Introducción a los Delitos Informáticos en la Legislación Peruana*

JUAN MANUEL HURTADO FALVY
Alumnos del octavo ciclo de la
Facultad de Derecho de la
Pontificia Universidad Católica del Perú.

"Lo más importante es dar lo mejor de uno y disfrutar haciéndolo"

Russell Baker

I. INTRODUCCION

"Sorry, I hacked you"Este cordial mensaje apareció en la pantalla de todos los usuarios que escribieron el 14 de abril de 1999 el nombre de dominio[1] correspondiente a una dirección electrónica del sistema abierto de Internet. Al "otro lado de la pantalla" los ejecutivos de Sound & Tell Co. no compartieron el mismo sentido del humor del carismático cracker, y no era para menos, su página establecida en la red a través del World Web Wide tuvo imposibilitado el acceso a sus potenciales clientes alrededor del mundo por doce horas durante el mencionado día. Recordemos que dicha corporación registra un promedio de ventas a través de la red de treinta mil dólares diarios sin contar los beneficios obtenidos por el alquiler de espacios publicitarios en su *web site.*

A fin de milenio presenciamos la agonía de diversos medios tradicionales de interrelación personal como el correo , con sobre, papel y cartero, las oficinas de archivos o la venta de bienes en vitrina de locales establecidos fisicamente. frente al apogeo de la nueva era informática, donde, como señaló el vicepresidente de Estados Unidos Al Gore, "El que no está en Internet, no existe". Actualmente el procesamiento y transmisión digitalizado de la información se ha convertido en el eje central de la actividad diaria de millones de personas, principalmente en las sociedades donde los sistemas informáticos les permite obtener una marcada ventaja frente a sus competidores, al desarrollar su actividad de una manera mas eficiente, organizando su información (contabilidad, proyectos, programas, correo, cartera de clientes, etc.) y facilitando el acceso e intercambio de datos en el mercado (ampliando el universo de clientes, agilizando la comunicacion, ahorrando costos en intermediarios) de una manera mas rápida y eficaz.

Algunos países han podido involucrarse en mayor proporción en este desarrollo estableciendo notorias diferencias frente a otros, principalmente en el plano

* A mi padre, Carlos Alavedra.

1 Denominación adoptada por el titular de un determinado sitio en La Red.Está conformada por distintos niveles separados por un signo de puntuación.El primer nivel contado de derecha a izquierda suele hacer referencia a la procedencia geográfica de la página (por ejemplo,la sílaba pe señala Perú), el segundo nivel hace referencia al tipo de organización (así: gov corresponde a las organizacione gubernamentales; com a las instituciones comerciales; net a los servicios de proveedores de network, etc), el tercer nivel está formado generalmente por una palabra que guarda estrecha relación con la actividad desarrollada en la página (suele ser su nombre comercial) esto se escribirá al lado de las letras http (que no forman parte del nombre de dominio) siglas de Hyper Text Transfer Protocol y sólo cuando la página este establecida a través de la Worl Web Wide se escribirá las iniciales www.

2 En la actualidad existen en el país 140,000 conexiones a intemet, que, aunque posibilitan el acceso a sólo el 2% de la población (cifra reducida en comparación al 38% de la población en EEUU y al 17% en la Unión Europea) es el resultado de un incremento de mas del 1000% en los últimos 6 años.

económico.Es en estos países de mayor desarrollo tecnológico donde nacen los primeros cuestionamientos a la existencia de protección-jurídica-penal de la información manejada en los sistemas El Perú aislado por la inflación y el terrorismo durante muchos años se vio imposibilitado de acoger la nueva tecnología en su nacimiento[2]. Hoy lentamente se toma conciencia respecto a las infinitas posibilidades ofrecidas en este campo, lo cual aumenta la concentración de las operaciones a través de estos sistemas generando una gran dependencia en ellos llegando incluso, a ser vitales para poder subsistir en el mercado. Es esta información la que se convierte en parte del patrimoni[3] de las personas. Bajo esta arriesgada premisa intentamos presentar en las próximas líneas una aproximación a las novísimas formas de actuaciones ilícitas que afectan la operatividad de los sistemas informáticos y el ámbito de protección que ofrece la legislación peruana ante ellas.

