES. *Los delitos informáticos en el Código Penal Peruano*. URQUIZO OLAECHEA. *Revista Peruana de Ciencias Penales*. No. 11. Lima, 2002.

(18) GONZÁLES DE CHAVES CALAMITA, María. *El llamado ´delito informático´*. En: *Anales de la Facultad de Derecho de la Universidad de la Laguna*. No. 21. España, 2004; pp. 44-65.

con María Luz Gutiérrez Francés, quien señala que es un delito pluriofensivo[19], sin perjuicio de que uno de tales bienes este independientemente tutelado por otro tipo penal[20].

1.6. Perfil del ciberdelincuente

El perfil del ciberdelincuente (*sujeto activo*) en esta modalidad delictual requiere que este posea ciertas habilidades y conocimientos detallados en el manejo del sistema informático[21]. Es en razón a esas cualidades que se les ha calificado a los sujetos activos como delincuentes de *cuello blanco*[22], que tienen como características:

a) Poseer importantes conocimientos informáticos.

b) Ocupar lugares estratégicos en su centro laboral, en los que se maneja información de carácter sensible (se denominan delitos ocupacionales, ya que se comenten por la ocupación que se tiene y el acceso al sistema).

Para Marcelo Manson, los infractores de la ley penal en materia de delitos informáticos no son delincuentes comunes y corrientes, sino que por el contrario, son personas especializadas en la materia informática[23]. Agrega que "las personas que cometen los delitos informáticos son aquellas que poseen ciertas características que no presentan el denominador común, esto es, habilidades para el manejo de los sistemas informáticos y que por su situación laboran en puestos estratégicos donde se maneja información sensible".

Camacho Losa considera que el perfil de estas personas no coincide con el de un delincuente marginal, y caracteriza a los autores de estas infracciones como empleados de confianza de las empresas afectadas[24].

Vives Antón y Gonzales Cussac afirman que "sujeto activo puede ser tanto las personas legítimamente autorizadas para acceder y operar el sistema (operadores, programadores u otros), como terceros no autorizados que acceden a las terminales públicas o privadas"[25].

Gutiérrez Francés y Ruiz Vadillo difieren de estos puntos de vista y sostienen que "el autor del delito informático puede serlo cualquiera, no precisando el mismo de determinados requisitos personales o conocimientos técnicos cualificados"[26]. Por nuestra parte, si bien consideramos que el sujeto activo puede ser cualquier persona (con conocimientos y habilidades en informática), compartimos parcialmente la postura de que el sujeto activo debe ocupar un puesto laboral que le permita acceder a información sensible. Sin embargo, no están excluidos los sujetos que sin ocupar algún cargo estratégico pueden ser sujeto activo por sus habilidades y conocimientos sobre la informática. Por ende, se trata de delitos de dominio.

A estos tipos de sujetos se les denomina de diferente manera dependiendo el modo como actúan y que conductas son las que realizan:

(19) GUTIERREZ FRANCES, María. *Fraude Informático y estafa*. En: *Centro de Publicaciones del Ministerio de Justicia*. Madrid, 1991.
(20) Por la ubicación sistemática de estos delitos dentro del Código Penal de 1991 y antes de la dación de la Ley penal especial 30096, el bien jurídico considerado era el patrimonio *por las conductas dirigidas a dañar, alterar o destruir una base de datos*. *Véase* GALVEZ VILLEGAS, Tomas y Walter DELGADO TOVAR. *Derecho Penal Parte Especial*. Tomo III. Lima: Jurista Editores, 2002; p.1207.
(21) AZAOLA CALDERON, Luis. *Delitos informáticos y Derecho penal*. México: UBIJUS, 2010; p. 27.
(22) "Se le denomina así a la delincuencia informática debido a los estudios sobre criminalidad informática orientados en las manifestaciones en el ámbito económico patrimonial, donde la doctrina determino que el sujeto activo del delito informático poseída un alto nivel socioeconómico". AZAOLA CALDERON, Luis. *Delitos informáticos y Derecho penal*. *Óp. cit.*; pp. 27 y 28.
(23) MANSON, Marcelo. *Legislación sobre delitos informáticos*. Referencia de 27 de diciembre del 2013. Disponible en web: https://dl.dropbox.com/u//dl. legislacioncomparada.pdf.
(24) CAMACHO LOSA, Luis. *El delito informático*. Madrid: Gráficas Cóndor, 1987; pp. 83- 84.
(25) VIVES ANTÓN, Tomás y José Luis GONZÁLES CUSSAC. *Comentarios al código Penal 1995*. Valencia: Tiront Blanch, 1996; p. 1238.
(26) GUTIERRES FRANCES, María. *Fraude informático y estafa*. RUIZ VADILLO, Enrique. *Tratamiento a la delincuencia informática*. En AZAOLA CALDERON, Luis. *Delitos informáticos y Derecho penal*. *Óp. cit*.; p. 29.

a) *Hackers*; Son personas dedicadas, por afición u otro interés, a violar programas y sistemas supuestamente impenetrables. Conocido como *delincuente silencioso o tecnológico*. Les gusta indagar por todas partes y conocer el funcionamiento de los sistemas informáticos. Son personas que realizan esta actividad como reto intelectual, sin producir daño alguno con la única finalidad de descifrar y conocer los sistemas informáticos.

   Para Sieber los *hacker* son "personas que acceden sin autorización a un sistema de proceso de datos a través de un proceso de datos a distancia, no cometido con finalidades manipuladoras, fraudulentas, de espionaje, ni sabotaje, sino sencillamente como paseo por placer no autorizado"(27). Morón Lerma define a los *hacker* como "personas que acceden o interfieren sin autorización, de forma subrepticia, a un sistema informático o redes de comunicación electrónica de datos y utilizan los mismos sin autorización o más allá de lo autorizado"(28).

b) *Crackers*; Son personas que se introducen en sistemas remotos con la intención de destruir datos, denegar el servicio a usuarios legítimos y, en general, a causar problemas a los sistemas, procesadores o redes informáticas, conocidos como *piratas electrónicos*.

   La característica que los diferencia de los *hacker* es que los *crackers* usan programas ya creados que pueden adquirir, normalmente vía internet; mientras que los *hackers* crean sus propios programas, tienen mucho conocimiento sobre los programas y conocen muy bien los lenguajes informáticos(29).

   Por otra parte, Morant Vidal define a estos sujetos como "personas que se introducen en sistemas remotos con la intención de destruir datos, denegar el servicio a usuarios legítimos, y en general a causar problemas"(30).

   Alfonso Laso sostiene que el *cracker* "es la persona que, de manera intencionada, se dedica a eliminar o borrar ficheros, a romper los sistemas informáticos, a introducir virus, etcétera"(31).

1.7. La situación de las personas jurídicas como sujeto activo y sujeto pasivo

1.7.1. Sujeto Activo

A nivel internacional, existe una gran división entre los Estados que aceptan la responsabilidad penal de las personas jurídicas de los que no la aceptan. Sin embargo, "los regímenes divergentes sobre la responsabilidad penal de las personas jurídicas pueden causar problemas para las empresas internacionales con sucursales en más de un Estado"(32).

