Nº 1:69-80 (Lima, UNMSM, 2014)

TIPIFICACIÓN DE LOS DELITOS INFORMÁTICOS PATRIMONIALES EN LA NUEVA LEY DE DELITOS INFORMÁTICOS N°30096

TYPING CYBERCRIME PATRIMONIAL IN THE NEW LAW ON CYBERCRIME N°30096

Silfredo Jorge Hugo Vizcardo

RESUMEN:

La utilización de computadoras, es decir, de sistemas informáticos, incide fundamentalmente sobre el desarrollo social de cada país (en relación directa con el grado de desarrollo cultural y económico). Por ello se dice contemporáneamente que la lucha por el poder político y económico se ha trasladado del ámbito del control de las grandes energías al del dominio de la información. Esta realidad ha determinado, como contrapartida negativa, la aparición de actos vulnerantes o lesionantes contra los derechos que alrededor de la propiedad o utilización de los medios informáticos se han ido generando y que han fundamentado una nueva gama de bienes jurídicos a proteger. Aparece así la criminalidad por computadora o "delito informático" (computer crime), que, desde la perspectiva político-criminal, es necesario definir y tipificar adecuada y sistemáticamente en el marco de los principios penales rectores, como el principio de legalidad, entre otros.

Palabras clave: *Delitos informáticos en materia patrimonial.*

ABSTRACT:

The use of computers, ie computer systems falls mainly on the social development of each country (thus directly related to the degree of cultural and economic development) (for it is said at one time that the struggle for political power and economic field was transferred from the control of the great powers to the domain of information) . This reality has been determined as negative counterpart , the appearance of vulnerant or acts against the rights or property around the use of information technology have been generated and have founded a new range of legal services to protect assets. Thus appears the computer crime or "cybercrime" ("computer crime") , that since the criminal political perspective is necessary to define and establish appropriate and systematically under criminal guiding principles such as the rule of law among others.

Keywords: *Computer crimes in volving property.*

Marco normativo: *Ley de Delitos Informáticos Nº 30096, Constitución Política. Código Penal D. Leg.*

I. INTRODUCCIÓN

Producto de la evolución del ingenio humano y de la ciencia, que siempre está a la vanguardia de la creación de mejores posibilidades de vida y sustento, modernamente aparecieron las denominadas computadoras u ordenadores, que revolucionaron el modo de vida social de toda la humanidad y dieron origen a la informática, concebida como la ciencia de la elaboración, memorización, conservación, análisis y recuperación de datos en forma significativa o simbólica (Durand 2002:167). Técnicamente concebido, el computador u ordenador es un dispositivo electrónico digital de programa almacenado capaz de memorizar, elaborar o recuperar información o datos.

Se trata de una herramienta muy técnica y sofisticada, de enorme aplicación práctica. Es la única máquina programable, ya que sale de fábrica con una capacidad instalada que constituye su sistema general (posee "capacidad" para interpretar cierto tipo de lenguaje o programa), y corresponde posteriormente al ingenio del hombre determinar la vastedad de su aplicación objetiva, mediante la inserción de una serie de datos o instrucciones que constituyen los programas de computación. En tal sentido, "las posibilidades del ordenador son inmensas, infinitas; permiten una verdadera enseñanza conforme a las ideas, las necesidades y lo que pretende el hombre, llegando a hacer muchas cosas como este, pero a mucha velocidad y sin cansancio"
(Núñez Ponce 1996:19).

Las aplicaciones de las computadoras son diversas, dependiendo de los programas que se utilicen. Inciden decisivamente en los diversos niveles de las relaciones humanas. Se constituye en una forma de "inteligencia artificial" de uso instantáneo, práctico y seguro. Pueden utilizarse en los negocios, industria, empresa, medicina, derecho, contabilidad, etc.; puede ser utilizado, como de hecho lo es, tanto por el sector público como el privado.

Actualmente, dentro de la denominada era de la automatización o revolución cibernética (comparable solo con la Revolución industrial), que caracteriza al mundo contemporáneo desde la década de los 50, no existe un solo sector de la sociedad que no se vea influenciado por la evolución alcanzada por la informática. Una de las principales causas de este fenómeno es el empleo generalizado y globalizado de la Internet, concebida como un sistema transnacional de comunicación que, gracias a unos estándares comunes y usando tecnologías y redes de telecomunicación, permite el intercambio y la obtención de información mediante el uso de diversas modalidades de comunicación en línea (listas de correo, grupos de discusión de Usenet, FTP, www, chats, etc.).