II. GENERALIDADES DE UNA COMPUTADORA

La PC (personal computer) debe su nombre a IBM, pero comparte los mismos elementos entre todos los fabricantes de computadoras personales los cuales son a nuestro interés, el hardware que es la parte física del sistema (el monitor, el mouse, el teclado,etc.) y la parte intangible denominada software constituída por los programas y utilidades (aquí encontramos los sistemas operativos que traducen nuestras órdenes para que puedan ser desarrolladas, tales como el windows, word, access,etc.). La computadora para poder funcionar utiliza su memoria ROM, mientras que para iniciar un programa se necesitará utilizar parte de su memoria RAM, esta permitirá almacenar los datos que utiliza el programa,por ello algunas computadoras que no tienen suficiente capacidad de memoria no puedan hacer funcionar los programas que les permitan estar interconectados.

Una gran ventaja de las computadoras es que nos permite trabajar en base a programas predeterminados donde podemos introducir información y archivarla para nuestra utilidad, existen para este fin dos clases de unidades de almacenamiento; los discos magnéticos entre los cuales se encuentra el disco duro (instalado en forma permanente en el interior de la computadora ,depositario del software que ella utiliza) y el floppy disk (disco flexible), conocido como diskett cuya capacidad es sumamente restringida.El disco magnético es la otra clase de soporte que permite almacenar la información, El CD-ROM tiene una capacidad de almacenamiento de datos de mas de 450 veces que el diskett.

"Junto a los avances informáticos han surgido nuevas conductas delictivas que perjudican el normal funcionamiento de los sistemas afectando así a las personas que desarrollan actividades a través de ellas"

En la actualidad esta información puede ser intercambiada con otra computadora, en cualquier lugar del mundo gracias a la interconexión. La Red es el conjunto de computadoras interconectadas entre sí. Esto se hace vía telefónica a través de un servidor que está conectado permanentemente quien realizará las interconexiones. Como se puede colegir ninguna computadora puede tener la suficiente memoria que le permita hacer trabajar un software que pueda ordenar toda la información que se desenvuelve en La Red, es por ello que se utilizan múltiples servidores.

Lamentablemente junto a los avances informáticos han surgido nuevas conductas delictivas, cometidas por hombres, que perjudican el normal funcionamiento de los sistemas afectando así a las personas que desarrollan actividades a través de ellas.

3 Completos trabajos sobre el tema han sido desarrollados por autores españoles como Gutiérrez Francés,Mariluz,Universidad de Salamanca. 1994.ROMEO CASABONA,Carlos María.,Delitos Patrimoniales en conexión con sistemas infomáticos y de telecomunicación. Facultad de Derecho de Zaragoza, Zaragoza,1989. y del mismo autor Poder Informático y seguridad Jurídica.Madrid,1987

III. SOBRE LOS DELITOS INFORMÁTICOS

Cuando el estratega militar chino Sun Tzu reveló las pautas a desarrollar en el Arte de la Guerra (pautas que son ampliamente citadas y utilizadas en diversos niveles competitivos en que se desenvuelven las relaciones humanas) aseguró que un sabio líder conoce los movimientos del oponente a través de los cinco espías básicos (el local, el interno, el contraespía, el muerto y el vivo quien regresará a informarle) Definitivamente este gran filósofo nunca se imaginó que dos mil años mas tarde existirían "espías" que podrían captar,alterar o destruir la información valorada por las empresas a kilómetros de distancia sin dejar el menor rastro que les permita ser identificados.Ellos son quienes constituyen una verdadera amenaza al soporte lógico de las computadoras, a la información contenida en ellas así como a las actividades que dependen del normal funcionamiento del sistema.

Para el Departamento de Justicia Norteamericana, delito informático es cualquier acto ilegal en relación con el cual el conocimiento de la tecnología informática es esencial para su comisión, investigación y persecución. De otro lado la Organización para la Cooperación Económica y el Desarrollo los define como "cualquier conducta no ética, o no autorizada, que involucra el procesamiento automático de datos y/o la transmisión de datos". Al respecto Miguel Gómez[4] señala que un delito informático es el conjunto de comportamientos dignos de reproche penal que tienen por instrumento o por objeto a los sistemas o elementos de técnca informática, o que están en relación significativa con ésta, pudiendo presentar múltiples formas de lesión de variados bienes jurídicos.