En el caso peruano, dada la vigencia del principio s*ocietas delinquere non potest*, no se puede considerar a la persona jurídica como sujeto activo. Sin embargo, en el Derecho Penal peruano se cuentan con las figuras de las Consecuencias Accesorias (artículo 105

(27) SIEBER, Ulrich. *Criminalidad informática: peligro y prevención*; p. 77. MIR PUIG, Santiago. *Delincuencia informática*.
(28) MORON LERMA, Esther. *Internet y Derecho Penal: hacking y otras conductas ilícitas en la red*. 2da edición. Navarra: Aranzadi; p. 51.
(29) AZAOLA CALDERON, Luis. *Óp. cit.*; p. 32.
(30) MORANT VIDAL, Jesús. *Protección penal de la intimidad frente a las nuevas tecnologías*. Valencia: Práctica de Derecho, 2002; p. 44.
(31) DE ALFONSO LASO, Daniel. *El hackerin blanco. Una conducta ¿punible o impune?* En *Internet y derecho penal, Cuadernos de Derecho Judicial, Consejo General del poder Judicial*. Madrid, 2001; pp.110-111.
(32) "En el contexto de las dificultades (…) en lo que respecta a las investigaciones y la ejecución, es recomendable crear la responsabilidad de las personas jurídicas que operan en un entorno transnacional". KLIP, André. *Sociedad de la Información y derecho penal*. Relación general en: *Revista Internacional de Derecho Penal, Asociación Internacional de Derecho Penal AIDP*. Francia, 2014; p. 449.

del Código Penal), del actuar por otro (artículo 27 del Código Penal) y las reglas procesales en el Código Procesal Penal del 2004, cuando se trata de delitos cometidos a través de las personas jurídicas; además del Acuerdo Plenario 7-2009/CJ-116 (*Personas jurídicas y consecuencias accesorias*).

Sin embargo, la ley de delitos informáticos regula dos supuestos de carácter administrativos donde la persona jurídica se niega a brindar información sobre el levantamiento del secreto bancario (decima disposición complementaria final) y cuando se niega a brindar información referente a los registros de comunicaciones telefónicas (Undécima disposición complementaria final), cuando así lo solicite a través de una orden judicial; a consecuencia de esto la SBS y OPSITEL respectivamente les aplicaran una sanción administrativa consistente en una multa.

1.7.2. Sujeto Pasivo
La persona jurídica sí puede ser considerada como sujeto pasivo, como por ejemplo, empresas públicas y privadas (bancos, instituciones públicas, industrias, seguros, etcétera), aunque en ciertos casos, estas personas jurídicas no denuncian los delitos de los que son víctimas por temor al desprestigio o al impacto entre sus clientes y consecuentes pérdidas económicas.

Además, esta ley menciona dos supuestos en donde la persona jurídica es sujeto pasivo de los delitos informáticos: (i) el artículo 6 (tráfico ilegal de datos, que consiste en crear, ingresar o utilizar indebidamente una base de datos sobre una persona natural o jurídica) y (ii) el artículo 9 (suplantación de identidad, él que mediante las TIC suplanta la identidad de una persona natural o jurídica).

Gutiérrez Francés señala que el sujeto pasivo por excelencia del ilícito informático es la persona jurídica(33), debido al tráfico económico en el que desarrollan sus actividades, por ello son los sectores más afectados por la criminalidad mediante computadoras. Y entre ellos están: la banca, las instituciones públicas, la industria de transformación, etcétera.

2. De los delitos informáticos en la ley 30096 y su modificación por la ley 30171

2.1. Delitos contra datos y sistemas informáticos (Capítulo II)

Este capítulo está conformado por las siguientes figuras penales: el artículo 2 (acceso ilícito), el artículo 3 (atentando a la integridad de datos informáticos) y el artículo 4 (atentando a la integridad de sistemas informáticos).

> "Artículo 2.-
> El que deliberada e ilegítimamente accede a todo o parte de un sistema informático, siempre que se realice con vulneración de medidas de seguridad establecidas para impedirlo, será reprimido con pena privativa de libertad no menor de uno ni mayor de cuatro años y con treinta a noventa días-multa.
> Será reprimido con la misma pena el que accede a un sistema informático excediendo lo autorizado"(34).

Esta figura penal de *acceso ilícito* sanciona la violación de la confidencialidad, que se realiza a través del acceso no autorizado al sistema, vulnerando las medidas de seguridad establecida para evitar que ajenos ingresen a un sistema informático(35); por el verbo rector *acceder* se entiende el hecho de entrar en un lugar o pasar a él, que en esta figura se entiende el acto de entrar sin autorización del titular a un sistema. El término *vulnerar* se entiende como "transgredir, quebrantar"(36), que se entiende

(33) GUTIÉRREZ FRANCÉS, María. *Fraude informático y estafa*. Madrid: Ministerio de Justicia, 1991; p. 76.
(34) Artículo 1 de la Ley 30171 que modifica el artículo 2 de la Ley 30096.
(35) *Diccionario de la Real Academia Española*. Referencia de 28 de marzo del 2014. Disponible en web: http://lema.rae.es/drae/?val=acceder.
(36) *Diccionario de la Real Academia Española*. Referencia de 28 de marzo del 2014. Disponible en web: http://lema.rae.es/drae/?val=vulnerar.

como el hecho de trasgredir las barreras de protección diseñados para el sistema[37].

Por la característica que presenta este tipo penal (*acceso ilícito*) se clasifica como un *delito de mera actividad*, porque esta figura exige el acto de acceder (*entrar en un lugar o pasar a él*) sin autorización a un sistema informático y vulnerar las medidas de seguridad. De esta manera se configura el ilícito. Por tanto el delito queda consumado en el momento que se vulnera las medidas de seguridad establecida para impedir el acceso ilícito, y para ellos es necesario que se realice esta conducta con dolo. Por ejemplo, el acceso a la cuenta de correo electrónico ajeno protegido mediante una contraseña de seguridad o el acceso no autorizado al sistema informático de una entidad aprovechando las debilidades inadvertidas por la programación.

La fuente legal de este artículo es el Convenio de Budapest, porque cumple con describir la acción delictiva en los mismos términos estandarizados de la norma internacional. Por mencionar los términos *deliberación* y *falta de legitimación*[38] de la acción contenida en el texto del Convenio de Budapest guarda cierta identidad con el dolo (conocimiento y voluntad)[39].

> "Artículo 3.-
> El que deliberada e ilegítimamente daña, introduce, borra, deteriora, altera, suprime o hace inaccesible datos informáticos, será reprimido con pena privativa de libertad no menor de tres ni mayor de seis años y con ochenta a ciento veinte días multa"[40].

Esta figura penal sanciona la conducta de dañar (causar detrimento, perjuicio, menoscabo)[41], introducir (entrar en un lugar)[42], borrar (desvanecer, quitar, hacer que desaparezca algo)[43], deteriorar (empeorar, degenerar)[44], alterar (estropear, dañar, descomponer)[45], suprimir (hacer cesar, hacer desaparecer)[46] y hacer inaccesible los datos informáticos a través de la utilización de las TIC. Por la característica que presenta este tipo penal (*atentado a la integridad de los datos informáticos*) es clasificado como un delito de mera actividad, porque esta figura exige el solo cumplimiento del tipo penal, la sola realización de la conducta de *introducir*, *borrar*, *deteriorar*, *alterar*, *suprimir* y *hacer inaccesible* los datos informáticos para que se pueda configurar el ilícito, sin importar el resultado posterior. Por tanto el delito queda consumado al realizarse cualquiera de estos actos.

Este artículo en mención es compatible parcialmente con el artículo 4 del Convenio de Budapest[47] que sanciona el atentado contra la integridad y la disponibilidad del dato informático.

