EL DELITO DE ORDENADOR

Daniel Ernesto Peña Labrin *

RESUMEN.

El presente artículo de investigación jurídica, tiene por finalidad examinar la problemática de los delitos informáticos; la técnica legislativa que a su vez se ha visto rebasada por la realidad avasallante del siglo XXI, causando alarma social por la cifra negra que cohabita en esta clase de ilícitos penales, que aun se cubren por la afanada impunidad, en relación a las conductas antisociales y delictivas que pululan en el ciberespacio, resaltando las limitaciones de la descripción típica de los delitos informáticos patrimoniales vigentes y la necesidad ineluctable de su ampliación, existiendo conflictos y reservas legales que no están renovados a los indudables reclamos punibles del enjambre colectivo, exigiendo una respuesta inmediata al Derecho Penal, como mecanismo de control formal de la criminalidad informática.

PALABRAS CLAVE:

Ius Cibernética, Delitos Informáticos, Derecho Informático, Informática Jurídica, Seguridad Informática y Prevención.

SUMARIO:

* Abogado & Sociólogo-UIGV, Lima- Perú, Investigador permanente, Premio Excelencia Académica (1995-1999), Magíster en Derecho Penal- UNFV (2009), Diploma de Post Grado en Derecho Informático y Comercio Electrónico-UIGV (2004); Diploma de Honor por la Participación en el Primer Concurso Nacional de Investigación Jurídica 2007, Convocado por el Ilustre Colegio de Abogados de Lima; Catedrático en la Facultad de Derecho y Ciencias Políticas de la Universidad Inca Garcilaso de la Vega; Sub-Director de la Revista Electrónica: "Ultima Ratio" de la Facultad de Derecho y Ciencias Políticas de la Universidad Alas Peruanas; Miembro de la Comisión Consultiva de Derecho y Comunicación en Tecnología Informática del Ilustre Colegio de Abogados de Lima - 2007.Catedrático Principal de la EMCH y del Portal Web: enplenitud.com, Bs As-Argentina. Email:oficinacist@yahoo.es

1. NOTAS PRELIMINARES

En el enjambre mundial, todos los ciudadanos de una u otra forma encuentran su accionar cotidiano vinculado a la informática. La ingerencia del ordenador electrónico ha rebasado distintas esferas y relaciones sociales que obligan al profesional del **siglo XXI**, a conocer y dominar esta disciplina que nos trae la modernidad[1]. En tal sentido el uso de las computadoras y su interconexión, ha dado lugar a un fenómeno de nuevas dimensiones: el delito instrumentado mediante el uso del computador, hablándose hoy en día de la **ius cibernética**. Si bien no existe aún una medida exacta de la importancia de estas transgresiones, es probable que su incidencia se acentúe con la expansión del uso de computadoras y redes telemáticas. Los tipos penales tradicionales resultan en nuestros países inadecuados para encuadrar las nuevas formas delictivas, tal como la interferencia en una red bancaria para obtener, mediante una orden electrónica, un libramiento ilegal de fondos o la destrucción de datos. El tema plantea, además, complejos perfiles para el Derecho Internacional cuando el delito afecta a más de una jurisdicción nacional. [2]

En la actualidad, el lado más dinámico de la relación **Informática y Derecho**, es la **Informática Jurídica**. En el cual la información contenida en soportes electromagnéticos y otros complementarios podrá ser compartida y analizada por diferentes juristas nacionales y extranjeros, y el aporte del **Derecho Informático** es la solución legal de problemas jurídicos que traen la aplicación de las nuevas tecnologías de información, constituyendo las dos caras de una misma moneda, unidas irremediablemente.[3]

Los avances tecnológicos, el acceso masivo a **Internet**, el aumento de la pobreza y la relación al cambio bursátil del peso de las monedas extranjeras son identificados como los principales factores que explican la profundización de este delito. Las cámaras digitales y los videos grabadoras son cada vez más accesibles para los cibernautas de clases media y

---

[1] PEÑA LABRIN, Daniel Ernesto, Prólogo de la Obra: Informática Jurídica. En BLOSSIERS HÜME, Juan José, Informática Jurídica, Edit. Portocarrero, Lima, 2003, Pág.13

[2] PEÑA LABRIN, Daniel Ernesto, Informática Jurídica, Revista de Derecho-Asociación Peruana de Ciencias Jurídicas y Conciliación. APECC, Año I, Nº 2 , Lima 2004, Pág. 83

[3] GUZMÁN COBEÑAS, María del Pilar, Ponencia sobre Pornografía Infantil, ECAI 2008, Lima, Pág. 03

alta. No obstante, a medida de que bajen los costos las conexiones de banda ancha se multiplicaran, lo que propicia aún más el delito de ordenador.[4]

Ante esto, señala **Klaus Tiedemann**[5] que la tarea del Derecho no es la de quedarse atado a viejas categorías teóricas que nada sirven sino más bien de adaptarse y proveerse de nuevas formas de prevención y protección a la sociedad. Es por ello que el Derecho Penal debe revisarse así mismo, y encuadrarse en estas situaciones que protejan a las personas y no esconderse en lagunas legales que no ayudan a nada.