Es oportuno señalar que numerosas clasificaciones doctrinales se basan en distinguir los delitos informáticos a partir de dos criterios: como instrumento (o medio) u como fin (u objeto). Nosotros en cambio; clasificamos las acciones cometidas por estas personas susceptibles de ser consideradas como Delitos Informáticos, a partir de las acciones cometidas sobre los sistemas por cuanto consideramos que la información, el elemento lógico del sistema, se constituye en sí misma como un bien materia de protección jurídica.

3.1. Delitos de Captación de información

Es todo acceso no autorizado a la información contenida en los sistemas. Esta actuación suele constituirse en una etapa previa hacia la comisión de un delito mayor. Se puede dividir en:

3.1.1. Hacking[5]

La intrusión busca una satisfacción moral, interna o un reconocimiento social.

3.1.2. Espionaje Electrónico

El acceso es motivado por el interés de lograr una ventaja económica de la información obtenida.

A modo de ejemplo podemos señalar la violación del correo electrónico o la obtención indebida de claves de acceso de los usuarios.

3.2. Delitos de Destrucción de Información

Busca impedir, al titular o a la persona autorizada, el normal acceso de los programas informáticos al inutilizarlo destruir el soporte lógico de un sistema computacional. Estos a su vez pueden ser dos tipos:

3.2.1. Sabotaje de Datos

Impide el normal acceso a los datos almacenados,como sucede al borrar documentos sobre contabilidad, planes de inversión, cartera de clientes, etc.

4 GÓMEZ PERALS, Miguel.Los Delitos Informáticos en el Derecho Españo EN Informática y Derecho N° 4. setiembre 1992.
5 Suele diferenciarse al hacker del cracker en la medida de que éste último a pérdido toda filosofía o principio de conocer y explorar buscando únicamente satsfacciones económicas o la inutilización de los sistemas.

3.2.2. Sabotaje de Programas

Impide el normal acceso a los sistemas informáticos, por ejemplo, eliminar archivos de Word, Excel, etc

Estas acciones pueden ser realizadas por quien tenga un acceso físico directo a la unidad o ejecutadas a distancia a través de un virus informático[6]. En el Perú los virus pueden ser creados en media hora por quien tenga un mínimo de conocimiento de computación debido a la abundante información que se puede conseguir para ello en la red[7]. Los casos más comunes son los macrovirus anexados (attached), sucede cuando se recibe un mensaje de un correo electrónico familiar con un archivo anexado, y en consecuencia el usuario al intentar abrir el archivo adjunto, está convirtiendo a su computadora en portadora de un virus.

3.3. Delitos de Alteración de Información

Son los delitos de manipulación no autorizada de la información en provecho del agente o de un tercero. Así, tenemos entre ellos:

3.3.1. Alteración Informátic

Modificación de la información contenida en los sistemas, puede comprender una previa destrucción de la misma.

3.3.2. Estafa Electrónica

Es habitual encontrar esta modalidad clasificada en un rubro independiente[8]. Por nuestra parte, consideramos al igual que Ventura Monfort[9], que existe una gran proximidad entre la estafa y el hurto,produciendo infracciones penales conexas en el ámbito informático, por ello a nuestra razón lo relevante es la manipulación informática no autorizada de los sistemas de procesamiento de datos que generará como consecuencia que se le prive al titular de la disponibilidad de su bien.

Entonces pues, la estafa informática no es otra cosa que la manipulación informática no autorizada realizada con el fin de provocar en el sistema, usuario o en el servidor un error que origina una "transferencia" patrimonial.

a. Técnica del Salami: es la modificación de las instrucciones del programa con el fin de realizar transferencias no autorizadas de dinero (por lo general en sumas muy pequeñas) de unas cuentas a otras .Un ejemplo común es el Redondeo que consiste en llevar los decimales de las cuentas a cero, así, una que tenga en su haber S/ 9'163,657. 15 al ser manipulada queda con S/ 9'163,657.10 cifra que pasará imperceptible , pero que sumadas a otras podrían ser exorbitantes.

b. Datos Falsos: se modifican las instrucciones con el fin de que las operaciones de ingreso o salida de dinero se destinen a una cuenta no autorizada.También se puede buscar confundir al programa sobre la identidad del verdadero dueño del dinero.