(37) STERN, Enrique. *El sentido de la privacidad, la intimidad y la seguridad en el mundo digital: ámbito y límites*. En: *Eguzkilore*. No. 21; p. 187.
(38) *Véase Convenio sobre la ciberdelincuencia – Budapest, 23.XI.2001*. Capítulo II. Sección 1º. Titulo 1º. Artículo 2º.- Acceso ilícito.
(39) VILLAVICENCIO TERREROS, Felipe. *Derecho Penal. Parte general*. Lima: Grijley, 2013; p. 354.
(40) Artículo 1 de la Ley 30171 que modifica el artículo 3 de la Ley 30096.
(41) *Diccionario de la Real Academia Española*. Referencia de 28 de marzo del 2014. Disponible en web: http://lema.rae.es/drae/?val=dañar.
(42) *Diccionario de la Real Academia Española*. Referencia de 28 de marzo del 2014. Disponible en web: http://lema.rae.es/drae/?val=introducir .
(43) *Diccionario de la Real Academia Española*. Referencia de 28 de marzo del 2014. Disponible en web: http://lema.rae.es/drae/?val=borrar.
(44) *Diccionario de la Real Academia Española*. Referencia de 28 de marzo del 2014. Disponible en web: http://lema.rae.es/drae/?val=deteriorar.
(45) *Diccionario de la Real Academia Española*. Referencia de 28 de marzo del 2014. Disponible en web: http://lema.rae.es/drae/?val=alterar.
(46) *Diccionario de la Real Academia Española*. Referencia de 28 de marzo del 2014. Disponible en web: http://lema.rae.es/drae/?val=suprimir.
(47) *Véase*: *Convenio sobre la ciberdelincuencia – Budapest, 23.XI.2001*. Capítulo II. Sección 1º. Titulo 1º. Artículo 4º.- Ataques a la integridad de los datos.

> "Artículo 4.-
> El que deliberada e ilegítimamente inutiliza, total o parcialmente, un sistema informático, impide el acceso a este, entorpece o imposibilita su funcionamiento o la prestación de sus servicios, será reprimido con pena privativa de la libertad no menor de tres ni mayor de seis años y con ochenta a ciento veinte días-multa"(48).

Está figura penal sanciona las conductas que están dirigidas a inutilizar (hacer inútil, vano o nulo algo)(49) total o parcialmente un sistema informático, entorpecer (retardar, dificultar)(50) e imposibilitar (quitar la posibilidad de ejecutar o conseguir algo)(51) su funcionamiento o la prestación de sus servicios utilizando las TIC. Por la característica que presenta este tipo penal (atentado contra la integridad de sistemas informáticos) se clasifica como un delito de resultado, porque para la configuración de este ilícito no basta con cumplir el tipo que es (inutilizar o perturbar), sino además es necesario que la acción vaya seguido de un resultado (impedir el acceso, imposibilitar su funcionamiento, o la prestación de sus servicios). Por tanto, el delito se consuma cuando se *impide el acceso*, se *imposibilita el funcionamiento*, etcétera; del sistema informático, caso contrario el hecho solo dará lugar a la tentativa.

Este artículo guarda cierta relación de compatibilidad con el artículo 5 del Convenio de Budapest(52), en tanto se puede entender la *obstaculización grave* de un sistema informático con el de la *inutilización total o parcial* del sistema.

Son ejemplos de esta figura penal los siguientes delitos:

a) Delito de daño; que es comportamiento consistente en dañar, destruir o inutilizar un bien, que en este caso es el sistema informático. Dice Bramont-Arias que el delito de daños existirá si usuarios, carentes de autorización, alteran o destruyen archivos o bancos de datos a propósito; la destrucción total de programas y de datos ponen en peligro la estabilidad económica de una empresa(53). El *modus operandi* se viene perfeccionando con el tiempo: virus, cáncer *rotudtine*. Estos actos deben causar un perjuicio patrimonial.

b) El sabotaje informático; que consiste básicamente en *borrar*, *suprimir* o *modificar* (alterar) sin autorización funciones o datos de las computadoras con intención de obstaculizar el funcionamiento normal del sistema, que se conoce comúnmente como *virus informático*(54).

Marchena Gómez señala que el "sabotaje informático es la conducta que consiste en la destrucción o en la producción generalizada de daños"(55). Morant Vidal señala que "el sabotaje informático se dirige a inutilizar los sistemas informáticos causando daños a los programas"(56).

---

(48) Artículo 1 de la Ley 30171 que modifica el artículo 4 de la Ley 30096.
(49) *Diccionario de la Real Academia Española*. Referencia de 28 de marzo del 2014. Disponible en web: http://lema.rae.es/drae/?val=inutilizar.
(50) *Diccionario de la Real Academia Española*. Referencia de 28 de marzo del 2014. Disponible en web: http://lema.rae.es/drae/?val=entorpecer.
(51) *Diccionario de la Real Academia Española*. Referencia de 28 de marzo del 2014. Disponible en web: http://lema.rae.es/drae/?val=imposibilitar.
(52) *Véase*: *Convenio sobre la ciberdelincuencia – Budapest, 23.XI.2001*. Capítulo II. Sección 1º. Titulo 1º. Artículo 5º.- Ataques a la integridad del sistema.
(53) BRAMONT-ARIAS, Luis. *Delitos informáticos*. En: *Revista Peruana de Derecho de la Empresa, Derecho Informático y Teleinformática Jurídica*. No. 51. Lima: Asesorandina, 2000.
(54) AZAOLA CALDERON, Luis. *Delitos informáticos y Derecho penal*. México: UBIJUS, 2010; p. 69.
(55) MARCHENA GOMEZ, Manuel. *El sabotaje informático: entre los delitos de daños y desordenes públicos*. En: *Internet y Derecho Penal, Cuadernos de Derecho Judicial*. Madrid, 2001; p. 356.
(56) MORANT VIDAL, Jesús. *Protección penal de la intimidad frente a las nuevas tecnologías*. Valencia: Práctica de Derecho, 2003; pp. 46- 47.

Las técnicas que permiten cometer sabotaje informático son las siguientes[57]:

b.1. Bomba lógica; que consiste en la introducción de un programa de un conjunto de instrucciones indebidas que van a actuar en determinada fecha, destruyendo datos del ordenador, distorsionando el funcionamiento del sistema o paralizando el mismo.

b.2. Rutinas de cáncer; que son distorsiones al funcionamiento del programa, la característica es el auto reproducción.

b.3. Gusanos; que se infiltran en los programas ya sea para modificar o destruir los datos, pero a diferencia de los virus estos no pueden regenerarse.

b.4. Virus informáticos y *Malware*; que son elementos informáticos que destruyen el uso de ciertos antivirus[58]. Por ejemplo borrar los antecedentes policiales, judiciales y penales de una persona; alterar la deuda real de un cliente en una entidad financiera; cambiar la clave secreta o eliminar la cuenta electrónica (correo, *twitter*, *Facebook*) para impedir al titular el acceso a su cuenta.

2.2. Delitos informáticos contra la indemnidad y libertad sexual (Capítulo III)

Este capítulo está conformado por el artículo 5 (proposición a niños, niñas y adolescentes con fines sexuales por medios tecnológicos), que sanciona la propuesta sexual (solicitar u obtener material pornográfico, llevar a cabo actividades sexuales) a niños, niñas y adolescentes utilizando los medios tecnológicos.

"Artículo 5.- El que a través de internet u otro medio análogo contacta con un menor de catorce años para solicitar u obtener de él material pornográfico, o para llevar a cabo actividades sexuales con él, será reprimido con pena privativa de libertad no menor de cuatro ni mayor de ocho años e inhabilitación conforme a los numerales 1, 2 y 4 del artículo 36 del Código Penal.