Por lo tanto, el Derecho Penal debe también prevenir la comisión de éste tipo de hechos que de ninguna manera pueden ser entendidos como errores involuntarios, ya que son realizados por personas que generalmente están se encuentran especializadas en el trabajo con computadoras y que pueden conocer como entrar en los archivos de datos de cualquier individuo.[6]

Sin embargo, el catálogo punitivo, debe resguardar los intereses de la sociedad, evitando manipulaciones computarizadas habituales o no, basadas en conocimiento de los objetos, programas, así como de algunas informaciones que extiendan y hagan imposible la detección de estos ilícitos, aprovechándose de la **cifra negra,** en este novísima clase de delitos, que aún se cubren bajo el manto de la afamada impunidad. [7]

2. PROBLEMÁTICA

El incuestionable perfeccionamiento actual y moderno ha traído ventajas substanciales para la humanidad, pero es penoso a su vez que

---

[4] PEÑA LABRIN, Daniel Ernesto, Curso de Filosofía del Derecho, Universidad Privada San Juan Bautista, Lima, 2007, Pág.15

[5] TIEDEMANN, Klaus, Derecho Penal y Nuevas Formas de Criminalidad, Edit. Idemsa, Lima, 2000, Pág. 267

[6] BLOSSIERS HÜME, Juan José, Criminalidad Informática, Editorial Portocarrero, Lima, 2003,Pág.145

[7] PEÑA LABRIN, Daniel Ernesto, La Firma Digital, En Revista "El Diplomado", Editada por la Escuela Universitaria de Post Grado de la Facultad de Derecho y Ciencia Política de la Universidad Nacional Federico Villarreal, Lima,2005,Pág.145

vengan acompañados de hechos delictivos no anhelados siendo imperioso e ineludible estudiar e indagar su accionar delictivo.[8]

La definición genérica de la **Organización para la Cooperativa Económica y el desarrollo, delito informático** («**computer crimen**») es «cualquier conducta ilegal, no ética o no autorizada que involucra el procesamiento automático de datos y/o la transmisión de datos». Estos delitos, conforme a **Sieber**, pueden ser clasificados en las siguientes categorías:[9]

a) Fraude por manipulaciones de un computador contra un sistema de procesamiento de datos;
b) Espionaje informático y Robo de Software;
c) Sabotaje Informático;
d) Robo de Servicios;
e) Acceso no autorizado a Sistemas de Procesamiento de Datos y Ofensas tradicionales en los negocios asistidos por computador.

El fraude por manipulación, incluye el cambio de datos o informaciones para obtener un beneficio económico. Estos delitos pueden afectar datos que representen activos (depósitos monetarios, créditos, etc.) o bien objetos materiales (manejo de inventario). Su perpetración puede acrecentarse en la medida que se difunden los cajeros automáticos, puntos de venta y otras máquinas electrónicas. La acción criminal puede basarse en la introducción de datos falsos en la computadora (diversos casos de este tipo se han dado en entidades bancarias), o bien en la modificación de los resultados.[10]

Del mismo modo, resultan del cambio en los programas de computación, tal como las fórmulas de «**Caballo de Troya**» (introducción de instrucciones para que el programa realice funciones no autorizadas, por ejemplo, acreditar la cuenta bancaria o un salario en la cuenta designada por el delincuente) o el «programa virus» (instrucciones que se infiltran

[8] PEÑA LABRIN, Daniel Ernesto, Curso –Taller de Investigación Jurídica, Edit. Centro de Investigaciones Sociales & Tributarias, Lima,2006,Pág.15

[9] HUGO VIZCARDO, Silfredo, Delitos Informáticos, En Revista Agora. Facultad de Derecho y Ciencias Políticas - U.I.G.V, Edición Nº 1, Lima, 2004, Pág. 95

[10] BLOSSIERS HÜME, Juan José, Criminología & Victimología, Edit. Disartgraf, Lima, 2005, Pág.158

automáticamente en otros programas y archivos). En la «técnica salami» (por ejemplo, redondear cuentas bancarias y acreditar lo montos resultantes en una cuenta) el acto delictivo se repite automáticamente indefinidas veces, sin ulterior intervención del defraudador.

Dado que en algunos países la figura del fraude requiere que una persona sea engañada, ella puede no ser aplicable cuando es la computadora la que ha sido objeto del engaño. Por otro lado, el tipo penal de abuso de confianza y el de falsificación encuentran límites en su aplicabilidad a estos casos. Para salvar los vacíos normativos, se han dictado normas penales especialmente referidas a los fraudes informáticos en Suecia (es punible la persona que ilegalmente obtiene acceso a registros de datos sujetos a procesamiento o altera, destruye o ingresa esos datos en un archivo); numerosos Estados de América, Inglaterra, Australia (criminalizan a cualquier persona que ilegalmente altere, falsifique, borre o destruya cualquier material de procesamiento de datos con una intención fraudulenta); Canadá, Alemania (la Segunda Ley para la Prevención del Crimen Económico, no requiere la presencia de una persona engañada para tipificar el delito de fraude); y Dinamarca, respectivamente.

Empero, los delitos de espionaje se refieren principalmente a la obtención (generalmente por parte de competidores) de resultados de investigaciones, direcciones de clientes, etc. Pueden ser cometidos introduciendo programas copiadores o por otros métodos (la radiación electrónica que emite un terminal informático puede ser captada y registrada sin mayor complicación hasta cerca de un kilómetro del lugar de la instalación).

De otro lado, el sabotaje cibernético puede referirse a los datos y los programas (por ejemplo, una «bomba de tiempo» que destruye el programa o una «**rutina cáncer**» que distorsiona el funcionamiento de aquel mediante instrucciones que se auto reproducen), o bien al equipamiento en sí. Algunas legislaciones, como se ha visto, y otras propuestas de ley en Francia, Suiza, Portugal, etc., se han elaborado para penalizar el daño cometido, aún cuando sólo abarque bienes intangibles (datos y programas).[11]

[11] DAVARA RODRIGUEZ, Miguel Ángel, Derecho Informático, Edit. Aranzandi, Madrid, 1997, Pág. 300

El «**robo de servicios**» (o «hurto de tiempo») se da generalmente cuando los empleados utilizan sin autorización horas de máquina del empleador, para realizar trabajos particulares.

La primordial modalidad del acceso no autorizado a sistemas de procesamiento de datos es el acceso remoto del que puede resultar la obtención ilegal de información, la destrucción de ésta u otras acciones delictuales. La ley Sueca castigó el mero acceso a un sistema de procesamiento de datos. en los Estados Unidos la «**Counterfeit Access Device and Computer Fraud and Abuse**» tipifica penalmente el acceso no autorizado a sistemas informáticos operados por el gobierno y en particular a los asociados a la defensa nacional, las relaciones externas y la energía atómica, así como a los de instituciones financieras.