3.3.3. El Hurto Electrónico

Modificación no autorizada de la información para

6 Este nombre fue dado en 1986 por Fred Cohen a los programas que pueden modificar a otros para incluir una copia posiblemente evolucionada, de sí mismos hasta el infinito, clasificándolos como Trojan Horse (Caballo de Troya) y Worms (gusanos). Aunque estos programas se remontan hacia 1942 cuando por primera vez John Von Newman presentó unos con la capacidad de multiplicarse y esparcirse en la memoria sin la intervención del programador, fue recién hacia 1987 cuando los virus mostraron su poder destructivo al aparecer Brain, el primer virus para PC con sistema operativo MS-DOS.

7 Estadísticas actuales señalan que el 95% de los virus nacionales lo conforman la familia de macrovirus de Word y Excel, cifras lógicas si tenemos en cuenta que cualquier estudiante de sistemas conoce el Visual Basic (lenguaje en que son creados los macrovirus). Según Network Associates y McAfee Antivirus. Huesped no deseado. P.12 En PC WORLD Lima. N193 Mayo 1999.

8 Así lo considera: BARRIUSO RUIZ, Carlos.Interacción del Derecho y la Informática, Madrid,1996.p.245-252. JOVER PADRÓ,Josep. El código penal de la informática, Pamplona,1997.p.360-365.DAVARA RODRÍGUEZ,Miguel Angel.Manual de Derecho Informático.Pamplona:Arazandi,1997, entre otros.

9 VENTURA MONFORT,Joaquín.La estafa cometida mediante la utilización de medios informáticos.Castellón 1997.

obtener bienes ajenos.Nos referimos al "robo de tiempo", "suplantación de personalidad" o la copia ilegal de programas en el caso de por ejemplo, las adquisiciones directas, esto último sucede, a raíz de que el comercio electrónico a través de Internet puede realizarse en forma indirecta cuando se adquieren bienes materiales que necesitan un posterior envio y en forma directa, cuando se venden servicios o información sin necesidad de realizar los clásicos trámites aduaneros. La venta de música o libros que necesitarán ser grabados o impresos por el comprador en su propia unidad constituye un ejemplo de venta directa. En estos casos existe la posibilidad de acceder ilícitamente a los programas que manejan estos servicios y obtener en beneficio propio o de un tercero los bienes ofrecidos. La tendencia actual es considerar el comercio de un producto digitalizado como un servicio donde el mayor valor agregado se encuentra en haber convertido precisamente el bien en un producto digitalizado.

Una vez presentado una aproximación al conocimiento de los delitos informáticos intentaremos exponer el ámbito de protección que ofrece la legislación peruana al respecto.

IV. LOS DELITOS INFORMÁTICOS EN LA LEGISLACIÓN PERUANA

Es preciso resaltar que nuestra Constitución consagra al Principio de Legalidad como una garantía fundamental para toda persona, (principio recogido a su vez por el artículo II del Título Preliminar del Código Penal) así pues, al señalar que *"nadie será procesado ni condenado por acto u omisión que al tiempo de cometerse no esté previamente calificado en la ley,de manera expresa e inequívoca, como infracción punible, ni sancionado con pena no prevista en la ley"* nos obliga a actuar cautelosamente al encuadrar estos actos que atentan contra la información (manejada a través de la informática), como tipos penales regulados explícitamente en la legislacion. No se puede permitir interpretaciones extensivas.

Defendemos lo antes señalado, al referirnos que la información se constituye en un bien valorable que amerita protección jurídica por cuanto constituye en un primer momento una necesidad para el desenvolvimiento económico de su titular así como, una ventaja competitiva de la empresa que le permite una mejor posición en el mercado. A continuación examinaremos los tipos penales que hacen referencia a los delitos informáticos.