Cuando la víctima tiene entre catorce y menos de dieciocho años de edad y medie engaño, la pena será no menor de tres ni mayor de seis años e inhabilitación conforme a los numerales 1, 2 y 4 del artículo 36 del código Penal"[59].

Esta figura penal sanciona el contacto (establecer contacto o comunicación con alguien)[60] realizado con un menor de edad con fines a obtener material pornográfico o con el propósito de llevar a cabo actividades sexuales que involucren el quebrantamiento de la libertad sexual del menor (violación sexual o actos contra el pudor); en este artículo hay dos supuestos:

a) El primer supuesto es el *contacto* con un menor de catorce años para solicitar u obtener material pornográfico o para realizar actos sexuales, cuya pena es de 4 a 8 años de pena privativa de libertad e inhabilitación.

b) El segundo supuesto es el *contacto* con un menor que tiene entre catorce y dieciocho años para solicitar, obtener material pornográfico o para realizar actos sexuales, cuya pena es de 3 a 6 años de pena privativa de libertad e inhabilitación

Este tipo sanciona el acto de contactar que significa "establecer contacto o comunicación

(57) AZAOLA CALDERON, Luis. *Delitos informáticos y Derecho Penal*. México: UBIJUS, 2010; p. 70.
(58) MATA BARRANCO, Norberto y Leyre HERNÁNDEZ DÍAZ. *El delito de daños informativos: una tipificación defectuosa*. En: *Revista de Estudios Penales y Criminológicos*. Volumen XXIX. España, 2009; pp. 311- 362.
(59) Artículo 1 de la Ley 30171 que modifica el artículo 5 de la Ley 30096.
(60) *Diccionario de la Real Academia Española*. Referencia de 28 de marzo del 2014. Disponible en web: http://www.rae.es/recursos/diccionarios/drae.

con alguien"[61], y el término *para* es un elemento subjetivo que determina la intención del sujeto activo y es este elemento que convierte a la figura penal en un *tipo de tendencia interna trascendente* (*delitos de intención*)[62], porque este ilícito en su *parte interna* requiere de una intención especial, que no corresponde a la parte externa objetiva, que en este caso es obtener material pornográfico y/o tener actividades sexuales con el menor; por consiguiente este tipo legal queda consumado cuando se produce el resultado típico, no siendo necesario que el agente consiga realizar su especifica tendencia trascendente. Por estas características se clasifica a esta figura como un *delito de resultado cortado*, porque en este ilícito el agente persigue un resultado que está más allá del tipo y que ha de producirse por sí solo, sin su intervención y con posterioridad[63].

En esta figura penal el legislador adelanta las barreras de punibilidad al sancionar el solo hecho de contactar con el menor de edad, sin importar si logra su objetivo el que es obtener material pornográfico o llegar a obtener acceso sexual; sin embargo, este articulo tiene muchas falencias que podría violar el principio de legalidad, al no tener una redacción clara, y a consecuencia de ello se podría sancionar a personas que sólo contactan con un menor de edad sin tener la finalidad de obtener material pornográfico y otro similar porque el término *contactar* no está delimitado, por consiguiente se estaría sancionando el solo hecho de establecer un *contacto* o comunicación con un menor de edad.

a) Delitos contra la libertad sexual; que son acciones destinado a vulnerar tanto la indemnidad sexual como la libertad sexual del menor.

   Este delito se consuma con la sola proposición, a un menor de edad con fines sexuales, ya sea para obtener material pornográfico o para acceder sexualmente, esta conducta es sancionable porque afecta la indemnidad del menor y la libertad sexual y el medio utilizado para facilitar el contacto es la informática.

b) Pornografía Infantil; en esta conducta tipificada se nota la intención del legislador de proteger penalmente varios bienes jurídicos, cuya titularidad corresponde a menores de edad, cuales son los adecuados procesos de formación y socialización de unos y otros, y su intimidad[64].

Lo que busca sancionar con esta tipo penal es el acto de *ofrecer*, *vender*, *distribuir*, exhibir material pornográfico de menores de edad. Esta conducta está referida a un sujeto activo indiferenciado (*delito de dominio*), es de mencionar que esta modalidad es dolosa: el sujeto ha de conocer la naturaleza del material y ha de querer realizarlo, difundir o poseer con dichos fines siendo indiferente que lo haga con ánimo lubrico o de lucro.

2.3. Delitos informáticos contra la intimidad y el secreto de las comunicaciones (Capítulo IV)

Este capítulo está conformado por las siguientes figuras penales: el artículo 6 (Derogado por la ley 30171 *Ley que Modifica la Ley 30096, Ley de Delitos* Informáticos) [65] y el artículo 7 (*interceptación de datos informáticos*).

(61) *Diccionario de la Real Academia Española*. Referencia de 28 de marzo del 2014. Disponible en web: http://www.rae.es/recursos/diccionarios/drae.

(62) VILLAVICENCIO TERREROS, Felipe. *Derecho Penal. Parte General*. 1era edición. Lima: GRIJLEY, 2010; p. 375. Define a los *tipos de tendencia interna trascendente* como aquellos delitos "cuya parte interna requiere de una intención especial que consiste en la búsqueda de un resultado diferente al exigido típicamente y que, por ende, no es exigente para la consumación del delito, debiendo entenderse solo para efectos de llenar el tipo".

(63) VILLAVICENCIO TERREROS, Felipe. *Óp. cit.*; p. 375.

(64) ORTS BERENGUER, Enrique y Margarita ROIG TORRES. *Delitos informáticos y delitos comunes cometidos a través de la informática*. Valencia: Tirant lo Blanch, 2001; p. 129.

(65) El artículo 6 de la ley 30096, *Ley de Delitos Informáticos*; fue derogado por la *única disposición complementaria derogatoria* de la ley 30171, *Ley que modifica la Ley Nº 30096, Ley de Delitos Informáticos*.

"Artículo 6.- (derogado por la Única Disposición Derogatoria de la Ley 30171 *Ley que modifica la Ley 30096*)"

"Artículo 7.- El que deliberadamente e ilegítimamente intercepta datos informáticos en transmisiones no públicas, dirigidas a un sistema informático, originadas en un sistema informático o efectuadas dentro del mismo, incluidas las emisiones electromagnéticas provenientes de un sistema informático que transporta dichos datos informáticos, será reprimido con pena privativa de la libertad no menor de tres ni mayor de seis años.

La pena privativa de libertad será no menor de cinco ni mayor de ocho años cuando el delito recaiga sobre información clasificada como secreta, reservada o confidencial de conformidad con la Ley 27806, Ley de Transparencia y Acceso a la información Pública.

La pena privativa de libertad será no menor de ocho ni mayor de diez años cuando el delito comprometa la defensa, la seguridad o la soberanía nacionales.

Si el agente comete el delitos como integrante de una organización criminal, la pena se incrementa hasta en un tercio por encima del máximo legal previsto en los supuestos anteriores"[66].

La figura penal sanciona la conducta que deliberada e ilegítimamente intercepta (*interrumpe*, *obstruye*)[67] datos informáticos y las emisiones electromagnéticas que transportan estos datos en las transmisiones privadas. Este artículo contiene tres agravantes:

a) La primera agravante se aplica cuando la interceptación recaiga sobre *información* clasificada como *secreta*, *reservada* o *confidencia*l, de conformidad con la Ley 27806, Ley de Transparencia y Acceso a la información Pública, cuya penalidad oscila entre cinco a ocho años

b) La segunda agravante se aplica cuando la interceptación recaiga sobre *información* que compromete a la *defensa*, *seguridad* o *soberanía nacional*, cuya penalidad se encuentra entre ocho a diez años.

c) La tercera agravante consiste en la calidad del agente (*integrante de una organización criminal*) que comete delitos cuya penalidad se incrementa hasta en un tercio por encima del máximo legal previsto en los supuestos anteriores.