II. CONCEPTO

La utilización de computadoras, es decir, de sistemas informáticos, incide fundamentalmente sobre el desarrollo social de cada país (en relación directa con el grado de desarrollo cultural y económico). Por ello se dice contemporáneamente que la lucha por el poder político y económico se ha trasladado del ámbito del control de las grandes energías al del dominio de la información. Esta realidad ha determinado, como contrapartida negativa, la aparición de actos vulnerantes o lesionantes contra los derechos que alrededor de la propiedad o utilización de los medios informáticos se han ido generando y que han fundamentado una nueva gama de bienes jurídicos a proteger. Aparece así la criminalidad por computadora o delito informático ("computer crime"), que es definido como "la realización de una acción que, reuniendo las características que delimitan el concepto de delito, sea llevada a cabo utilizando un elemento informático o vulnerando los derechos del titular de un elemento informático, ya sea de hardware o de software" (Dávara 1993, p. 318). Conforme lo señala Tiedemann, con la expresión "criminalidad mediante computadoras" se alude a todos los actos antijurídicos según la ley penal vigente (o socialmente perjudiciales y por eso penalizables en el futuro), realizados con el empleo de un equipo automático de procesamiento de datos (1985:122).

Se trata de delitos instrumentados mediante el uso del computador. La Organización para la Cooperación Económica y el Desarrollo ha definido al delito informático como cualquier conducta ilegal, no ética, o no autorizada que involucra el procesamiento de datos y/o la transmisión de datos.

Para Camacho, el delito informático es toda acción dolosa que provoca un perjuicio a persona o entidades, sin que necesariamente conlleve un beneficio

material para su autor o que, por el contrario, produzca un beneficio ilícito a su autor aun cuando no perjudique de forma directa o inmediata a la víctima, y en cuya comisión intervienen necesariamente de forma activa dispositivos habitualmente utilizados en las actividades informáticas. Por su parte, Rafael Fernández Calvo define al delito informático como "la realización de una acción que, reuniendo las características que delimitan el concepto de delito, se ha llevado a cabo utilizando un elemento informático o telemático contra los derechos y libertades de los ciudadanos definidos en el título 1 de la Constitución Española.

Al respecto, es preciso tener en cuenta lo manifestado por Dávara, en el sentido de que generalmente concurren determinadas características comunes a todas las conductas catalogadas como delitos informáticos que nos permiten clasificarlas de acuerdo con la función y actividad que se realiza para cometerlos. Estos delitos poseen unas especialidades que los hacen más difíciles de detectar. Y aun detectados, no son denunciados por múltiples razones, y si son denunciados son difíciles de perseguir. Todos ellos centran su principal actividad en el acceso y/o la manipulación de datos —que se encuentran en soportes informáticos— o de programas de ordenador utilizados en su procesamiento (1993:322).

Debido a su gran vastedad y especialidad, la tarea de tipificación de esta clase de delitos resulta una labor muy complicada, siendo necesario delimitar con mucha precisión las características adecuadas de la criminalización de estas conductas y, por sobre todo, el bien jurídico afectado, como base de la sistematización. Adicionalmente a ello, "debe encuadrarse la problemática de la prueba de la comisión de los delitos informáticos, con su descubrimiento y comprobación mediante la Auditoria Informática" (Falconí Pérez, 1991:253).

> En tal sentido, podemos apreciar que contemporáneamente 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 (denominado "delito informático", "delito electrónico", "delito relacionado con las computadoras", "crímenes por computadora" o "delincuencia relacionada con el ordenador"). 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 muchos 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.
> (Carlos Correa y otros 1987:295).

Por ello, bien dice Tiedemann 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 nadie (1999:23).

El Derecho Penal debe también prevenir la comisión de este tipo de hechos, que de ninguna manera pueden ser entendidos como errores involuntarios, pues son realizados por personas que generalmente están familiarizadas y especializadas en el trabajo con computadoras, por lo que fácilmente pueden conocer cómo entrar en los archivos de datos de cualquier individuo.

El Derecho Penal 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 (el desarrollo actual y moderno nos ha traído avances importantes para la humanidad, pero es penoso que vengan acompañados de hechos delictivos no deseados).

III. TIPIFICACIÓN Y CLASIFICACIÓN

Conforme a la definición genérica de la Organización para la Cooperación Económica y el Desarrollo, delito informático *(computer crime)* 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:

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.

f) Ofensas tradicionales en los negocios asistidos por computador.

Por otro lado (en su clasificación), los tipos de delitos informáticos reconocidos por Naciones Unidas son:

1. Fraudes cometidos mediante manipulación de computadoras:

a. Manipulación de los datos de entrada

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

b. Manipulación de programas

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

c. Manipulación de los datos de salida

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

d. Manipulación informática

Aprovecha las repeticiones automáticas de los procesos de cómputo. Es una técnica especializada que se denomina "técnica salami" o "técnica del salchichón", en la que "rodajas muy finas", apenas perceptibles de transacciones financieras, se van sacando repetida y automáticamente de una cuenta y se transfieren a otra.