De otro lado, la **pornografía infantil**, difundida depredadoramente en nuestros días, donde los pedófilos del ciberespacio utilizan ese medio para saciar sus anómalos apetitos y perversiones sexuales, aflorando y poniendo en evidencia las psicopatológicas sexuales que padecen, transmitiendo imágenes donde el ultraje a menores de edad constituye su negocio ante la inusitada demanda de un sinnúmero de personas que adquieren material electromagnético que incluye **Email, Audio, Chat, Messenger y Video**, aflorando una variedad de **psicopatologías sexuales**.

Verbigracia, en la **República de Chile** se prevé que cometerá delito informático la persona que maliciosamente uso o entre a una base de datos, sistema de computadores o red de computadoras o a cualquier parte de la misma con el propósito de diseñar, ejecutar o alterar un esquema o artificio, con el fin de defraudar, obtener dinero, bienes o información. Asimismo, comete este tipo de delito el que maliciosamente y a sabiendas y sin autorización, intercepta, interfiere, recibe, usa, altera, daña o destruye una computadora, un sistema o red de computadoras, un soporte lógico o programa de la computadora o los datos contenidos en la misma, en la base, sistema o red».

La postrera categoría enunciada, según la **clasificación de Sieber**, se refiere al uso de un computador propio para defraudar o enmascarar acciones punibles (en los casos anteriores se trata generalmente del uso o acceso al computador del tercero damnificado). Por ejemplo, la supresión de datos contables, la alteración de informaciones sobre stoks, etc.

Como puede denotarse, la problemática del cyberdelito requiere un estudio especial y conocimientos de causa (dada su tecnicidad), para poder cumplir con la labor de tipificar suficientemente estos delitos con vista a una adecuada protección social, ya que es creciente la expansión de la cultura informática en nuestro medio, tanto en el sector público como en el privado (el comercio, la actividad bancaria, la actividad industrial, el negocio de los particulares y empresas, etc.)[12]. Por tal motivo, es relevante para el ejercicio de la función del jurista, pues las características propias de la informática: memorización, comunicación, cálculo y asociación lógica, son imprescindibles para grabar y archivar las normas, analizar el lenguaje y el discurso lógico contenido en ellas[13]. Es necesario prepararse para prevenir y reprimir este tipo de conductas, ya que de acuerdo al axioma de la «auditoría», todo ilícito que tenga la más mínima posibilidad de ocurrir inexorablemente sino se lo previene (también es preciso tener en cuenta que es importante la influencia de las posibilidades técnicas de nuevas y más avanzadas máquinas, programas, capacidad de archivos de datos, etc.).

Lo descrito ultra supra, nos permite detallar que siendo tan amplio el espectro delictivo informático y para evitar la distorsión y dispersidad de normas, sería conveniente **postular un nuevo Título en el Libro Segundo del Código Penal**, que trate la **tipificación coherente y sistemática**, de todas las conductas criminales que esta actividad involucra y **no sólo los de carácter patrimonial**. Es por ello, sin duda alguna, que ha llegado el momento que la **Ciencia Penal** responda a las **exigencias sociales que la modernidad exige**, y de esta forma, rompa su moldura rígida clásica y evolucione conjuntamente con el desarrollo del conocimiento científico, permitiendo así la real protección de la seguridad y protección de la sociedad, ya que al parecer, se está quedando lisiado en esta materia de los flamantes delitos informáticos.[14]

Si inspeccionamos nuestro sistema penal, podemos apreciar que no tiene adecuadamente ampliado el tema, los delitos informáticos tienen su radio de acción principalmente en los atentados contra los derechos de

[12] PEÑA LABRIN, Daniel Ernesto, Curso de Criminología, Centro Nacional de Estudios Criminológicos y Penitenciarios CENECEP-INPE, Callao,2007, Pág.16

[13] PEÑA LABRIN, Daniel Ernesto, La Sociedad de la Información, Revista de Derecho & Informática-PCLEXPERU, Lima ,2005, Pág. 15

[14] HUGO VIZCARDO, Silfredo, Ob. Cit. Pág. 97

autor, violación de la intimidad personal, falsificación de documentos informáticos, entre otros. Indubitablemente, podemos apreciar que nuestro texto punitivo tipifica ciertas conductas posibles de ser cometidas mediante medios informáticos, tales como el hurto agravado utilizado sistema de transferencia electrónica de fondos de la telemática en general, descrito en el numeral 3 del segundo párrafo del artículo 186; el delito de fraude en la administración de personas jurídicas en la modalidad de uso de bienes informáticos (**Inciso 8 del artículo 198**), e incluso el delito de daños (**Art. 205**), desde la perspectiva del atentado contra el hardware (en su condición de bien material),etc. Por lo tanto, cualquier bien jurídico podrá ser vulnerado por el medio informático.

3. DELITO DE ORDENADOR

Mediante la disposición introducida por **Ley 27309, de fecha 17 de julio del 2000** se **modificó el Título V, del Libro Segundo del C. P**., insertando un nuevo capítulo (**Capítulo X**), denominado «**Delitos Informáticos**», que, como hemos visto, **sólo constituyen un sector parcial de este género delictivo**, orientado específicamente **al ámbito patrimonial**.