Este tipo penal (*interceptar datos informáticos*) es un delito de *peligro abstracto* y por ende, sólo basta con demostrar la interceptación de datos informáticos para que el delito quede consumado. Por ende, se trata de un *delito de mera actividad* porque basta con el solo hecho de interceptar datos informáticos para que se consuma el delito. Por ejemplo la interceptación de archivos que contengan información relacionada con una investigación reservada por ley o la interceptación de comunicaciones que contenga información sensible que puede ser utilizada por algún país en un contexto bélico.

2.4. Delitos informáticos contra el patrimonio (Capítulo V)

Este capítulo está integrado por el artículo 8 (*fraude informático*), que sanciona la acción de *diseñar*, *introducir*, *alterar*, *borrar*, *suprimir* y *clonar datos informáticos* en perjuicio de tercero.

"Artículo 8.-
El que deliberadamente e ilegítimamente procura para sí o para otro un provecho ilícito en perjuicio de tercero mediante el diseño, introducción, alteración, borrado, supresión; clonación de datos informáticos o cualquier interferencia o manipulación en el funcionamiento de un sistema informático, será reprimido con una pena privativa de libertad no menor de tres ni

(66) Artículo 1 de la Ley 30171 que modifica el artículo 7 de la Ley 30096.
(67) *Diccionario de la Real Academia Española*. Referencia de 28 de marzo del 2014. Disponible en web: http://lema.rae.es/drae/?val=interceptar.

> mayor de ocho años y con sesenta a ciento veinte días multa.
>
> La pena será privativa de libertad no menor de cinco ni mayor de diez años y de ochenta a ciento cuarenta días multa cuando se afecte el patrimonio del Estado destinado a fines asistenciales o a programas de apoyo social"[68].

Este tipo penal (*fraude informático*) sanciona diversas conductas. Entre ellas a diseñar (proyecto o plan)[69], introducir (entrar en un lugar)[70], alterar (estropear, dañar, descomponer) [71], borrar (desvanecer, quitar, hacer que desaparezca algo)[72], suprimir (hacer cesar, hacer desaparecer)[73], clonar (producir clones)[74] datos informáticos o cualquier interferencia, o manipular (operar con las manos o con cualquier instrumento) [75] el funcionamiento de un sistema informático procurando (conseguir o adquirir algo)[76] un beneficio para sí o para otro en perjuicio de tercero; y por la forma como esta estructura (a propósito de la mala redacción que genera mucha confusión al momento de interpretar la figura, y las conductas inadecuadas como "diseñar, introducir, alterar, borrar y suprimir" que no encajan en el delito de fraude informático; estas conductas son propios del delito de daño) se clasifica como un *delito de resultado* porque no basta cumplir con el tipo penal para que se consuma el delito de fraude informático, sino que además, es necesario que esa acción vaya seguida de un resultado separado de la misma conducta el que consiste en causar un perjuicio a tercero, de otro modo el delito quedaría en tentativa. Por ejemplo clonar tarjetas bancarias, el fraude informático que afecta los programas sociales JUNTOS o PENSIÓN 65, destinados a apoyo social.

Este artículo es compatible con el artículo 8 del Convenio de Budapest[77], porque ambos artículos sancionan el empleo indebido de datos informáticos y la manipulación del funcionamiento del sistema mismo.

2.5. Delitos informáticos contra la fe pública (Capítulo VI)

El artículo 9 de la ley (*suplantación de identidad*), sanciona la suplantación de identidad de una persona natural o jurídica, siempre que de esto resulte algún perjuicio.

> "Artículo 9.- El que, mediante las tecnologías de la información o de la comunicación suplanta la identidad de una persona natural o jurídica, siempre que de dicha conducta resulte algún perjuicio, será reprimido con pena privativa de libertad no menor de tres ni mayor de cinco años".

Este tipo penal sanciona el hecho se suplantar (ocupar con malas artes el lugar de alguien,

(68) Artículo 1 de la Ley 30171 que modifica el artículo 8 de la Ley 30096.
(69) *Diccionario de la Real Academia Española*. Referencia de 28 de marzo del 2014. Disponible en web: http://www.rae.es/recursos/diccionarios/drae.
(70) *Diccionario de la Real Academia Española*. Referencia de 28 de marzo del 2014. Disponible en web: http://www.rae.es/recursos/diccionarios/drae.
(71) *Diccionario de la Real Academia Española*. Referencia de 28 de marzo del 2014. Disponible en web: http://www.rae.es/recursos/diccionarios/drae.
(72) *Diccionario de la Real Academia Española*. Referencia de 28 de marzo del 2014. Disponible en web: http://www.rae.es/recursos/diccionarios/drae.
(73) *Diccionario de la Real Academia Española*. Referencia de 28 de marzo del 2014. Disponible en web: http://www.rae.es/recursos/diccionarios/drae.
(74) *Diccionario de la Real Academia Española*. Referencia de 28 de marzo del 2014. Disponible en web: http://www.rae.es/recursos/diccionarios/drae.
(75) *Diccionario de la Real Academia Española*. Referencia de 28 de marzo del 2014. Disponible en web: http://www.rae.es/recursos/diccionarios/drae.
(76) *Diccionario de la Real Academia Española*. Referencia de 28 de marzo del 2014. Disponible en web: http://www.rae.es/recursos/diccionarios/drae.
(77) *Véase Convenio sobre la ciberdelincuencia – Budapest, 23.XI.2001*. Capítulo II. Sección 1º. Titulo 2º. Artículo 8º.- fraude informático.

defraudándole el derecho, empleo o favor que disfrutaba)[78] la identidad de una persona natural o jurídica causando algún perjuicio.

Esta figura penal (*suplantación de identidad*) se clasifica como un delito de resultado porque no basta con realizar la conducta típica el cual es *suplantar* la identidad, sino que además es necesario que esa acción vaya seguida de un resultado separado de la misma conducta el cual es causar un perjuicio. Por ejemplo. crear perfiles falsos en las redes sociales (correo electrónico, *Facebook*, *twitter*) atribuidos a personas naturales y/o jurídicas para engañar y perjudicar a terceros[79].

2.6. Disposiciones comunes (Capítulo VII)

Este capítulo está integrado por las siguientes figuras penales: el artículo 10 (abuso de mecanismos y dispositivos informáticos) y el artículo 11 (agravantes).

> "Artículo 10.- El que deliberadamente e ilegítimamente fabrica, diseña, desarrolla, vende, facilita, distribuye, importa u obtiene para su utilización, uno o más mecanismos, programas informáticos dispositivos, contraseñas, códigos de acceso o cualquier otro dato informático, específicamente diseñados para la comisión de los delitos previstos en la presente ley, o el que ofrece o presta servicio que contribuya a ese propósito, será reprimido con pena privativa de libertad no menor de uno ni mayor de cuatro años y con treinta a noventa días-multa"[80].

Este tipo penal sanciona diversas conductas, entre ellas fabricar (producir objetos en serie, generalmente por medios mecánicos) [81], diseñar (hacer un diseño)[82], desarrollar, vender (traspasar a alguien por el precio convenido la propiedad de lo que uno posee) [83], facilitar (proporcionar o entregar)[84], distribuir (entregar una mercancía a los vendedores y consumidores)[85], importa (dicho de una mercancía: valer o llegar a cierta cantidad)[86] y obtener (alcanzar, conseguir y lograr algo que se merece, solicita o pretende), para la utilización de mecanismos, programas informáticos, contraseñas, etcétera; diseñados específicamente para la comisión de los delitos previstos en esta ley. Este artículo es una expresión del adelantamiento de las barreras punitivas, porque se sanciona la participación y más aún el sólo hecho de ofrecer un servicio que facilite la comisión de algún delito previsto en la presente ley.