2. Falsificaciones informáticas:

a. Como objeto

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

b. Como instrumento

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

3. Daños o modificaciones de programas o datos computarizados:

a. Sabotaje informático

Es el acto de borrar, suprimir o modificar sin autorización funciones o datos de computadora con inten-

ción de obstaculizar el funcionamiento normal del sistema. Las técnicas que permiten cometer sabotajes informáticos son: "virus", "gusanos" o "bomba lógica o cronológica".

b. Acceso no autorizado a servicios y sistemas informáticos

Ello por diversos motivos, desde la simple curiosidad, como en el caso de muchos piratas informáticos (*hackers*), hasta el sabotaje o espionaje informático. El acceso se efectúa a menudo desde un lugar exterior, situado en la red de telecomunicaciones, recurriendo a diversos medios. El delincuente puede aprovechar la falta de rigor de las medidas de seguridad para obtener acceso o puede descubrir deficiencias en las medidas vigentes de seguridad o en los procedimientos del sistema. A menudo, los piratas informáticos se hacen pasar por usuarios legítimos del sistema; esto suele suceder con frecuencia en los sistemas en los que los usuarios pueden emplear contraseñas comunes o contraseñas de mantenimiento que están en el propio sistema.

c. Reproducción no autorizada de programas

Esta puede entrañar una pérdida económica sustancial para los propietarios legítimos. El problema ha alcanzado dimensiones transnacionales con el tráfico de esas reproducciones no autorizadas a través de las redes de telecomunicaciones modernas.

4. Los delitos informáticos también pueden ser clasificados en atención a los siguientes criterios:

a. Como instrumento o medio

Comprendiendo a las conductas criminógenas que se valen de las computadoras como método, medio o símbolo en la comisión del ilícito. Ejemplo: los falsificadores de tarjetas de crédito, billetes y/o documentación oficial (debiendo agregar a los equipos que emiten hologramas oficiales de verificación y de tenencias).

b. Como fin u objeto

En esta categoría se enmarcan las conductas criminógenas que van dirigidas en contra de la computadora, accesorios o programas como entidad física. Para ejemplificar este criterio quiénes si no los crackers y los hackers, que han revolucionado a los programas de seguridad y se han convertido en un filtro más en la efectividad del desarrollo de software especializado.

Con respecto al tema, el derecho comparado informa la necesidad actual de combatir esta especial forma delictual, con medidas jurídico-penales especializadas que trasciendan los moldes tradicionales del derecho punitivo y permitan la necesaria adopción de medidas legislativas precisas y oportunas. En los Estados industriales de Occidente, existe un amplio consenso sobre estas valoraciones, que se refleja en las formas legales de los últimos diez años.

Pocos son los países que disponen de una legislación adecuada para enfrentar tal problemática.

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

- Espionaje de datos (202 a).

- Estafa informática (263 a).

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

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

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

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

En lo que se refiere a la estafa informática, la formulación de un nuevo tipo penal tuvo como dificultad

principal el hallar un equivalente análogo al triple requisito de acción engañosa, causación del error y disposición patrimonial en el engaño del computador, así como en garantizar las posibilidades de control de la nueva expresión legal, quedando en la redacción que el perjuicio patrimonial que se comete consiste en influir en el resultado de una elaboración de datos por medio de una realización incorrecta del programa, a través de la utilización de datos incorrectos o incompletos, mediante la utilización no autorizada de datos o a través de una intervención ilícita.

Sobre el particular, cabe mencionar que esta solución en forma parcialmente abreviada fue también adoptada en los países escandinavos y Austria.

El legislador alemán ha introducido un número relativamente alto de nuevos preceptos penales, pero no ha llegado tan lejos como los Estados Unidos. De esta forma, observan los especialistas, no solo ha renunciado a tipificar la mera penetración no autorizada en sistemas ajenos de computadoras, sino que tampoco ha castigado el uso no autorizado de equipos de procesos de datos, aunque tenga lugar de forma cualificada.

En el caso de Alemania, se ha señalado que a la hora de introducir nuevos preceptos penales para la represión de la llamada criminalidad informática, el Gobierno tuvo que reflexionar acerca de dónde radicaban las verdaderas dificultades para la aplicación del Derecho Penal tradicional a comportamientos dañosos en los que desempeña un papel esencial la introducción del proceso electrónico de datos, así como acerca de qué bienes jurídicos merecedores de protección penal resultaban así lesionados.

Fue entonces cuando se comprobó que, por una parte, en la medida en que las instalaciones de tratamiento electrónico de datos utilizadas para la comisión de hechos delictivos, en especial en el ámbito económico, pueden conferir a estos una nueva dimensión, en realidad tan solo constituyen un nuevo modus operandi que no ofrece problemas para la aplicación de determinados tipos.