Por la **similitud del texto patrio**, consideramos que la fuente directa la encontrarnos en el proyecto de «**Ley de Informática**» del **Ministerio de Justicia de Chile** (**Abril de 1986**), que establece que: «cometerá delito informático la persona que maliciosamente use o entre a una base de datos, sistema de computadores o red de computadoras o a cualquier parte de la misma con el propósito de diseñar, ejecutar o alterar un esquema o artificio, con el fin de defraudar, obtener dinero, bienes o información. También comete este tipo de delito el que maliciosamente y a sabiendas y sin autorización intercepta, interfiere, recibe, usa, altera, daña o destruye una computadora, un sistema o red de computadoras, un soporte lógico o programa de la computadora o los datos contenidos en la misma, en la base, sistema o red».[15]

EI Libro Segundo, Título V del C. P., contiene a través de la **Ley Nº 27309 – Capítulo X: Ley de Delitos Informáticos siguiente clasificación típica:**

[15] BLOSSIERS HÜME, Juan José, Ob. Cit. Pág. 192

- **Acceso indebido a base de datos, sistema o red de computadoras..... Art. 207-A**
- **Sabotaje Informático..... Art.207-B**
- **Circunstancias agravantes... ..... Art. 207-C**

Nos resulta atípico que el legislador haya decidido ubicar la sistemática de los delitos informáticos dentro de los delitos contra el patrimonio, sin tener en cuenta que se incluye la protección de la intimidad en una de sus modalidades. El cimiento, a nuestro entender, debió ser el agrupar en un solo capítulo el empleo de los medios informáticos sin importar la afectación de distintos bienes jurídicos ya sea **individuales**: La vida, la libertad, el honor, el patrimonio, etc., y **colectivos**: El medio ambiente, la administración pública, el orden socioeconómico (concepción mixta o jurídica-económica del patrimonio), entre otros. Al respecto, indica **Javier Momethiano**[16] es un delito multiofensivo, incluyéndose en el ámbito del **Derecho Penal Económico**, pues la conducta del agente constituye una avanzada forma de ataque a bienes jurídicos cuya salvaguarda ya lo había reconocido el **Derecho Penal.**

En la codificación nacional como señalamos, fueron incorporados a través de la **Ley Nº 27309 – Capítulo X: Ley de Delitos Informáticos**, los que suscintamente explicaremos.[17]

- **Acceso indebido a base de datos, sistema o red de computadoras - Art. 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 cincuenta y dos a ciento cuatro jornadas.»

«Si el agente actúo con el fin de obtener un beneficio económico, será reprimido con pena privativa de libertad no mayor de tres años o con

[16] MOMETHIANO SANTIAGO, Javier Israel, Código Penal Fundamentado, Edit. San Marcos, Lima,2008,Pág.192

[17] Capítulo incorporado por la Ley Nº 27309, Publicada el 17 de Julio del 2000

prestación de servicios comunitarios no menor de ciento cuatro jornadas».[18]

Este delito es conocido también por la doctrina internacional como «**Hacking**» o «**Hacking lesivo**».

Ahora bien, podríamos señalar 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 descripción del tipo penal se puede denotar que el bien jurídico protegido en este delito no es el patrimonio, sino más bien, preliminarmente, la intimidad. Ello a consecuencia que en el tipo no se exige que el sujeto tenga la finalidad de obtener un beneficio económico, este requisito sine quanon es constitutivo de la modalidad agravada, más no de la conducta delictiva descrita en el tipo básico, ya que el legislador considera el mero ingreso no autorizado como afectación a la intimidad.

Empero, 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 indebido.

En tal sentido, el objeto material de la conducta realizada (no la que tiene eurísticamente el agente) es la base de datos, sistema o redes informáticas. A partir de esta óptica, debemos dejar en claro que el 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, 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. Con relación a la conducta típica, ésta comprende el hecho de utilizar o ingresar indebidamente a una base de datos, sistema o red de ordenadores.

Ergo, el término «**indebidamente**» debe ser entendido como el ingreso o la utilización de manera indebida o ilícitamente. El vocablo

[18] CÓDIGO PENAL PERUANO, Edit. Jurista Editores, Lima, 2007, Pág. 220. Pág. 256

«**indebido**» se refiere a lo injusto, ilícito y falto de equidad. El carácter indebido adjetiviza las conductas de ingresar o utilizar una base de datos, sistema o red de computadoras, deplorablemente el legislador penal no ha tomado en la promulgación de la ley y el hecho que aún no se ha regulado los ingresos indebidos a la red, por lo que se encuentra un vacío de contenido material en este artículo, ya que no se ha dicho nada al respecto; sin embargo, 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.

Por su parte, **Luís Alberto Bramont-Arias**[19] 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, verbigracia, la persona, en un descuido de un trabajador de la empresa que ha dejado encendida su computadora porque se ha ido a refrigerio, se aprovecha para utilizar la base de datos o el sistema. En dichos casos, se requiere que no se tenga la autorización debida, ya que el tipo penal señala «**el que utiliza o ingrese indebidamente**».[20]

Por lo tanto, 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 es óbice a que señalemos que con relación al bien jurídico: seguridad informática las conductas descritas en el **artículo 207°-A,** producen su lesión, por que afirmamos que se trata de un tipo penal de lesión y no de puesta en peligro. En suma, para la afectación 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 con que cuente el agente.

---

[19] BRAMONT-ARIAS TORRES, Luis Alberto, El Delito Informático en el Código Penal Peruano. Edit. Biblioteca de Derecho Contemporáneo, Volumen VI, Pontificia Universidad Católica del Perú, Lima, 2000, Pág. 72

[20] Ibidem. Pág. 75

Sin embargo, la descripción típica 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 pensamos que no es necesario a partir de reconocer a la seguridad informática como bien jurídico protegido en el delito de acceso indebido a base de datos, sistema o red de computadoras.

Por lo tanto, 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 éste es el sustento central de la conducta prohibida.

En el **artículo 207°- A**, si bien es punible 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**», más aún, cuando el propio legislador concibe como finalidad del ingreso el acceso, luego no puede darse una conducta de ingresar para acceder. Sin embargo, debemos aclarar que en cuanto al aspecto subjetivo, el **primer párrafo del numeral 207-A**, exige las finalidades antes descritas como elementos subjetivos de intención trascendente, no siendo necesaria su realización material.

