Nociones básicas sobre los Delitos Informáticos

Guillermo Beltramone - Rodolfo Herrera Bravo – Ezequiel Zabale

Abogados

(Ponencia preparada en conjunto con los profesores argentinos Guillermo Beltramone y Ezequiel Zabale, y presentada en el X Congreso Latinoamericano y II Iberoamericano de Derecho Penal y Criminología, celebrado en la Universidad de Chile en agosto de 1998.

Introducción. Concepto. Categorías. Sujeto activo y pasivo. Nuevas formas delictivas. Perfiles. Cuestiones de Jurisdicción y Competencia. Algunos casos.

I.- Introducción.

La era de las comunicaciones, la materialización de la idea del mundo como una aldea global, el ciberespacio y las ciberculturas, y el impacto de las tecnologías de la información han implicado una transformación en la forma de convivir en sociedad.

Dentro de este marco de transformación, el cambio producido por el mal uso de la informática ha hecho que surjan nuevas conductas merecedoras del reproche social que, sin embargo, no siempre son fáciles de tipificar. Así, han surgido modalidades delictivas relacionadas con la informática.

En primer lugar, ciertas figuras típicas convencionales han empezado a realizarse mediante el empleo de las Tecnologías de las Información, es decir, ha comenzado a ser utilizada la informática como un medio de comisión específico. Dichas conductas pueden ser comprendidas dentro del tipo penal del delito produciéndose una informatización de un ilícito tradicional que ya está tratado en el Código Penal, por lo que no hacen necesaria la creación de nuevos tipos, y en el caso que no se ajusten completamente a la conducta descrita, bastaría con ampliar el tipo penal para actualizarlo. A estos delitos tradicionales le llamaremos Delitos Computacionales para distinguirlos de los Delitos Informáticos.

Pero además han surgido nuevas conductas, impensadas por el legislador de hasta hace medio siglo, que por su especial naturaleza no admiten encuadrarse dentro de figuras convencionales informatizadas sino que es necesario que se creen nuevos tipos. Son estos nuevos delitos a los que con propiedad llamaremos Delitos Informáticos.

Ahora bien, si deseamos seguir la tendencia del derecho comparado a evitar una "inflación penal", es decir, un crecimiento desmedido del Derecho Penal que vaya contra la tendencia hacia la reducción de la esfera punitiva, debemos entender que no toda conducta impropia relacionada con la informática merece el carácter de delito informático. Primero, sólo serán delitos los que se tipifiquen como tales en virtud del principio de legalidad. Segundo, es conveniente que solo las conductas más graves y preferentemente dolosas, se castiguen penalmente, dado el carácter de "última ratio", de último recurso de la pena dentro del sistema de control social, es decir, que solo una vez que las medidas sancionatorias civiles y administrativas han sido descartadas, las sanciones serán las penales.

Pero resulta innegable que estas nuevas conductas tienen un enorme disfavor para con el medio, causando perjuicios a terceros a veces en forma indeterminada, por ejemplo, perjudicando a una gran masa de usuarios.

Por lo tanto, son varias las cuestiones a resolver por la doctrina, como es el caso del concepto, tipología y clasificación de los delitos informáticos, el bien jurídico que protegen, los sujetos involucrados, el perfil criminológico, la internacionalización de las conductas típicas, por mencionar algunas.

II.- Concepto.

Aún no es fácil conceptualizar a los delitos informáticos por su novedad, variedad y complejidad. La doctrina no se apoya en un parámetro claro y común desde el cual comenzar los intentos de definición. No obstante, trataremos de despejar algunas confusiones habituales que nos permitan esbozar un concepto de delito informático, a nuestro juicio, apropiado.

Una primera idea al respecto la señala el profesor méxicano Julio Téllez Valdés, quien lo conceptualiza desde dos ópticas. Nos dice que desde un punto de vista atípico son "actitudes ilícitas en que se tiene al computador como instrumento o fin", y desde uno típico son "conductas típicas, antijurídicas y culpables en que se tiene a las computadoras como medio o fin"[1].

Esta primera idea es común en los textos del área, así por ejemplo, Nidia Callegari define al delito informático como "aquél que se da con la ayuda de la informática o de técnicas anexas".

[1] Téllez V., Julio; "Derecho Informático". Editorial McGraw-Hill, México, 1996. P. 104

Para Carlos Sarzana, el delito informático “es cualquier comportamiento criminógeno en que la computadora está involucrada como material, objeto o mero símbolo”.