Por otra parte, sin embargo, la protección fragmentaria de determinados bienes jurídicos ha puesto de relieve que estos no pueden ser protegidos suficientemente por el derecho vigente contra nuevas formas de agresión, que pasan por la utilización abusiva de instalaciones informáticas. Las diversas formas de aparición de la criminalidad informática propician además la aparición de nuevas lesiones de bienes jurídicos merecedoras de pena, en especial en la medida en que el objeto de la acción puedan ser datos almacenados o transmitidos o se trate del daño a sistemas informáticos.

En Austria, la ley de reforma del Código Penal del 22 de diciembre de 1987 contempla los siguientes delitos: destrucción de datos (personales, no personales y los programas), estafa informática (causar perjuicio patrimonial a un tercero influyendo en el resultado de una elaboración de datos automáticos a través de la confección del programa, por la introducción, cancelación o alteración de datos, o por actuar sobre el curso del procesamiento de datos). Además contempla sanciones para quienes cometen este hecho utilizando su profesión.

En Francia, la ley número 88-19 del 5 de enero de 1988 regula el fraude informático, tipificando las conductas de acceso fraudulento a un sistema de elaboración de datos (se sanciona tanto el acceso al sistema como al que se mantenga en él y aumenta la sanción si de ese acceso resulta la supresión o modificación de los datos contenidos en el sistema o resulta la alteración del funcionamiento del sistema), sabotaje informático (impedir o falsear el funcionamiento de un sistema de tratamiento automático de datos), destrucción de datos (introducir —intencionalmente y con menosprecio de los derechos de los demás— datos en un sistema de tratamiento automático o suprimir o modificar los que este contiene o los modos de tratamiento o de transmisión), falsificación de documentos informatizados y uso de documentos informatizados falsos.

En Estados Unidos es importante mencionar la adopción, en 1994, del Acta Federal de Abuso Computacional (18 U.S.C. Sec. 1030), que modificó el Acta de Fraude y Abuso Computacional de 1986 (con la finalidad de eliminar los argumentos hipertécnicos acerca de qué es y qué no es un virus, un gusano, un caballo de Troya, etc., y en qué difieren de los virus). La nueva acta proscribe la transmisión de un programa, información, códigos o comandos que causen daños a la computadora, al sistema informático, a las redes, información, datos o programas. La nue-

va ley es un adelanto porque está directamente en contra de los actos de transmisión de virus.

El acta de 1994 diferencia el tratamiento a aquellos que de manera temeraria lanzan ataques de virus, de aquellos que lo realizan con la intención de hacer estragos. El acta define dos niveles para el tratamiento de quienes crean virus, estableciendo para aquellos que intencionalmente causen un daño por la transmisión del virus el castigo de hasta diez años en prisión federal más una multa, y para aquellos que lo transmitan solo de manera imprudencial, la sanción fluctúa entre una multa y un año en prisión. La referida acta de 1994 precisa también que el creador de un virus no podrá escudarse en el hecho de que no conocía que con su actuar iba a causar daño a alguien o que él solo quería enviar un mensaje.

En opinión de los legisladores estadounidenses, la nueva ley constituye un acercamiento más responsable al creciente problema de los virus informáticos, específicamente no definiendo a los virus sino describiendo el acto para dar cabida en un futuro a la nueva era de ataques tecnológicos a los sistemas informáticos en cualquier forma que se realicen. Diferenciando los niveles de delitos, la nueva ley da lugar a que se contemple qué se debe entender como acto delictivo.

En el Estado de California, en 1992 se adoptó la Ley de Privacidad, en la que se contemplan los delitos informáticos pero en menor grado que los delitos relacionados con la intimidad, que constituyen el objetivo principal de esta ley.

Consideramos importante destacar las enmiendas realizadas a la sección 502 del Código Penal, relativas a los delitos informáticos, en las que, entre otras, se amplían los sujetos susceptibles de verse afectados por estos delitos, la creación de sanciones pecuniarias de $10,000 por cada persona afectada y hasta $50,000 el acceso imprudencial a una base de datos, etc. El objetivo de los legisladores al realizar esta enmienda, según se infiere, era la de aumentar la protección a los individuos, negocios y agencias gubernamentales de la interferencia, daño y acceso no autorizado a las bases de datos y sistemas computarizados creados legalmente. Asimismo, los legisladores consideraron que la proliferación de la tecnología de computadoras ha traído consigo la proliferación de delitos informáticos y otras formas no autorizadas de acceso a las computadoras, a los sistemas y a las bases de datos, y que la protección legal de todos sus tipos y formas es vital para la protección de la intimidad de los individuos, así como para el bienestar de las instituciones financieras, de negocios, agencias gubernamentales y otras relacionadas con el Estado de California que legalmente utilizan esas computadoras, sistemas y bases de datos.