4.1. Delitos contra el Patrimonio

> *"En el sentido clásico, por apoderarse se entiende toda acción de poner bajo el dominio y disposición inmediata de una persona un bien que antes se encontraba en la esfera de custodia de otra, donde podemos notar que lo relevante del comportamiento es la existencia de la sustracción del bien del lugar donde se encuentra"*

Como ya hemos señalado el Hardware está constituido por toda la parte material de los sistemas informáticos, todo lo tangible, sobre este punto no hay discusión alguna encontrándose toda acción ilícita que se cometa contra ella perfectamente regulada por el Código. Lamentablemente no se a considerado la diferencia en el valor económico que puede existir entre el soporte material y el software que es la parte lógica, intangible. Son a éstos programas a los que nos remitimos a continuación.

4.1.1. Hurto

"El que, para obtener provecho, se apodera ilegítima-mente de un bien mueble, total o parcialmente ajeno, sustrayéndolo del lugar donde se encuentra [...]

Se equiparan a bien mueble la energía eléctrica, el gas , el agua y cualquier otra energía o elemento que tenga valor económico, así como el espectro electromagnético."

El comportamiento tipificado consiste en apoderarse ilegítimamente de un bien mueble, sustrayéndolo del lugar donde se encuentra, en donde, ha sido tradicionalmente entendido, por bien mueble, todo objeto del mundo exterior con valor económico, que sea susceptible de apoderamiento material y de desplazamiento[10].

En el sentido clásico, por apoderarse se entiende toda acción de poner bajo el dominio y disposición inmediata de una persona un bien que antes se encontraba en la esfera de custodia de otra, donde podemos notar que lo relevante del comportamiento es la existencia de la sustracción del bien del lugar donde se encuentra. La dificultad nace en encuadrar al patrimonio informacion, como elemento que pueda ser objeto del requisito "desplazamiento"[11] que comprende la sustracción, sin referir a su soporte material (diskette o papel) teniendo en cuenta que hoy en día se puede acceder indebidamente a información ajena a kilómetros de distancia.

Ante la aplicación del "apoderamiento" a estos supuestos , habrá que preguntarnos si concuerda con la intención de la norma o si está realizando un cambio completo del lenguaje jurídico creando un nuevo tipo penal.

Sobre el agravante:"*si el hurto es cometido: mediante la utilización de transferencia electrónica de fondos, de la telemática en general, o la violación del empleo de claves secretas*", es preciso mencionar que se tipifica el uso indebido de los sistemas informáticos como medio para la comisión de un delito, el hurto de los fondos, interesante y previsora respuesta del legislador; empero, ahora nos interesa la acción cometida contra la información en sí.

4.1.2. Estafa

"El que procura para sí o para otro un provecho ilícito en perjuicio de tercero, induciendo o manteniendo en error al agraviado mediante engaño, astucia, ardid u otra forma fraudulenta..."

Esta forma tradicional de estafa difiere del concepto manejado de estafa informática[12] en la medida que para esta última ya no es relevante el engaño ni el error en la persona engañada, ahora hablamos de soportes informáticos, que trabajan sobre la base de información preestablecida en su memoria. La estafa electrónica se centra en la manipulación informática para obtener un provecho, punto que no prevé nuestro ordenamiento.

4.1.3. Daños

"El que daña destruye o inutiliza un bien, mueble o inmueble....."

Una vez mas nos encontramos frente a problemas de lenguaje jurídico. Es evidente que el legislador del 91 no proyectó la avalancha informática desarrollada en todo el quehacer cotidiano en nuestro país en los últimos años. Es difícil encontrar en este tipo penal la intención de distinguir la parte material de la parte intangible, así, sólo podríamos recurrir a este supuesto, cuando se halla producido un daño contra el soporte físico de la computadora mas no frente a daños ocasionados a los programas, los cuales pueden, por ejemplo, ser mucho más valiosos que los pocos soles que cuesta un CD que los almacene.