María Cinta Castillo y Miguel Ramallo entienden que “delito informático es toda acción dolosa que provoca un perjuicio a personas o entidades en cuya comisión intervienen dispositivos habitualmente utilizados en las actividades informáticas”.

Por su parte, Lilli y Massa afirman que la locución “delito informático” puede entenderse en un sentido restringido y otro amplio. En su concepto restringido, comprende los hechos en que se atacan elementos puramente informáticos (independientemente del perjuicio que pueda causarse a otros bienes jurídicamente tutelados y que eventualmente puedan concurrir en forma real o ideal); mientras que en su concepto amplio abarca toda acción típicamente antijurídica y culpable para cuya consumación se utilizó o se afecta una computadora o sus accesorios.[2]

Estas definiciones deben ser precisadas para no inducir a error, ya que no todo ilícito en el que se emplee un computador como medio o instrumento para su consumación tendrá tal carácter, ya que puede tratarse de una figura típica tradicional informatizada a la que llamamos delito computacional.

Eso sí, aclaremos que no puede afirmarse que todo delito en el que interviene un computador como medio es un delito informático o un delito computacional, pues el uso que se le dé, debe ser el normal de acuerdo a su naturaleza. Por ejemplo, no sería un delito computacional las lesiones que se le causen a una persona golpeándolo con un monitor o un teclado, por ejemplo.

Por lo tanto, una primera conclusión que nos llevará a un concepto de delito informático es excluir de la definición a los delitos computacionales.

Ahora bien, teniendo claro que buscamos conceptualizar a conductas ilícitas nuevas, cometidas generalmente a través de equipos computacionales, pero en donde el elemento central no es el medio de comisión sino que es el hecho de atentar contra un bien informático, se hace necesario destacar que no todos los bienes informáticos son objeto de estos delitos.

Los sistemas de tratamiento automatizado de la información se basan en dos grandes tipos de soportes, el físico y el lógico. Así, por una parte, los bienes informáticos que dicen relación son el soporte físico conforman el hardware, es decir, los equipos computacionales, que son bienes corporales muebles como el procesador o la unidad central de proceso y los dispositivos

[2] Riquert, Marcelo A.; “Derecho penal e informática: una aproximación genérica a su ardua problemática”, Periódico Económico Tributario, Año V, Nº144, pág.2.

periféricos de entrada y salida, como por ejemplo, el monitor, el teclado, la impresora, un escáner, etc. En cambio, por la otra, existen bienes intagibles que constituyen el soporte lógico del sistema o software. Dentro de él están los datos digitalizados (es decir, transformados a un lenguaje computacional basado en un sistema binario o de base 2, en donde sólo existen dos cifras, los ceros y los unos), que se ingresan al computador para que sean procesados y puedan constituir información. Además, encontramos otros bienes informáticos como los programas computacionales, que son un conjunto de instrucciones para ser usadas directa o indirectamente en un computador a fin de efectuar u obtener un determinado proceso o resultado.

Pues bien, no todos los bienes computacionales son objeto de delitos informáticos. Contra el hardware o soporte físico se cometen o delitos convencionales o delitos computacionales (si usa como instrumento a la computación), pero no delitos informáticos, es decir, figuras nuevas no encuadrables en las ya existentes.

Si los equipos computacionales son bienes tangibles, corporales, muebles no hay inconvenientes para que se cometan en su contra los tradicionales delitos de hurto, robo o daños. De esta forma, descartamos la incorrecta idea que algunos autores sostienen en relación a calificar como delitos informáticos al hurto de un computador, el robo de un cajero automático, los incendios intencionales y atentados terroristas en contra de una central de computación, por ejemplo.

Es más, incluso empleando como medio de comisión a las tecnologías de la información no estamos en presencia de un delito informático, sino que en ese caso, de un delito computacional. Por ejemplo, el introducir un “virus físico o destructivo”, que altera el funcionamiento del sistema exigiéndolo más allá de sus capacidades logrando un sobrecalentamiento que acarrea que se queme, por ejemplo, el disco duro, la tarjeta de video o el monitor, es un delito de daños convencional informatizado o delito computacional.

Hay autores que clasifican estas conductas destinadas a destruir los elementos físicos del sistema dentro del sabotaje informático. Ellos justifican la penalización de tales conductas como delitos informáticos basados en la desproporción que existe entre el valor de los equipos y el perjuicio que implica la destrucción correlativa; en la impunidad de los autores favorecida por la detectabilidad del ilícito bastante tiempo después; y por la gran dificultad que presentan para valorar la real cuantía del daño producido en atención al valor del material destruido.