Es importante mencionar que en uno de los apartados de esta ley se contempla la regulación de los virus (*computer contaminant*) conceptualizándolos, aunque no los limita a un grupo de instrucciones informáticas comúnmente llamados virus o gusanos, sino que contempla otras instrucciones designadas a contaminar otros grupos de programas o bases de datos, a modificar, destruir, copiar o transmitir datos o a alterar la operación normal de las computadoras, los sistemas o las redes informáticas.

En Gran Bretaña, debido a un caso de *hacking* en 1991, comenzó a regir la *Computer Misuse Act* (Ley de Abusos Informáticos). Mediante esta ley, el intento, exitoso o no, de alterar datos informáticos es penado con hasta cinco años de prisión o multas. Esta ley tiene un apartado que especifica la modificación de datos sin autorización. Los virus están incluidos en esa categoría. Liberar un virus tiene penas desde un mes a cinco años, dependiendo del daño que estos causen.

En los países latinoamericanos no existe una legislación específica al respecto. En Argentina no encontramos la tipificación de los delitos informáticos, solo están protegidas las obras de bases de datos y de software, agregados a la lista de ítems contemplados por la ley 11.723 de propiedad intelectual, gracias al decreto número 165/94 del 8 de febrero de 1994.

Por su parte, en Chile (que fue el primer país latinoamericano en sancionar una ley contra delitos informáticos <7 de junio de 1993>) se prevé 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 ellas, para 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 ella, en la base, sistema o red.

Como puede apreciarse, la problemática de los delitos informáticos requiere un estudio especial y conocimiento técnico-científico para poder cumplir con la labor de tipificar suficientemente estos delitos, con vista a una adecuada protección social, pues 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.). Es necesario prepararse para prevenir y reprimir este tipo de conductas, puesto que, de acuerdo al axioma de la "auditoria", todo ilícito que tenga la más mínima posibilidad de ocurrir ocurrirá inexorablemente si no se 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.).

Todo ello nos permite decir 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. Esto en razón de que ha llegado ya el momento que el Derecho Penal rompa su moldura rígida clásica y evolucione conjuntamente con el desarrollo del conocimiento científico, para permitir así la real protección de la seguridad y la sociedad, ya que al parecer es anticuado en este aspecto de los delitos informáticos.

En nuestro sistema penal, que no tiene suficientemente desarrollado el tema, los delitos informáticos tienen su radio de acción principalmente en los atentados contra los derechos de autor, violación de la intimidad personal, falsificación de documentos informáticos, ofensas al pudor, violación de la intimidad y las comunicaciones, fraude informático electoral, entre otros. En el campo de los delitos patrimoniales, podemos apreciar que nuestro texto punitivo tipifica ciertas conductas posibles de ser cometidas mediante medios informáticos, tales como el hurto agravado que utiliza 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).

IV. TRATAMIENTO LEGISLATIVO NACIONAL: La tipificación inicial

En atención a los vacíos legales existentes en esta materia tan especializada, es que mediante la disposición introducida por ley 27309 de fecha 17 de julio del 2000, se modifica el título V, del libro segundo del C{odigo Penal, insertando un nuevo capítulo (Capítulo X), denominado **"Delitos Informáticos"**, que, como apreciamos en su oportunidad, solo tipificaron un sector parcial de este género delictivo, orientado específicamente al ámbito patrimonial; **por lo que debió denominárseles con más propiedad: "delitos informáticos patrimoniales".**

De manera similar al texto patrio, el proyecto de "ley de informática" del Ministerio de Justicia de Chile (abril de 1986) 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".

El título contenía la siguiente clasificación típica (que ya fue derogada por la ley 30096):

• Instrusismo informático	(primera parte)	Art. 207-A
• Fraude informático	(segunda parte)	Art. 207-A
• Sabotaje informático		Art. 207-B
• Circunstancias agravantes		Art. 207-C
• Tráfico ilegal de datos (Ley 30096; 19-08-13)		Art. 207-D

Dado que en general estos delitos precisaban en su materialidad el reproche a quien utilizaba o ingresaba indebidamente a una base de datos, sistema o red de computadoras o cualquier parte de ella, 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, **la identificación del BIEN JURÍDICO PROTEGIDO, exigía tener presente la ubicación legislativa de estos delitos,** que se insertaron en título V, del libro segundo del Código Penal referido a la protección del patrimonio económico, insertando un nuevo capítulo X, (Delitos Informáticos), lo que permitía concluir en que el bien jurídico tutelado es el "patrimonio", desde la perspectiva del derecho a la propiedad que tiene el sujeto pasivo a su base de datos, sistema o red de computadoras.