Este tipo penal (*abuso de mecanismos y dispositivos informáticos*) se clasifica como un *delito de mera actividad*, porque la figura exige cumplir con la conducta descrita en el tipo penal para la consumación del delito sin

(78) *Diccionario de la Real Academia Española*. Referencia de 28 de marzo del 2014. Disponible en web: http://lema.rae.es/drae/?val=suplantar.

(79) "Una abogada había sido suplantada en el *Facebook* y correo electrónico, por la pareja de su amiga, fingiendo ser lesbiana, para captar personas y ganarse la confianza a través del falso perfil y poder obtener materiales (fotos intimas) que luego eran utilizados para extorsionar a sus víctimas que ingenuamente creyeron estar en contacto con la persona suplantada, este acto trajo perjuicios económicos, laborales, familiares y psicológicos a la suplantada". CUARTO PODER. *Reportaje de Noticia de Fecha: 02/12/13*.

(80) Artículo 1 de la ley 30171 que modifica el artículo 10 de la ley 30096.

(81) *Diccionario de la Real Academia Española*. Referencia de 28 de marzo del 2014. Disponible en web: http://www.rae.es/recursos/diccionarios/drae.

(82) *Diccionario de la Real Academia Española*. Referencia de 28 de marzo del 2014. Disponible en web: http://www.rae.es/recursos/diccionarios/drae.

(83) *Diccionario de la Real Academia Española*. Referencia de 28 de marzo del 2014. Disponible en web: http://www.rae.es/recursos/diccionarios/drae.

(84) *Diccionario de la Real Academia Española*. Referencia de 28 de marzo del 2014. Disponible en web: http://www.rae.es/recursos/diccionarios/drae.

(85) *Diccionario de la Real Academia Española*. Referencia de 28 de marzo del 2014. Disponible en web: http://www.rae.es/recursos/diccionarios/drae.

(86) *Diccionario de la Real Academia Española*. Referencia de 28 de marzo del 2014. Disponible en web: http://www.rae.es/recursos/diccionarios/drae.

importar el resultado posterior. Aquí, el legislador adelanta las barreras de punibilidad al sancionar el solo hecho de fabricar, diseñar, vender, etcétera; mecanismos y programas orientados a cometer diversos delitos previstos en la ley. Esta figura penal es una construcción cercana a la idea del llamado *derecho penal del enemigo* porque se sanciona actos preparatorios alegando la puesta en peligro de la seguridad informática. Por ejemplo tráfico de datos de usuarios y contraseñas obtenidas ilícitamente para cometer fraudes informáticos, comercializar equipos especializados en capturar, interceptar información, etcétera.

Este artículo es compatible con el artículo 6 de la Convención de Budapest, sin embargo, hay una interpretación muy amplia, un vacío de este articulo por cuanto se extiende a toda gama de delitos previstos en la presente ley y que podría generar problemas en la interpretación judicial, debido a la extensión de ilícitos como: *interferencia telefónica*, *pornografía infantil*, etcétera.

> "Artículo 11.- El juez aumenta la pena privativa de libertad hasta un tercio por encima del máximo legal fijado para cualquiera de los delitos previstos en la presente Ley, cuando:
>
> 1. El agente activo integra una organización criminal.
>
> 2. El agente tiene posición especial de acceso a la data o información reservada.
>
> 3. El delito se comete para obtener un fin económico.
>
> 4. El delito compromete fines asistenciales, la defensa, la seguridad y soberanía nacional".

Este artículo regula las agravantes de los delitos previstos en la presente ley, y que en base a este artículo el juez puede aumentar hasta en un tercio por encima del máximo legal fijado. Por ejemplo participación de integrantes de la organización criminal en la comisión de delitos informáticos o el acceso ilícito a la cuenta de correo electrónico a cambio de un pago (los *hackers* de un centro comercial).

> "Artículo 12.- Está exento de responsabilidad penal el que realiza las conductas descritas en los artículos 2, 3, 4 y 10 con el propósito de llevar a cabo pruebas autorizadas u otros procedimientos autorizados destinados a proteger sistemas informáticos"(87).

Este artículo, incorporado por el artículo 3 de la Ley 30171 *Ley que modifica la Ley 30096, Ley de Delitos Informáticos*, exime de responsabilidad penal a toda persona que realiza alguna de las conductas regulado en el artículo 2, 3, 4 y 10 de la presente Ley. Esta cláusula de exención de responsabilidad se fundamenta en la conducta legal (autorizado por la autoridad correspondiente) para realizar pruebas u otro procedimiento con el objetivo de proteger los sistemas y datos informáticos. Este artículo es compatible con el artículo 6, inciso 2 del Convenio de Budapest.

2.7. Sanciones a personas jurídicas impuestas por organismos reguladores

La nueva ley de delitos informáticos contiene once disposiciones complementarias finales, de las cuales sólo nos enfocaremos a lo referente a las personas jurídicas, que se encuentran en la décima y undécima DCF de la nueva Ley.

Regulación e imposición de multas por la Superintendencia de Bancas, Seguros y AFP.

> "Décima.- La Superintendencia de Banca, Seguros y AFP establece la escala de multas atendiendo a las características, complejidad y circunstancias de los casos aplicables a las empresas bajo su supervisión que incumplan con la obligación prevista en el numeral 5 del artículo 235 del Código Procesal Penal, aprobado por Decreto Legislativo 957.

(87) Artículo 12.- EXENCIÓN DE RESPONSABILIDAD PENAL**,** incorporado por el artículo 3º de la ley 30171, *Ley que modifica la Ley Nº 30096, Ley de Delitos Informáticos*. Publicado el 10 de marzo del 2014.

> El juez, en el término de setenta y dos horas, pone en conocimiento del órgano supervisor la omisión incurrida por la empresa, con lo recaudos correspondientes sobre las características, complejidad y circunstancias del caso particular, a fin de aplicarse la multa correspondiente"

Esta disposición establece que la Superintendencia de Banca, Seguros y AFP determina la escala de multa de acuerdo a la característica, complejidad y circunstancias de los casos aplicables de las empresas bajo su supervisión que incumplan con la obligación de acuerdo con el artículo 235, inciso 3 del Código Procesal penal.

Este tipo legal tiene las características de una norma en blanco porque se complementa en otra ley (*Ley general del sistema financiero y del sistema de seguros y orgánica de la superintendencia de banca y seguros*, Ley 26702) para establecer las sanciones a las empresas que omiten una orden judicial.

Esta modificación completa el círculo de la facultad sancionadora que tiene el Estado, con la sanción administrativa por el incumplimiento de las entidades del sistema financiero de la obligación de entregar la información correspondiente a la orden judicial de levantamiento del secreto bancario.

Regulación e imposición de multas por el organismo Supervisor de Inversión privada en telecomunicaciones.

> "Undécima.- El Organismo Supervisor de Inversión Privada en Telecomunicaciones establece la escala de multas atendiendo a las características, complejidad y circunstancias de los casos aplicables a las empresas bajo su supervisión que incumplan con la obligación prevista en el numeral 4 del artículo 230 del Código Procesal Penal, aprobado por Decreto Legislativo 957.
>
> El juez, en el término de setenta y dos horas, pone en conocimiento del órgano supervisor la omisión incurrida por la empresa, con los recaudos correspondientes sobre las características, complejidad y circunstancias del caso particular, a fin de aplicarse la multa correspondiente".