DELITOS CONTRA LA LIBERTAD

Es oportuno señalar que a consecuencia del avance informático surgen nuevas conductas delictivas que tienen por objeto a estos sistemas o que utilizan a éstos como medio para la comisión de delitos, queremos poner énfasis en que es al primer supuesto al

10 MUÑOZ CONDE, Derecho Penal.Parte Especial. 9ed.Valencia:Tirant lo blanch.1993,BRAMONT-ARIAS,Luis.Manual de Derecho Penal 2ed. Lima:San Marcos.1996,BUSTOS RAMÍREZ,Juan.Manual de Derecho Penal.Parte Especial..Barcelona:Ariel.1986

11 BRAMONT-ARIAS,Luis.op.cit.,p.265

12 Al respecto vease:los conceptos de fraude y estafa manejado por BARRIUSO RUIZ,C opcit,JOVER PADRÓ,J op.cit, , VENTURA MONFORJ op.cit. y GUTIERREZ FRANCÉS,M..Fraude Informático y Estafa.enpublicaciones del ministerio de justicia.Madrid.1991

que se ocupa este estudio, si para ello se utiliza tecnología informática es un punto secundario.

Violación de la Intimidad

El artículo 154 pretende proteger la intimidad personal y familiar como garantía de un ámbito de no intervención en la vida privada, reservándose así sólo la calidad de sujeto pasivo a la persona o a la familia a la que se viola la intimidad siendo común encontrar posiciones que acuerdan en señalar que una persona jurídica no puede gozar de esta calidad[13].

Si quisieramos considerar al artículo 157 que hace referencia al "uso indebido" de cualquier archivo que contenga datos, esto sólo sería aplicable a la información almacenada referente a personas naturales y como es lógico, si se desea cierto grado de intimidad no estarán expuestas a través de estos sistemas informáticos.

Violación del Secreto de las Comunicaciones

El artículo 161 abarca el comportamiento consistente en abrir o apoderarse de una comunicación que no le esté dirigida abarcando así parte de los supuestos que estudiamos en la medida que los datos contenidos en los sistemas hallan sido transmitidos.

Al proteger el secreto en las comunicaciones en los artículos 161 y 162 palabras como "cualquier otro documento análogo" o "similar" respectivamente, pueden englobar al correo electrónico o el "chat" si entendieramos como la posibilidad de acceso a estos datos el abrir o interferir. Lamentablemente el artículo 163 no lo toma en cuenta, por lo tanto un comportamiento dirigido a hacer desaparecer el contenido de un e-mail sería impune.

Violación del Secreto Profesional

"El que, teniendo información por razón de su estado, oficio, empleo, profesión o ministerio, de secretos cuya publicación pueda causar daño, los revele sin consentimiento del interesado..."

La tutela penal de la intimidad de este artículo puede extenderse también a los datos reservados de las personas jurídicas cubriendo aquellos supuestos en los cuales los encargados, bajo una relación laboral, de las operaciones informáticas dan a conocer tales secretos.

Quedará por establecer, entonces, qué sucede cuando el acceso a esta información lo realizan personas totalmente ajenas al interesado, hasta que punto se puede distinguir cuando una información es realmente valiosa y cuando se puede convertir su divulgación en un daño.

Delitos contra los Derechos Intelectuales

El objeto de protección penal está representado por el derecho de los inventores a que se respete y reconozca el resultado de su creación intelectual[14]. Esto es, a que se protejan las invenciones y los signos distintivos que ellos han creado, así en opinión preponderante[15] el derecho nace con el registro, por lo tanto siempre debe mediar la resolución correspondiente para tal efecto.

Es oportuno tomar en cuenta como nos lo recuerda Prado Saldarriaga[16], que la protección jurídica de estos derechos se estructuran en función de disposiciones extrapenales. Estas normas las podemos encontrar en la Constitución(Art.2, num.8), en la Decisión 344 del Acuerdo de Cartagena referido al régimen

13 BRAMONT-ARIAS,A.op.cit. , p.177
14 PRADO SALDARRIAGA,Victor.Derecho Penal.Lima:San Marcos.p.260
15 BAJO FERNANDEZ,Miguel.Manual de Derecho Penal.Parte esoecial. Madrid: CEURA.1987.p.235.BUSTOS RAMIREZ,J.op.cit.p.252.
16. PRADO SALDARRIAGA,Victor.op.cit.p.261

común sobre propiedad industrial para los países andinos, en el Convenio de París para la protección de la propiedad industrial, en el Código Civil (arts.18, 884 y 886 num.6) y en los decretos legislativos 822 y 823 referidos a la Ley sobre el Derecho de Autor y a la Ley de Propiedad Industrial respectivamente.