No obstante, es necesario precisar que en general se tratan de delitos pluriofensivos, porque atentan no solo contra el patrimonio, sino también contra el orden económico, el sistema informático, la libertad e intimidad personal y la titularidad del derecho intelectual, entre otros (que es la orientación de la nueva legislación de delitos informáticos).

Respecto de las características típicas de los delitos tipificados, podemos observar las siguientes:

EL INTRUSISMO INFORMÁTICO: se tipificaba como un tipo doloso de mera actividad y de peligro, en el que para su consumación resultaba suficiente que el sujeto haya ingresado o utilizado indebidamente la base de datos o sistema de computadoras, sin necesidad de un resultado material separable de la conducta (aventura, curiosidad, etc).

EL FRAUDE INFORMÁTICO: que en esencia viene a ser una modalidad del intrusismo informático motivado por *animus lucrandi*, lo que denotaba la presencia de un tipo de tendencia interna trascendente. Esta modalidad, conocida también como "estafa informática", corresponde a un tipo de mera actividad y de peligro.

El SABOTAJE INFORMÁTICO: la conducta se verificaba con la mera actividad intrusista dolosa, animada por la intencionalidad dañosa por parte del agente (*cracker*), de datos y/o programas del ordenador. "Con el fin de alterarlos, dañarlos o destruirlos", refería el tipo penal.

EL TRÁFICO ILEGAL DE DATOS: que sancionaba a quien ingresaba o utilizaba indebidamente una base de datos sobre una persona natural o jurídica, identificada o identificable, para comercializar, traficar, vender, promover, favorecer o facilitar información relativa a cualquier ámbito de la esfera personal, familiar, patrimonial, laboral, financiera u otro de naturaleza análoga, creando o no perjuicio (conducta de tráfico ilegal de datos, tipificada hoy en el art. 6 de la Ley de Delitos Informáticos, dentro de los "delitos informáticos contra la intimidad y el secreto de las comunicaciones").

EL TIPO AGRAVADO:

Se presentaba solo para las formas intrusistas, cuando:

a) El agente accedía a una base de datos, sistema o red de computadoras haciendo uso de información privilegiada, obtenida en función de su cargo.

b) El agente ponía en peligro la seguridad nacional.

V. TRATAMIENTO LEGISLATIVO NACIONAL: La tipificación introducida por la nueva ley

En un desenlace accidentado, pues el proyecto de ley original (proyecto Beingolea) fue abruptamente cambiado en su esencia, el Pleno del Congreso de la República, en la sesión del 12 de setiembre de 2013, aprobó (por unanimidad) la ley N° 30096, publicada el 22 de octubre del 2013 en el Diario Oficial El Peruano.

Dicha ley, que básicamente sigue los postulados del Convenio de Budapest, introduce en nuestro sistema punitivo los denominados "delitos informáticos".

Declarativamente, la ley tiene por objeto prevenir y sancionar las conductas ilícitas que afectan los sistemas y datos informáticos y otros bienes jurídicos de relevancia penal, cometidas mediante la utilización de tecnologías de la información o de la comunicación, con la finalidad de garantizar la lucha eficaz contra la ciberdelincuencia (art. 1).

En este contexto, introduce, en sus diferentes capítulos, la siguiente sistemática:

CAPÍTULO II DELITOS CONTRA DATOS Y SISTEMAS INFORMÁTICOS Artículo 2. Acceso ilícito Artículo 3. Atentado contra la integridad de datos informáticos Artículo 4. Atentado contra la integridad de sistemas informáticos

CAPÍTULO III DELITOS INFORMÁTICOS CONTRA LA INDEMNIDAD Y LIBERTAD SEXUALES Artículo 5. Proposiciones a niños, niñas y adolescentes con fines sexuales por medios tecnológicos.

CAPÍTULO IV DELITOS INFORMÁTICOS CONTRA LA INTIMIDAD Y EL SECRETO DE LAS COMUNICACIONES Artículo 6. Tráfico ilegal de datos Artículo 7. Interceptación de datos informáticos.

CAPÍTULO V DELITOS INFORMÁTICOS CONTRA EL PATRIMONIO Artículo 8. Fraude informático.

CAPÍTULO VI DELITOS INFORMÁTICOS CONTRA LA FE PÚBLICA Artículo 9. Suplantación de identidad.

CAPÍTULO VII DISPOSICIONES COMUNES A LOS DELITOS INFORMÁTICOS Artículo 10. Abuso de mecanismos y dispositivos informáticos Artículo 11. Agravantes.