Al considerarse dentro del carácter indebido de la conducta el hecho de no contar con autorización, el consentimiento del titular del sistema, base de datos o red de computadoras constituye causa de atipicidad.

Recordemos que el **segundo párrafo del artículo 207°-A**, contempla una **modalidad agravada** del **acceso indebido de datos**, **sistema o red de computadoras**, 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.

Con relación a los sujetos activos de esta figura penal, **Luis Alberto Bramont-Arias** opina «que cualquier persona puede cometer este ilícito penal y que no requiere tener grandes conocimientos de informática».[21]

[21] Ibidem, Pág. 76

En efecto, 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 en este tipo de delito exige el dolo del sujeto activo, ya que se requiere en el sujeto conciencia y voluntad de utilizar 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.

En el **artículo en exégesis**, 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**.

Se parte que 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.

Prosigue, **Luis Alberto Bramont-Arias** que 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, generaría un concurso de delitos. Este autor considera que en estos casos, el tipo penal 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 es de resultado, vale decir, el hurto agravado, subsume al delito de peligro, y al delito informático.[22]

Desde la óptica de la **seguridad informática** como bien jurídico protegido en el delito informático, se ha de precisar que no se deberá

[22] BLOSSIERS HÜME, Juan José, Ob. Cit. Pág. 162

acudir al empleo de elementos subjetivos de intención trascendente que pretendan vincular la conducta realizada con los **bienes jurídicos intimidad y patrimonio**, ya que los comportamientos objetivamente descritos en el **artículo 207°-A,** son suficientes para su lesión. Somos de la opinión de la eliminación de tales elementos subjetivos y la configuración del delito de acceso a base de datos, sistema o red de computadoras, vinculado a la afectación de la **seguridad informática**, ejerciendo así una protección antelada de los mencionados **bienes jurídicos individuales**. Ello no es óbice para que se pueda configurar **tipos penales específicos** que sancionan la lesión del **patrimonio o la intimidad** a través de medios informáticos.

Por último, siendo un tipo de resultado material, es posible la configuración de la tentativa, con las dificultades ya expresadas para la consumación y prueba del ilícito, por la especialidad del delito en análisis. Asimismo, dada su característica típica, la instigación y la complicidad es perfectamente posible. El que financia, el que induce, el que presta los equipos, el que aporta los datos o claves necesarias, etc.

· **Sabotaje Informático: Art. 207-B**

«El que utiliza, ingresa o interfiere indebidamente una base de datos, sistema, red o programa de computadora o cualquier parte de la misma con el fin de alterarlos, dañarlos o destruirlos, será reprimido con pena privativa de libertad no menor de tres ni mayor de cinco años y con setenta a noventa días multa».[23]

El delito de «**sabotaje informático**» es conocido también con el nombre de daño informático. Pensamos 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**, El ánimo del legislador ha sido configurar este delito como delito de peligro abstracto, en cuyo caso, para

[23] CÓDIGO PENAL PERUANO, Ob. Cit. Pág. 259

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.

En la descripción típica literal 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 sabotaje 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.

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. Asimismo, en el aspecto subjetivo tenemos al dolo sumado al ánimo de dañar, destruir o alterar la base de datos o sistema informático constituye un elemento subjetivo de intención trascendente, cuya realización material no es exigida por el tipo penal.

Luis Alberto Bramont Arias,[24] aclara que la diferencia entre los artículos 207°-A y 207°- B, versan en torno al aspecto subjetivo, esto es, la finalidad que tienen el sujeto activo al momento de realizar su conducta, ya que si la persona es detenida en el instante que está utilizando sin autorización una base de datos, para poder determinar que tipo penal se aplicaría, habría que preguntarse cuál es su animus en ese momento, vale decir, si el agente quiere destruir se le aplicará el artículo 207°-B, en caso

[24] BRAMONT-ARIAS TORRES, Luís Alberto, Ob. Cit. Pág. 79

contrario, habría que demostrar alguna de las finalidades previstas en el artículo 207°-A.

No obstante, respecto de este delito existirá la dificultad acerca de los elementos de prueba para determinar el animus del delincuente informático, ya que sino se puede determinar la intención 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. Con relación a este tema, pensamos que el legislador ha debido determinar la alteración, daño o destrucción de sistemas informáticos como consumación del delito.

Entendemos que para estos supuestos fácticos 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 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.

Acabaríamos, advirtiendo que el concurso de delitos que se daría desde esta perspectiva, entre el delito de Acceso indebido a base de datos, sistema o red de computadoras 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. Entonces, estaríamos frente a un concurso real de delitos debido a tratarse de hechos independientes y a la afectación de dos bienes jurídicos distintos.

Es ineludible precisar que en cuanto a la pena que se establece en este delito. **Luis Miguel Reyna Alfaro**[25] opina que «en el presente supuesto el legislador ha debido incluir la **inhabilitación como pena**

[25] REYNA ALFARO, Luis Miguel, Los Delitos Informáticos, Aspectos Criminológicos, Dogmáticos y de Política Criminal, Edit. Jurista, Lima, 2002, Pág. 278

principal». No obstante, para el mencionado 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**.

· **Circunstancias Agravantes Art. 207-C**

Conforme a lo dispuesto por el **artículo 207- C**, el tipo se agrava cuando:

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

La pena aplicable, en la **figura simple**, es privativa de libertad **no menor de tres ni mayor de cinco años y con setenta a noventa días multa** y el **tipo agravado no menor de cinco ni mayor de siete años**.[26]

En el **artículo 207 –C**, de nuestro Código Penal se describen dos agravantes; la primera con relación al cargo que posee el sujeto activo, la segunda, en razón a la seguridad nacional.