Es interesante señalar que estas leyes como el Decreto Legislativo 822 protege, entre otros,la base de datos entendida como la compilación de obras, hechos o relatos en forma impresa, en unidad de almacenamiento de ordenador a partir de su concepción como creación intelectual(art. 78) . Así también la Ley de Propiedad Industrial protege(entre otros elementos constitutivos de la propiedad industrial) en su Título VIII a los secretos profesionales contra la revelación, adquisión o uso en la medida que la información tenga un valor comercial efectivo o potencial por ser secreta centrando su objetivo al ciclo de los productos y a la prestación de los servicios. En ambos casos encontramos ciertos vacíos (como los casos de sabotaje contra la información) pero lo que centra nuestra atención es que sólo se protege derechos de naturaleza creativa no la capacidad operativa de los sistemas ni la información como tal.

Si se pudiera medir una norma por su eficiencia para prevenir el ilícito diríamos que, por ejemplo, sólo en 1998 la piratería de software en el Perú generó pérdidas a las empresas titulares de los derechos por 18 millones de dólares.

Una vez más deseamos detenernos para resaltar que no es materia de nuestro análisis los delitos cometidos utilizando a los sistemas como instrumento para la comisión del ilícito, pues llegado el momento la evolución informática posibilitará que incluso se puedan cometer asesinatos utilizando estos medios (por ejemplo, el caso extremo de una persona que dependa de un sistema interconectado de respiración artificial).

De lo expuesto en línea anteriores y siguiendo los lineamientos de Rodrigues da Costa[17] podemos advertir que la velocidad del desarrollo tecnológico en el sector de la informática, no garantiza que se pueda, eternamente, mantener la aplicación de nuestras actuales normas, o sea , la subsunción de los delitos comunes en las conductas típicas de los delitos informáticos.

APUNTES GENERALES

Los sistemas informáticos han logrado cruzar el ámbito empresarial para instalarse en toda esfera de la vida humana, dependemos cada día más del adecuado funcionamiento de una computadora para cubrir todo tipo de necesidades, así,mientras más avance esta dependencia mas vulnerables estaremos frente a los "fantasmas" que se desenvuelven a través de los sistemas. Los llamamos así por la gran dificultad que existe para presentar pruebas que permitan inputarles la calidad de agentes de estos delitos informáticos.

Esta dificultad sumada a la común inacción de los agraviados, que por lo general prefieren evitar la divulgación de estas acciones que demuestran una cuestionable vulnerabilidad de sus sistemas de información, además de la dificultad de descubrir cuando se ha cometido un comportamiento ilícito nos llevan a pedir una regulación cautelosa y específica sobre el tema. Para ello podemos optar por dos caminos. reconocer que las acciones generadas sobre los sistemas informáticos y los datos contenidas en estos pueden estar relacionadas con figuras convencionales tales como, el hurto, estafa,violación del secreto de las comunicaciones, etc. pero al realizarse sobre éstos se precisa, en cada caso, un reanálisis de los elementos de la descripción legal, de la tipicidad; es decir, un reanálisis del texto de la norma vigente que conlleve a la modificación de ésta, haciéndola como bien señala Gómez Perez[18], apta para ser aplicada a esos actos humanos que se incrementan de forma directamente

17 RODRÍGUES DA COSTA,Marco Aurelio.El Derecho Penal Informático Vigente en Brasil.en Jus Navigandi.Uruguaiana
18 GOMEZ PEREZ:Mariana.Criminalidad Informática:un fenómeno de fin de siglo.EnRevista Electrónica de Estudios Jurídicos.Cuba

proporcional al desarrollo científico y técnico de la sociedad. El otro camino consistiría en crear un título especial en el Código Penal que comprenda estos tipos penales. Para el legislador capaz estos caminos no tienen por que ser cancelatorios.No compartimos la idea de crear una ley fuera del texto del Código Penal como la Ley Chilena N° 19.223 sobre Delitos Informáticos.