VI. DELITOS INFORMÁTICOS CONTRA EL PATRIMONIO

El artículo 8 de la "ley de delitos informáticos" tipifica una sola modalidad de delitos informáticos contra el patrimonio, al cual se rotula con el nomen iuris de "fraude informático":

> "El que, a través de las tecnologías de la información o de la comunicación, 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 manipulación en el funcionamiento de un sistema informático, será reprimido con una pena privativa de libertad no menor de tres ni 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".

El tipo coincide con lo normado por el artículo 8 de la Convención de Budapest, que bajo el membrete de "fraude informático", exhorta a que los Estados signatarios tipifiquen como delito los actos deliberados e ilegítimos que causen perjuicio patrimonial a otra persona mediante:

a. La introducción, alteración, borrado o supresión de datos informáticos.

b. Cualquier interferencia en el funcionamiento de un sistema informático, con la intención, dolosa o delictiva, de obtener de forma ilegítima un beneficio económico para uno mismo o para otra persona.

6.1. El bien jurídico protegido

La identificación del bien jurídico protegido exige tener presente la orientación político-criminal asumida por el legislador y plasmada en la ley sobre delitos informáticos, que en este extremo hace referencia a delitos informáticos "patrimoniales", elemento normativo que alude a los delitos que atentan contra el patrimonio, tipificados en el título V, del libro segundo del Código Penal, referidos a la protección del patrimonio económico (aunque en doctrina asumen carácter pluriofensivo, ya que concomitantemente afectan también contra el orden económico, el sistema informático, la libertad e intimidad personal, la titularidad del derecho intelectual, entre otros).

En tal sentido, el bien jurídico patrimonio es concebido como el derecho a la preservación del patrimonio económico que le asiste al sujeto pasivo, y que comprende el conjunto de bienes, materiales e inmateriales, susceptibles de valoración económica

que posee una persona (incluso el Estado), bajo la protección del ordenamiento jurídico y sobre el cual tiene la facultad de ejercer todos los derechos inherentes a la propiedad (propiedad, posesión, uso, disfrute, y los demás derechos inherentes a la propiedad), sin otra limitación que no sea derivada de la ley, la administración de justicia o el contrato.

De esta manera, el bien jurídico tutelado en este tipo de delitos informáticos es el "patrimonio", desde la perspectiva del derecho a la propiedad que tiene el sujeto pasivo a su base de datos informáticos y/o al adecuado funcionamiento de un sistema informático.

Conforme a la ley de delitos informáticos, se entiende:

Por sistema informático: todo dispositivo aislado o conjunto de dispositivos interconectados o relacionados entre sí, cuya función, o la de alguno de sus elementos, sea el tratamiento automatizado de datos en ejecución de un programa.

Por datos informáticos: toda representación de hechos, información o conceptos expresados de cualquier forma que se preste a tratamiento informático, incluidos los programas diseñados para que un sistema informático ejecute una función.

6.2. Tipicidad objetiva

El sujeto activo es genérico, el tipo no exige condición y/o cualidad específica. En igual sentido, el sujeto pasivo es también genérico, lo será el titular del derecho patrimonial informático (el tipo simple sitúa a cualquier particular como sujeto activo, mientras que el tipo agravado coloca al Estado en tal condición, cuando se afecta su patrimonio, en relación con los recursos económicos destinados a fines asistenciales o programas de apoyo social).

La ley tipifica el denominado "fraude informático", que en su materialidad reclama que el agente, a través de las tecnologías de la información o de la comunicación, procure para sí o para otro un provecho ilícito en perjuicio de tercero, mediante el diseño, introducción, alteración, borrado, supresión, clonación de datos informáticos o manipulación en el funcionamiento de un sistema informático.

La alusión al término "fraude" podría inducir a interpretar que esta modalidad delictiva reclame típicamente un acto fraudulento, en el sentido de la necesidad que el autor implemente una conducta engañosa que induzca al error en su víctima, pero no es así como debemos interpretar el contenido típico, que en realidad se refiere a la modalidad de "fraude o estafa informática", concebida como un acto de intrusismo orientado a la obtención de un beneficio económico.

No obstante, el carácter doloso del tipo permite que el comportamiento fraudulento pueda integrarse a esta modalidad delictiva (ello al modo del artículo 248 del Código Penal español, que tipifica como estafa la conducta de quien con ánimo de lucro y valiéndose de alguna manipulación informática o artificio semejante, consiga la transferencia no consentida de cualquier activo patrimonial en perjuicio de un tercero).

La nueva norma excluye así la modalidad del simple intrusismo del texto derogado, que ha sido incorporado como delitos contra datos y sistemas informáticos (arts. 2 <acceso ilícito> y Art. 3 <atentado contra la integridad de datos informáticos>). Igualmente, se excluye del contexto patrimonial el delito de sabotaje informático, que se ha incorporado en la nueva ley como delito de atentado contra la integridad de sistemas informáticos (art. 4).