Si bien reconocemos que estas son características que pueden darse cada vez que se atenta contra un sistema de tratamiento de información, en ningún caso son elementos que justifiquen un tipo penal distinto al delito de daños. Sin duda, la información que se perderá en este

tipo de atentados tiene un valor estratégico muchas veces no comparable con el valor económico del hardware, sin embargo, esto también ocurre cuando se atenta contra archivos, registros, bibliotecas o museos, circunstancia que el legislador no considera suficiente como para crear un "delito bibliotecario" por ejemplo, pero sí reconoce su importancia incluyéndolo dentro del delito de daños calificados. En este caso, si la protección que otorga este delito convencional no es suficiente, debería mejorarse el tipo o la pena y no crear un delito específico nuevo.

Finalmente, ¿acaso el insertar un clip en el mecanismo de los computadores para causar cortocircuitos eléctricos, verter café, soluciones de sal y agentes de limpieza cáusticos sobre el teclado y en otros periféricos, arrojar humo, spray de pelo y otros gases dentro del mecanismo, provocar temperaturas extremas calentando partes del computador mediante cigarrillos merecen calificarse de manera distinta a un delito de daños? Creemos que no y por ello damos como segunda conclusión para llegar al concepto que el delito informático no atenta contra el hardware sino que contra el soporte lógico.

¿Por qué el atentar contra el soporte lógico puede ser calificado como delito informático? Porque la especial naturaleza intangible de los datos digitalizados y de los programas computacionales, no le permite al tipo penal tradicional cubrirlo haciendo necesaria la creación de un delito nuevo.

Precisamente, el profesor chileno Renato Jijena Leiva sostiene esta postura. Es más, piensa que la especial naturaleza de los programas computacionales no les permite estar ni siquiera incluidos en una clasificación tan general como la de cosas corporales e incorporales. Si definimos a los programas computacionales como un conjunto de instrucciones para ser usadas en un computador, no podrán ser percibidas por los sentidos, y por ende, no son cosas corporales. Y tampoco consisten en meros derechos, es decir, no son cosas incorporales. Se trataría de meros impulsos electromagnéticos que se transmiten a través de circuitos electrónicos no perceptibles por los sentidos del hombre (ya que lo que se observa en un monitor es el resultado obtenido con el procesamiento electrónico de las instrucciones).

Como consecuencia de ello, por ejemplo, penalmente no se podrían cometer delitos patrimoniales de hurto, robo o apropiación indebida, al copiar ilegalmente un programa computacional, puesto que no sería ni un documento ni una cosa corporal mueble. Al ser intangibles e inmateriales no se pueden aprehender físicamente, es más, al copiarlos ilegalmente no le son privados en forma permanente a la víctima del delito. Sólo una nueva figura delictiva, es decir, un delito informático, podría sancionar penalmente tales conductas.

Por lo tanto, la definición que consideramos más apropiada para los delitos informáticos es *"toda conducta que revista características delictivas, es decir, sea típica, antijurídica y culpable, y atente contra el soporte lógico de un sistema de procesamiento de información, sea sobre programas o datos relevantes, a través del empleo de las tecnologías de la información, y el cual se distingue de los delitos computacionales o tradicionales informatizados".*

Esta idea es compartida por el autor más prestigioso de Europa en relación a los delitos informáticos, el profesor alemán Ulrich Sieber, quien los define como *"todas las lesiones dolosas e ilícitas del patrimonio relacionadas con datos procesados automáticamente".*

De nuestra definición aclararemos para terminar este punto, que no todos los datos digitalizados merecen una protección penal (sí una protección civil o administrativa frente al mal uso que se les dé). Sólo los datos relevantes deben ser protegidos penalmente. Por ejemplo, en relación a los datos personales, sólo los datos sensibles deben protegerse creando delitos, es decir, aquellos datos que son muy personales y que permiten llegar a conformar un perfil del individuo que puede ser usado para discriminarlo, como su tendencia política, religiosa, sexual, historial médico, etc.

El punto será determinar qué parámetro se considerará para dar relevancia o no a un dato digitalizado.

III.- Categorías.