A contrario del pensamiento común del cual nace un rechazo inicial a toda norma importada por no adecuarse a la realidad del país, este es un delito globalizado cuyo comportamiento está uniformizado alrededor del mundo , por ello creemos conveniente un adecuado estudio de las leyes sobre delitos informáticos desarrollados en los últimos años en países tales como Francia, Noruega y Suecia entre otros, incluyendo a algunos de la región[19], para encontrar el adecuado marco jurídico pertinente aplicable al nuestro.

En todo caso es necesario tener en cuenta ciertos lineamientos básicos que deberán ser consideradas en una futura[20] y necesaria regulación normativa sobre los Delitos Informáticos:

a. Reconocer y distinguir la Información manejada por una persona que sea susceptible de tutela jurídica en la medida que forme parte de su patrimonio.

b. Establecer un claro y definido marco conceptual frente al término "apoderarse" si la nueva legislación buscara apoyarse en este término.

c. Tener presente que los sistemas informáticos ante los cuales se cometan los actos que serán tipificados como delitos involucran siempre a personas que ejercen el control de los mismos.

d. Debe referirse claramente al sistema de procesamiento de datos para diferenciar al soporte lógico de la parte material.

e. Recordar que no siempre el ingreso, alteración de datos, obtención de información, etc. se hará con el propósito de obtener un beneficio económico.

f. Comprender que el ilícito se puede desarrollar por etapas, así luego de un ingreso lícito a un sistema por haber sido admitido a él ,puede él o un tercero ajeno obtener información por medios ilícitos.

g. El daño a los sistemas operativos de una computadora puede realizarse por una actuación final del propio usuario, como sucede cuando es él quien introduce el virus en su computadora cuando abre un mensaje anexado al original que lo contiene o cuando entra a una página otorgando su propia identificación.

h. El daño a los sistemas y a la información manejada por éstos puede realizarse a través de un acceso físico directo (daños contra la parte física de una computadora que ocasionará como consecuencia la perdida de la información) o a través de otro sistema.

i. Los delitos pueden dirigirse al normal funcionamiento de una página web cuya localización física será cuestionable para definir el estado que tenga Juridicción.

19 Veáse además en España la Ley Orgánica para la Regulación del Tratamiento Automatizado de Datos(LORTAD)y el Código Penal, en Chile la Ley N° 19.233 de junio de 1993 con 4 artículos al respecto,en Brasil la Ley 7.646 de diciembre de 1987 y la Ley 8.137 dediciembre de 1990 y los proyectos de Ley N°15 2y 597 de 1991 que dispone sobre el delito de interferencia en los sistemas informáticos.y la inviolabilidad de los datos de la comunicacióndel usuario

20 Al término del presente artículo existen en el Congreso de la República del Perú tres proyectos de ley relativos a los sistemas informáticos:El Proyecto N° 5071 que propone acertadamente la creación de un nuevo capítulo dentro del Código Penal sobre los Delitos Informáticos aunque con ciertos vacios; El Proyecto N° 5132 que presenta cuatro artículos sobre Delitos Informáticos con poca claridad y el El Proyecto N° 5326 que pretende modificar el artículo 196° del Código Penal estableciendo pena para aquel que valiéndose de alguna manipulación informática consiga la transferencia no consentida de cualquier activo patrimonial en perjuicio de tercero.

CONCLUSIONES

1. Debemos reconocer que el avance tecnológico producido en los últimos años en nuestro país y que sin duda será mayor cada año, a logrado abarcar tantos aspectos de las relaciones humanas que un adecuado funcionamiento de los sistemas informáticos a devenido en convertirse en una necesidad para la vida en sociedad.

2. Es necesaria una adecuada protección de las conductas indebidas que afecten los sistemas informáticos, la integridad, confidencialidad y disponibilidad de la información.

3. En la actualidad no existe en la legislación penal peruana un adecuado marco normativo que abarque directamente a los delitos informáticos. Urge la aparición de un adecuado sistema de normas que garanticen la seguridad informática, por tanto esta nueva normatividad puede partir de un reanálisis del texto de la norma vigente que conlleve la modificación de ésta o de nuevas figuras delictivas formando un nuevo capítulo en el Código Penal.