La amplitud del tipo permite incorporar el denominado "hurto electrónico", que se encontraba legislado en la segunda parte del artículo 186.3 del Código Penal y que ha sido derogado mediante la ley de delitos informáticos.

La acción material no recae sobre el aspecto extrínseco del ordenador o computador, denominado hardware (que como aparato físico, ya se encuentra protegido en otras figuras delictivas: hurto, robo, apropiación ilícita, daños, etc.), sino sobre su aspecto intrínseco, que contiene su sistema de soporte lógico, identificado con el concepto del software (que es el conjunto de instrucciones o expresiones que tienen como finalidad dotar al ordenador o computador de la capacidad de actuación determinando sus posibilidades de uso y aplicaciones concretas) (Núñez).

Se trata de un tipo de resultado material, que se consuma cuando el agente, motivado por el animus

lucrandi, afecta los datos informáticos o el funcionamiento de un sistema informático de tercero.

En tal sentido admite la tentativa, así como la coautoría y la participación delictiva.

6.3. TIPICIDAD SUBJETIVA

El tipo se representa como eminentemente doloso (dolo directo), se excluye la modalidad culposa que resulta atípica.

La norma presupone como condición objetiva de punibilidad que el comportamiento intrusista esté orientado a procurar, para sí o para otro, un provecho ilícito en perjuicio de tercero, exigiéndose de esta manera que el comportamiento esté motivado por un especial animus lucrandi, que debe comandar el inicio y desarrollo de la acción.

En tal sentido, el tipo asume carácter de tipo de tendencia interna trascendente.

VII. BIBLIOGRAFÍA

ABANTO VASQUEZ, Manuel (2000) *Derecho Penal Económico*. Lima: Idemsa.

ARBULU MARTINEZ, Víctor (2002) *Temas de Derecho Informático*. Lima: UNMSM

BACIGALUPO, Enrique (1994) *Estudios sobre la parte especial del Derecho Penal* (2da. edición). Madrid.

BAJO FERNANDEZ, Miguel (1991) *Manual de Derecho Penal*. Madrid: Centro de Estudios Ramón Areces.

BERNALES BALLESTEROS, Enrique (1996) *La Constitución de 1993: Análisis Comparado*. Lima: ICS.

BLOSSIERS MAZZINI, Juan José y CALDERON GARCIA, Silvia B. (2000). *Los delitos informáticos (en la Banca)*. Lima: RAO.

BRAMONT ARIAS TORRES, Luis Alberto (1977). *El Delito Informático en el Código Penal Peruano*. Lima: PUCP.

BUSTOS RAMIREZ, Juan (1986). *Manual de Derecho Penal*. Lima: Ariel.

CORREA, Carlos M. y otros (1987). *Derecho Informático*. Buenos Aires: Depalma.

DAVARA, Miguel Ángel (1993). *Derecho Informático*. Madrid: Aranzandi.

DURAND VALLADARES, Raúl (2002). *Cyber Delito o Delitos de Ordenadores Sistema Bancario Nacional*. Lima: Grafi Net.

FALCONÍ PÉREZ, Miguel (1991). *Protección Jurídica a los Programas de Computación*. Lima: Edino.

FERREYRA CORTEZ, Gonzalo (1990). *Virus en las Computadoras*. México: Macrobit.

HUGO VIZCARDO, Silfredo Jorge (2013). *Delitos Contra el Patrimonio* (3ra. edición). Lima: Pro Derecho Investigaciones Jurídicas.

LAMAS PUCCIO, Luis (1993). *Derecho Penal Económico, aplicado al Código Penal*. Lima.

MAZUELOS COELLO, Julio F. (2001). "Los Delitos Informáticos: Una Aproximación a la Regulación del Código Penal Peruano". En *Revista Peruana de Doctrina y Jurisprudencia Penales 2*.

MUÑOZ CONDE, Francisco (2002) *Teoría General del Delito*. Bogotá: Temis.

REYNA ALFARO, Luis M. (2002). *Manual de Derecho Penal Económico*. Lima: Gaceta Jurídica.

SCHONE, Wolfgang (1992). *Acerca del Orden Jurídico Penal*. San José: Juricentro.

TIEDEMANN, Klaus (1985) *Poder Económico y Delito*. Barcelona: Ariel.

TIEDEMANN, Klaus (1999). *Temas de Derecho Económico y Ambiental*. Lima: Idemsa.

VILLA STEIN, Javier (1998). *Derecho Penal*. Lima: San Marcos.

ZAFFARONI, Eugenio Raúl (1983). *Tratado de Derecho Penal*. Buenos Aires: Ediar.