Asimismo, se señala como agravante si el agente se aprovecha de la información que obtiene por la función que desempeña. Dicha agravación se encuentra en relación a la confianza depositada en la persona del autor y en el manejo de determinada información, como pueden ser claves de acceso, passwords, etc.

Evidentemente, en esta descripción típica resulta de aplicación la exigencia de 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 las mencionadas fórmulas penales.

[26] CÓDIGO PENAL PERUANO, Ob. Cit. Pág. 261

Al respecto **Luis Alberto Bramont-Arias**[27], manifiesta que las agravantes descritas en el **artículo 207- C**, parten de la afectación a la seguridad informática. Estamos convencidos 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 catalogo punitivo.

De ahí encontramos que los puntos de coincidencia entre el tipo penal del artículo **251-A** y los delitos informáticos sólo se tornarían con relación al segundo párrafo del **artículo 207-A**, en cuanto que el agente actúa con el fin de obtener un beneficio económico; considerando el principio de especialidad se debería optar por el tipo penal del **artículo 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.

Con relación al aspecto subjetivo, dicha agravante deberá comprender el **dolo** previsto para los **artículos 207-A o 207-B** y, adicionalmente, el ánimo del agente respecto del prevalecimiento de la función que desempeña. Consecutivamente, el **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, ya que lo punible se atribuye a su puesta en peligro.

Frente a este panorama, podríamos considerar que en cuanto a la realización de las conductas materiales previstas por los **artículos 207-A y 207-B**, están todas aquellas normas que regulan y protegen la seguridad nacional, tanto desde la Constitución Política, como leyes especiales y reglamentos Sobre el aspecto subjetivo de la conducta, el dolo del autor deberá circunscribirse a la conciencia y voluntad de poner en peligro la seguridad nacional. De otro lado, dentro de las características ya anotadas en el presente estudio, la tentativa si es posible. Igualmente, la participación es configurable en el tipo precedente.[28]

---

[27] BRAMONT-ARIAS TORRES, Luis Alberto, Ob. Cit. Pág. 81
[28] BLOSSIERS HÜME, Juan José, Ob. Cit. Pág. 165

4. RESERVAS LEGALES

De lo glosado líneas anteriores, debemos enfatizar que la citada ley, adolece de aspectos fundamentales; verbigracia: la delimitación del bien jurídico protegido. De la **hermenéutica de la Ley Nº 27309**, sobre **Delitos Informáticos**, aparecen diversas críticas en cuanto a la sistemática aplicada al caso submateria y a esto se suma la gran cantidad de inexactitudes que ésta contiene, sobre aspectos: conceptuales, gramaticales y relativos a los principios generales del Derecho Penal.

En esta clase de ilícitos penales, para configurar la competencia de los Estados en la persecución de delitos se atiende al lugar de su comisión. A esta competencia se la denomina **Principio de Territorialidad**, o también conocido por el brocardo: **lex loci denincri comniti**, el mismo que se encuentra inmerso en el **numeral 1° y el de Extraterritorialidad, artículo 2º, contenidos en el Capítulo I de la Parte General** de nuestra clasificación criminal. [29]

En este postulado, no existirá mayor dificultad cuando el delito sea cometido en territorio nacional. De otro lado, cuando la comisión del delito sea en una nación extranjera, será complicado distinguir si la acción y la afectación a la seguridad informática se originaron en el mismo lugar o no a consecuencia del amplio debate entre la **Teoría de la Actividad**, si 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 efecto, los tratadistas, mayoritariamente, se apoyan en la **Teoría de la Ubicuidad**, 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, esta teoría es la seguida por nuestra legislación tal y como lo prevé el **artículo 5 del Código Penal Peruano**.[30]

Sostenemos que es meritoria la propuesta contra la **delincuencia de alta tecnología** asumida por el **Consejo Europeo** sobre la elaboración de un convenio sobre la delincuencia en la red iniciada desde **febrero del**

[29] PEÑA LABRIN, Daniel Ernesto, Curso de Derecho Informático, Universidad Privada San Juan Bautista, Lima 2006, Pág.12

[30] DURAND VALLADARES, Raúl, Cyber-Delito o Delitos de Ordenadores. Sistema Bancario Nacional, Edit. Grafi. Net, Lima, 2000, Pág. 267

año 1997 y que terminó el 2002. Además, 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 la red.**

Las características resaltantes de ésta posición común, son las del compromiso de los Estados miembros en facilitar una investigación y **persecución enérgica de los ilícitos penales vinculados con sistemas y datos informáticos**, así como **innovar adecuadamente el Derecho Penal y ajustarlo a las exigencias jurídico-sociológicas del siglo XXI.**

Por tal motivo, los Estados miembros intercederán, si es admisible comprender una normatividad que exija la tipificación como delitos relacionados con el contenido de los comportamientos delictivos llevados a cabo mediante un sistema informático.[31]

Debemos urgir que aún es limitado encontrar policías especializados en informática para determinar en un Parte Policial o en un Atestado Policial, la comisión de un delito informático, seguidamente en la instrucción de un proceso penal es necesario, según sea el caso, una pericia emitida por peritos judiciales adscritos a la Corte Superior de Justicia, a fin de determinar de manera científica, si ha existido un perjuicio. Sin embargo, la **Dirección de Investigación Criminal-Patrulla Digital de la PNP**, gesta la proeza de constatar el incremento y tecnificación de los cyberdelitos el año 2006. De las 456 denuncias del rubro, se resolvieron 243 y quedaron pendientes 213.El número queda en segundo lugar después de los 485 casos de homicidio durante el 2006, habiéndose multiplicado dichas conductas ilícitas en los años subsiguientes, lo que grafica la importancia descollante del referido rubro innovador.

El común de la gente piensa que porque somos un país pobre no tenemos esta clase de actividad criminal, prenoción que se ve ensombrecida por la realidad que día a día nos sorprende, siendo la epidemia global, según **The New York Time**, la empresa de seguridad virtual **DEFENSE**, había detectado 200 programas para robar contraseñas durante el año 2000, la cifra había llegado a 100 en el año 2003. Para el año 2007 la cifra estimada por dicha compañía asciende a 6000, más que el 2006 y la proyección para los subsiguientes años es alarmante.