El Organismo Supervisor de Inversión privada en telecomunicaciones establece la escala de multas atendiendo a las características, complejidad y circunstancias de los casos aplicables a las empresas bajo su supervisión que incumplan la obligación prevista en el numeral 4 del artículo 230 del Código Procesal Penal.

Esta modificación, al igual que el ya mencionado, sanciona administrativamente el incumplimiento de las empresas prestadoras de servicios de comunicaciones y telecomunicaciones de la obligación de posibilitar la diligencia judicial de intervención, grabación o registro de las comunicaciones y telecomunicaciones.

3. Reformas del Código Penal relacionadas con los delitos informáticos

Los artículos 158, 162 y 323 del Código Penal fueron modificados por el artículo 4 de la ley 30171 (*Ley que modifica la Ley Nº 30096º, Ley de delitos informáticos*) en los siguientes términos:

> "Artículo 158**.-**
> Los delitos previstos en este capítulo son perseguibles por acción privada, salvo en el caso del delitos previsto en el artículo 154-A"

Este artículo, antes de la modificatoria, establecía la acción privada para los delitos comprendidos en el Capítulo II *Violación de la intimidad*. A partir de la incorporación del artículo 154-A *Tráfico ilegal de datos personales*, se prevé el ejercicio público de la acción penal sólo para el mencionado artículo incorporado.

> "Artículo 162.-
> El que, indebidamente, interfiere o escucha una conversación telefónica o similar, será reprimido con pena privativa de libertad no menor de tres ni mayor de seis años.

Si el agente es funcionario público, la pena privativa de libertad será no menor de cuatro ni mayor de ocho años e inhabilitación conforme al artículo 36, inciso 1, 2 y 4.

La pena privativa de libertad será no menor de cinco ni mayor de ocho años cuando el delito recaiga sobre información clasificada como secreta, reservada o confidencial de conformidad con la Ley 27806, *Ley de Transparencia y Acceso a la información Pública*.

La pena privativa de libertad será no menor de ocho ni mayor de diez años cuando el delito comprometa la defensa, la seguridad o la soberanía nacionales.

Si el agente comete el delito como integrante de una organización criminal, la pena se incrementa hasta en un tercio por encima del máximo legal previsto en los supuestos anteriores".

La modificación de este artículo se da porque la redacción anterior era muy amplia y dejaba al arbitrio del juzgador determinar qué información se clasifica como secreta, reservada o confidencial. Es ahí la necesidad de precisar la agravante del *delito de interferencia telefónica* cuando afecte la información secreta, reservada o confidencial y, esta precisión se encuentra en la Ley 27806 *Ley de transparencia y acceso a la información pública*.

A modo de información, debe mencionarse que después de la promulgación de la Ley 30096, el 5 de diciembre del año 2013 se ha presentado otro *proyecto de ley 3048/ 2013- CR*[88] que busca modificar el mencionado artículo, argumentado que no se ha regulado correctamente la conducta a sancionar, además agrega algunas agravantes como es el móvil de la interceptación[89].

"Artículo 154-A.-
El que ilegítimamente comercializa información no publica relativa a cualquier ámbito de la esfera personal, familiar, patrimonial, laboral, financiera u otro de naturaleza análogo sobre una persona natural, será reprimido con pena privativa de libertad no menor de tres ni mayor de cinco años.

Si el agente comete el delito como integrante de una organización criminal, la pena se incrementa hasta en un tercio por encima del máximo legal previsto en el párrafo anterior"[90].

Este delito de tráfico ilegal de datos personales sanciona la conducta de comercializar (*comercializar*, *traficar*, *vender*, *promover*, *favorecer* o *facilitar*) información no pública, independientemente si con estos actos se causa algún perjuicio.

Este injusto penal, por la característica que presenta, es un *tipo de tendencia interna trascendente* por que presenta el elemento subjetivo *para*, que denota una intención especial consistente en la búsqueda de un

(88) Proyecto de Ley presentado el 5 de diciembre del 2013 por el Congresista de la República José Luna Gálvez, integrante del Grupo Parlamentario Solidaridad Nacional.

(89) El Proyecto de Ley 3048/2013-CR, pretende incrementar las sanciones contempladas para este ilícito en su modalidad básica e incluye dos conductas que agravan la figura penal, en los supuestos de recaer sobre información clasificada como secreta, reservada o confidencial de conformidad con las normas de la materia y compromete la defensa, seguridad o la soberanía nacional. Este proyecto pretende una mejor regulación de la conducta prohibida, al sancionar no solo el hecho de interferir o escuchar una conversación telefónica, sino sobre todo al considerar que también se debió incluir el hecho de *grabar*, porque según fundamentan no es lo mismo interceptar, escuchar y grabar. Otra circunstancia que considera agravante, es la referida al móvil por el que se realiza la conducta típica, ya sea para obtener un provecho tanto para el autor como para un tercero a cambio de dinero y otra ventaja, o si la intención es para perjudicar a la victima de interceptación sea de manera económica o de otra manera. Otra circunstancia que considera agravante es la referida al móvil por el que se realiza la conducta típica, ya sea para obtener un provecho tanto para el autor como para un tercero a cambio de dinero y otra ventaja, o si la intención es para perjudicar a la victima de interceptación sea de manera económica o de otra manera.

resultado diferente exigido típicamente, por tanto se clasifica como un *delito de resultado cortado* por que el agente busca un resultado que está más allá del tipo, el cual es comercializar, traficar, etcétera, una base de datos. Ejemplo: la comercialización de bases de datos que contienen nombres, documentos de identidad, edad, estado civil, domicilio, teléfono, ocupación, puesto laboral, remuneración, etcétera.

> "Artículo 183-B.-
> El que contacta con un menor de catorce años para solicitar u obtener de él material pornográfico, o para llevar a cabo actividades sexuales con él, será reprimido con una pena privativa de libertad no menor de cuatro ni mayor de ocho años e inhabilitación conforme a los numerales 1, 2 y 4 del artículo 36.
>
> Cuando la víctima tiene entre catorce y menos de dieciocho años de edad y medie engaño, la pena será no menor de tres ni mayor de seis años e inhabilitación conforme a los numerales 1, 2 y 4 del artículo 36"[91].

Esta figura penal sanciona la conducta de contactar (establecer contacto o comunicación con alguien)[92] con un menor de catorce años para solicitar u obtener de él material pornográfico, o para llevar a cabo actividades sexuales. Esta figura regula la agravante cuando la víctima tiene entre catorce y menos de dieciocho años y medie engaño, para este supuesto la pena a imponer será no menor de tres ni mayor de seis años.

Este figura penal (*proposiciones sexuales a niños, niñas y adolescentes*), por la característica que presenta el tipo legal, se clasifica como un *tipo de tendencia interna trascendente*, por que presenta el elemento subjetivo *para* que denota una intención especial consistente en la búsqueda de un resultado diferente exigido típicamente, por tanto se clasifica como un *delito de resultado cortado*, por que el agente busca un resultado que está más allá del tipo, el cual es *obtener material pornográfico o tener acto sexual con la menor.*

4. Conclusiones

- La finalidad de la *Ley de Delitos Informáticos* es prevenir y sancionar las conductas ilícitas que afectan los sistemas y datas informáticos, secreto de comunicaciones, contra el patrimonio, la fe pública y la libertad sexual cometidos mediante la utilización de las TIC.