---

[31] MARCHENA GÓMEZ, Juan, Prevención de la Delincuencia Tecnológica, Edit, Lima, Lima, 1992, Pág. 447

Ante este panorama, apremia el aleccionamiento en informática capacitando a los administradores y personas de apoyo, especialmente en provincias. Proceso que deberá desarrollarse paulatinamente, pero que finalmente estamos convencidos que es necesario para poder combatir con eficacia el cyberdelito.

De otro lado, encontramos una diferencia sustancial entre la pena para el delito de daños informáticos y la 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. Tal como enfatiza **Durand Valladares**[32], 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.

5. CONFLICTO JURÍDICO-SOCIOLÓGICO

Para preservar los intereses sociales el Estado debe agotar los medios menos lesivos que el Derecho Penal otorga, antes de acudir a éste, como última ratio, 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. Asimismo, **fomentar la prevención, trabajando multisectorialmente,** sobre el rol de la sociedad y del Estado, procurando la protección de ésta, frente al **desbordante progreso informático** que vivimos hoy, **ya casi al final de la primera década del siglo XXI.**

Además, tal como sostiene **Santiago Mir Puig**[33] «Sólo cuando ningún mecanismo administrativo o civil sea suficiente, entonces estará legitimado el recurso de la pena o de la medida de seguridad, pues las

[32] DURAND VALLADARES, Raúl, Cyber-Delito o Delitos de Ordenadores. Sistema Bancario Nacional Edit. Grafi.Net, Lima, 2000, Pág. 200.

[33] MIR PUIG, Santiago, Derecho Penal – Parte General, Edit. PPU, Barcelona, 1996, Pág. 189

funciones del acceso y tránsito de la red y sistemas informáticos resultan ser las pautas sobre las que deberá construirse la regulación acorde a la realidad que el derecho exige», para ubicar, perseguir, enjuiciar y punir a los responsables de estos delitos, hasta ahora premunidos del cálido manto de la impunidad, en vista de legislaciones nacionales que enlacen sus limitados brazos naturales y las persecuciones se programen, ejecuten y consumen en colaboracionista forma supranacionales, que reflejan decisiones efectivas de intervenirlos.

6. CONCLUSIONES

PRIMERA: El acceso al conocimiento de la información es uno de los derechos constitucionales básicos que gozan los ciudadanos y es una forma de control público que es parte del sistema democrático. Si bien es cierto que el Estado se esfuerza para que esta información llegue a quien la solicite, aún es insuficiente, pues cotidianamente somos espectadores y a veces protagonistas disconformes, de cómo se administran estos servicios por lo que su manejo oficial no es satisfactorio para la colectividad, lo que origina el obsequio de una sombra de opacidad al desempeño gubernamental, lo que deja mucho que desear, por el sentimiento generalizado que exige, luego de la secuela dejada por la dictadura en la década anterior, que toda gestión refleje transparencia.

SEGUNDA: El progreso de la informática es una de las características primordiales y destacadas de este milenio, por lo que su utilización comprende un abanico de posibilidades que es indispensable delimitar a fin de combatir los excesos que se vienen apreciando. Por lo que ante esta situación, es natural la aparición de renovadas disposiciones penales en salvaguarda de los bienes jurídicos que urgen de protección. La sociedad debidamente organizada, a través de sus instituciones preclaras y los obligados a legislar, tiene la palabra para establecer propuestas que permitan su control y consecuente sanción.

TERCERA: Como es reconocido, el adelanto informático permite agilizar el conocimiento y las comunicaciones, pero también es verdad que su notable evolución ha permitido que emerjan conductas antisocial y delictivas que atentan contra los méritos del adelanto científico, pensado y fabricado para dotar a la humanidad de lo necesario para su eficaz desarrollo.

CUARTA: Desde la década del treinta Edwin Sutherland, gallardo sociólogo norteamericano, que ha pasado a la galería de los insobornables , advirtió y denunció ante el planeta, que la criminalidad no estaba circunscrita a los sectores menos pudientes de la sociedad, y documentadamente probó las actuaciones de los **"delincuentes de cuello blanco"** en las áreas económicas y financieras, por lo que su incursión en los ilícitos informáticos no debería sorprendernos, que gente de alto nivel socio-económico los perpetren sin miramientos, para favorecerse con alevosía.

QUINTA: El Derecho Informático se ocupa de los problemas jurídicos que se dan en la sociedad, motivados por el uso de las computadoras; sin embargo, la informática jurídica sirve aplicativamente, otorgando la posibilidad maximizar la misión de la administración de justicia; construyendo una base de datos, que permite que se automatice su gestión, como son: Asistentes, Especialistas, Técnicos, Auxiliares, etc., y asimismo, los bufetes de abogados, las oficinas de peritos, etc. Sistematizándose el conocimiento jurídico por medio de la inteligencia artificial.

SEXTA: Es que la **galaxia de Internet**, es una contundente realidad, que tiene que ser aprovechada por las civilizaciones; con ingerencia en las dinámicas políticas, sociales, de producción y comercialización, culturales, deportivas, religiosas, etc. Pero lamentablemente, en la **perniciosa criminalidad informática**, que es ejercitada por individuos y grupos sociales que manejan

programas de esta índole se aprovechan de omisiones legales y atipicidades, por ahora en el campo jurídico, lo cual les facilita mantenerse en el limbo de la impunidad, relajando el aporte de la informática a la humanidad.

SETIMA: Los delincuentes informáticos, saben bien los conceptos de **Red y Web**, dado que el primero es una simple red o varias, configurados por PC´s y cables que remiten paquetes de datos a cualquier parte del mundo. En cambio en la **Web** se encuentran documentos, sonidos, videos, e información variada. Por lo que la **Web** no podría existir sin la **Red** y ambos sirven al modernísimo **Internet.**

OCTAVA: Al Internet lo podemos definir como información, tecnología y una red física de telecomunicación, que lubrica para que cualquier persona se integre a este mundo oneline, necesitando para ello una computadora conectada al ciberespacio.

NOVENA: Sin duda, podemos obtener información al ingresar a un **Portal de Internet**, aunque hay que señalar que no toda la información disponible sirve para trabajos legales o para el desenvolvimiento cultural en sentido positivo, pues también se encuentra por desgracia, rufianismo, proxenetismo, de infanto prostitución, meretricio masculino y femenino, pornografía, promiscuidad, juegos compulsivos, dudoso turismo, propaganda de tóxicos no permitidos que alientan la drogadicción, etc. Todas conductas antisociales o delictivas que se dejan pasar ante la carencia de una regulación jurídica, por su atentatoria moral pública, lo que está desnaturalizando el objetivo para el que fue concebido el Internet, como el de compartir información, cultura, conocimientos alcanzados por la ciencia, deportes, tónicos, estilos de vida saludables, etc., pero no como medio difusivo de agresiones y perversiones contra los usuarios, que se encuentran

frágilmente desprotegidos ante la potencial vulneración de sus derechos fundamentales..

DÉCIMA: Si nos fijamos en el **Derecho Internacional** en lo que concierne a la protección de la información computarizada destacan las **legislaciones europeas de Francia, Portugal, Inglaterra** y en **España**, otorgando preponderancia a la **represión de personas o de empresas que transgreden la ley**, concediéndole un tratamiento importante al **aspecto preventivo** y para tal efecto, existe una pormenorizada normatividad tutelar, control en la administración y protección de la información computarizada. Situación que llamamos la atención al **parlamento nacional,** para que construya un **marco legal moderno y eficaz**, acorde a la **sociedad de la información** que vivimos y regule oportunamente, los **vacíos jurídicos del delito de ordenador, que predominan en la Web**. **Infine**.

7. REFERENCIAS BIBLIOGRÁFICAS

1. **BLOSSIERS HÜME, Juan José**, Criminalidad Informática, Editorial Portocarrero, Lima, 2003.
2. **BLOSSIERS HÜME, Juan José**, Criminología & Victimología, Editorial Disartgraf, Lima, 2005.
3. **BRAMONT-ARIAS TORRES, Luis Alberto**, El Delito Informático en el Código Penal Peruano. Editorial Biblioteca de Derecho Contemporáneo, Volumen. VI, Pontificia Universidad Católica del Perú, Lima, 2000.
4. **GUZMÁN COBEÑAS**, María del Pilar, Ponencia sobre Pornografía Infantil, **ECAI 2008**, Lima.
5. **CÓDIGO PENAL PERUANO**, Editorial Jurista Editores, Lima, 2007.
6. **DAVARA RODRÍGUEZ, Miguel Ángel**, Derecho Informático, Editorial Aranzandi, Madrid, 1997.
7. **DURAND VALLADARES, Raúl**, Cyber-Delito o Delitos de Ordenadores, Sistema Bancario Nacional, Editorial Grafi.Net, Lima, 2000.

8. **HUGO VIZCARDO, Silfredo**, Delitos Informáticos, En Revista Agora. Facultad de Derecho y CIENCIAS Políticas - U.I.G.V, Edición Nº 1, Lima, 2004.
9. **MARCHENA GÓMEZ, Juan**, Prevención de la Delincuencia Tecnológica, Editorial Lima, Lima, 1992.
10. **MIR PUIG, Santiago**, Derecho Penal – Parte General, Editorial PPU, Barcelona, 1996.
11. **MOMETHIANO SANTIAGO**, Javier Israel, Código Penal Fundamentado, Edit. San Marcos, Lima, 2008.
12. **PEÑA LABRIN, Daniel Ernesto**, Prologo del Obra: Informática Jurídica. En **BLOSSIERS HÜME, Juan José**, Informática Jurídica, Editorial Portocarrero, Lima, 2003.
13. **PEÑA LABRIN, Daniel Ernesto,** Informática Jurídica, Revista de Derecho-Asociación Peruana de Ciencias Jurídicas y Conciliación APECC, Año I, Nº 2, Lima, 2004.
14. **PEÑA LABRIN, Daniel Ernesto**, La Sociedad de la Información, Revista de Derecho & Informática - PCLEXPERU, Lima ,2005.
15. **PEÑA LABRIN, Daniel Ernesto**, La Firma Digital, Revista "El Diplomado", Editada por la Escuela Universitaria de Post Grado de la Facultad de Derecho y Ciencia Política de la Universidad Nacional Federico Villarreal, Lima,2005
16. **PEÑA LABRIN, Daniel Ernesto**, Curso de Derecho Informático, Universidad Privada San Juan Bautista, Lima, 2006.
17. **PEÑA LABRIN, Daniel Ernesto**, Curso-Taller de Investigación Jurídica, Editado por el Centro de Investigaciones Sociales y Tributarias, Lima 2006
18. **PEÑA LABRIN, Daniel Ernesto**, Curso de Criminología, Centro Nacional de Estudios Criminológicos y Penitenciarios CENECP-INPE, Callao, 2007.
19. **PEÑA LABRIN, Daniel Ernesto**, Curso de Filosofía del Derecho, Universidad Privada San Juan Bautista, Lima, 2007.
20. **REYNA ALFARO**, Luis Miguel, Los Delitos Informáticos, Aspectos Criminológicos, Dogmáticos y de Política Criminal, Editorial Jurista, Lima, 2002.
21. **TIEDEMANN, Klaus**, Derecho Penal y Nuevas Formas de Criminalidad, Editorial Idemsa, Lima, 2000.

Lima-Perú, Junio de 2009