- La figura penal de *acceso ilícito*, regulada en el artículo 2, se clasifica como un *delito de mera actividad*, porque en este ilícito el delito queda consumado en el mismo acto de vulnerar las medidas de seguridad de un sistema informático.

- La figura penal de *atentado contra la integridad de datos informáticos,* regulada en el artículo 3, se clasifica como un *delito de mera actividad*, porque en este ilícito el delito queda consumado en el mismo acto de introducir, borrar, deteriorar, alterar, suprimir y hacer inaccesible los datos informáticos.

- La figura penal de *atentado contra la integridad de sistemas informáticos*, regulada en el artículo 4, se clasifica como un *delito de resultado*, porque la configuración de este ilícito no basta con realizar la conducta exigida en el tipo, sino que es necesario un resultado posterior que consiste en impedir el acceso, imposibilitar el funcionamiento del sistema informático o impedir la prestación de su servicio.

- La figura penal de *proposición a niños, niñas y adolescentes con fines sexuales*

(90) Articulo incorporado al Código Penal por la Ley 30171.
(91) Articulo incorporado al Código Penal por la Ley 30171.
(92) *Diccionario de la Real Academia Española*. Referencia de 28 de marzo del 2014. Disponible en web: http://lema.rae.es/drae/?val=contactar.

por medios tecnológicos, regulada en el artículo 5, es un *tipo de tendencia interna trascendente* porque presenta un elemento subjetivo distinto del dolo que denota una especial intención del agente, por tanto esta figura se clasifica como un *delito de resultado cortado*, porque el agente persigue un resultado posterior el cual es obtener material pornográfico o alguna actividad sexual.

- La figura penal de *tráfico ilegal de datos*, regulada en el artículo 6, queda derogada por la única disposición complementaria derogatoria de la Ley 30171. Este articulo derogado fue incorporado al Código Penal (Artículo 154-A; *tráfico ilegal de datos personales*)

- La figura penal de *interceptación de datos informáticos*, regulada en el artículo 7, es un *delito de peligro abstracto*, y se clasifica como un *delito de mera actividad* porque en este ilícito el delito queda consumado en el mismo acto de interceptar datos informáticos

- La figura penal de *fraude informático*, regulada en el artículo 8, se clasifica como un *delito de resultado*, porque la configuración de este ilícito no basta con realizar la conducta exigida en el tipo legal (diseño, introducción, alteración, borrado, supresión, clonación de datos informáticos o cualquier interferencia o manipulación en el funcionamiento de un sistema informático), sino que es necesario un resultado posterior que consiste en causar un perjuicio a tercero.

- La figura penal de *suplantación de identidad*, regulada en el artículo 9, se clasifica como un *delito de resultado*, porque la configuración de este ilícito no basta con realizar la conducta exigida en el tipo (suplantar la identidad de una persona natural o jurídica), sino que es necesario un resultado posterior que consiste en causar un perjuicio.

- La figura penal de *abuso de mecanismos y dispositivos informáticos,* regulada en el artículo 10, se clasifica como un *delito de mera actividad*, porque en este ilícito el delito queda consumado en el mismo acto de fabricar, diseñar, vender, etcétera; el mecanismo o los programas orientados a cometer diversos delitos previstos en esta ley.

- La *Décima disposición complementaria final* regula la sanción administrativa para las personas jurídicas que están bajo la supervisión de la SBS que incumplan una orden judicial consistente en brindar información sobre el secreto bancario.

- La *Undécima disposición complementaria final* regula la sanción administrativa para las personas jurídicas que están bajo la supervisión de OSIPTEL que incumplan una orden judicial consistente en brindar información sobre la intervención, grabación o registro de las comunicaciones telefónicas.

5. Glosario de términos

- Activo patrimonial: Conjunto de bienes y derechos que integran el haber de una persona física o jurídica.

- Base de Datos: Conjunto completo de ficheros informáticos que reúnen informaciones generales o temáticas, que generalmente están a disposición de numerosos usuarios.

- *Browser* (Buscador): El software para buscar y conseguir información de la red WWW. Los más comúnmente usados son *Microsoft Explorer*, *Firefox* y *Opera*.

- *Cookie*: Es un archivo o datos dejados en su computadora por un servidor u otro sistema al que se hayan conectado. Se suelen usar para que el servidor registre información sobre aquellas pantallas que usted ha visto y de la información personalizada que usted haya mandado. Muchos usuarios consideran esto como una invasión de privacidad, ya que casi ningún sistema dice lo que está haciendo. Hay una variedad de *anti-cookie software* que automáticamente borran esa información entre visitas a su sitio.

- *Dialup* (marcar) El método de conectarse con internet vía la línea de teléfono normal

mediante un modem, en vez de mediante una LAN (red Local) o de una línea de teléfono alquilada permanentemente. Esta es la manera más común de conectarse a Internet desde casa si no ha hecho ningún arreglo con su compagina de teléfono o con un ISP. Para conexiones alternativas consulte con su ISP primero.

- *Digital Signature* (Firma digital): El equivalente digital de una firma autentica escrita a mano. Es un dato añadido a un fichero electrónico, diciendo que el dueño de esa firma escribió o autorizo el Archivo.

- Documento electrónico: Es la representación en forma electrónica de hechos jurídicamente relevantes susceptibles de

- HTTP (*Hyper Text Transport Protocol*): El conjunto de reglas que se usa en Internet para pedir y ofrecer páginas de la red y demás información. Es lo que se pone al comienzo de una dirección, tal como "http: /," para indicarle al buscador que use ese protocolo para buscar información en la página.

- *Internet Service Provider* (ISP) (Proveedor de Servicio de Internet): Una persona, organización o compagina que provee acceso a Internet. Además del acceso a Internet, muchos ISP proveen otros servicios tales como anfitrión de Red, servicio de nombre, y otros servicios informáticos.

- Mensaje de Datos: Es toda aquella información visualizada, generada enviada, recibida, almacenada o comunicada por medios informáticos, electrónicos, ópticos, digitales o similares.

- *Modem*: Un aparato que cambia datos del computador a formatos que se puedan transmitir más fácilmente por línea telefónica o por otro tipo de medio.

- Sistema Telemático. Conjunto organizado de redes de telecomunicaciones que sirven para trasmitir, enviar, y recibir información tratada de forma automatizada.

- Sistema de Información: Se entenderá como sistema de información, a todo sistema utilizado para generar, enviar, recibir, procesar o archivar de cualquier forma de mensajes de datos.

- Sistema Informático: Conjunto organizado de programas y bases de datos que se utilizan para, generar, almacenar, tratar de forma automatizada datos o información cualquiera que esta sea.

- Sociedad de la Información: La revolución digital en las tecnologías de la información y las comunicaciones (TIC) ha creado una plataforma para el libre flujo de información, ideas y conocimientos en todo el planeta. Ha causado una impresión profunda en la forma en que funciona el mundo. La Internet se ha convertido en un recurso mundial importante, que resulta vital tanto para el mundo desarrollado por su función de herramienta social y comercial, como para el mundo en desarrollo por su función de pasaporte para la participación equitativa y para el desarrollo económico, social y educativo.

- Soporte Lógico: Cualquiera de los elementos (tarjetas perforadas, cintas o discos magnéticos, discos ópticos) que pueden ser empleados para registrar información en un sistema informático.

- Soporte Material: Es cualquier elemento corporal que se utilice para registrar toda clase de información.

- Telemática: neologismo que hace referencia a la comunicación informática, es decir la transmisión por medio de las redes de telecomunicaciones de información automatizada.