La categorización y clasificación de los fenómenos tiene siempre un aspecto pedagógico, pues a través de las mismas se pueden apreciar con mayor nitidez las diferencias y relaciones que existen entre los sujetos sometidos a la comparación.

Nos referiremos aquí a las categorías de delitos informáticos reconocidas por las Naciones Unidas[3] y que ha sido aceptada por la mayoría de la doctrina especializada. Naciones Unidas distingue tres tipologías de delitos informáticos, a saber:

1-.Fraudes cometidos mediante manipulación de computadoras.

Entre estos se encuentran la manipulación de datos de entrada y salida y la manipulación de programas. En cada caso, lo que se trata es de colocar datos falsos en un sistema u obtener los datos del sistema en forma ilegal.

2-.Falsificaciones Informáticas.

En este punto se trata de usar las computadoras como elemento para falsificar entradas, dinero, tickets o cuentas bancarias. Siendo coherentes con nuestra definición de los delitos informáticos debemos advertir que en este caso serían más bien, delitos computacionales.

3-.Daños a Datos Computarizados.

Aquí se ubican los virus, las bombas lógicas, los gusanos, accesos no autorizados, etc. Se trata, en general, de programas o accionares que de una u otra forma dañan la información de un sistema determinado.

Otra clasificación tradicional propuesta por el profesor alemán Klaus Tiedemann y compartida por Ulrich Sieber, hace incapié en la necesidad de distinguir entre los delitos informáticos de carácter económico (cuando se produce un perjuicio patrimonial) y los que atentan contra la privacidad (mediante la acumulación, archivo y divulgación indebida de datos contenidos en los sistemas informáticos).[4]

Nosotros podríamos inclinarnos por distinguir dentro de los delitos informáticos a los fraudes informáticos o manipulaciones indebidas de datos, el sabotaje y el espionaje informático, el hacking o acceso no autorizado y la piratería de software o copia ilegal de programas. Sin perjuicio de ello, las clasificaciones son muy diversas en doctrina.

IV.- Sujetos Activo y Pasivo.

Se entiende por sujetos del delito a las personas o grupo de personas que pueden cometer (sujeto activo) o ser afectados (sujeto pasivo) por la comisión de un hecho ilícito, en este caso particular, de un delito informático.

Sujeto activo puede ser cualquier persona física o natural. No creemos, en cambio, que puedan serlo las personas jurídicas teniendo en cuenta la naturaleza de las acciones involucradas.

---

[3] Puede verse la clasificación completa en http://www.onnet.es
[4] Riquert, Marcelo A.; op cit, pág.2.

Respecto del sujeto pasivo, queda claro que cualquier persona natural o jurídica puede ser objeto de alguna de las actividades ilícitas de las que denominamos aquí como "delito informático". Claro que para poder entrar en la categoría de sujeto pasivo deberá cumplirse con una condición relevante, como es la de ser titular de información de carácter privado y confidencial en formato digital, es decir, almacenada en un medio informático.[5] Con ello queremos significar que, así como no pueden ser sujetos pasivos del delito de homicidio un perro o un gato (por citar un ejemplo), de la misma manera no pueden ser sujetos pasivos de un delito informático quienes no posean información digital que revista un cierto valor que requiera su confidencialidad.[6] Incluso puede darse el caso de detentar información importante pero que no se encuentra en formato digital, o aún estando en formato digital el desapoderamiento de la misma se realiza por la fuerza física. En ambos supuestos no puede afirmarse la existencia de un sujeto pasivo de delito informático, sino simplemente de un robo o un hurto según como se tipifique la conducta.

V.- Nuevas Formas Delictivas.

Desde los albores de la humanidad, el hombre ha ido creando una larga serie de normas tendientes a regular la convivencia en sociedad. Pero como reza un viejo adagio "hecha la ley, hecha la trampa". Para defenderse de quienes intentan burlar la ley, el Derecho, a través de sus operadores en los diferentes campos, fue delineando diferentes soluciones y así surgen, entre otras, la figura de las presunciones, aquellas que no admiten prueba en contrario, etc.

Tales soluciones han producido excelentes resultados en áreas como las del Derecho Civil, Comercial o Laboral; pero que son de imposible aplicación en el Derecho Penal dado que, según lo establecen los modernos ordenamientos jurídicos, lo que no está prohibido está permitido[7] impidiendo la misma ley, de este modo, recurrir a la analogía, a la presunción de derecho o al fraude a la ley.

Llegado este punto debemos notar que cada ciertos ciclos el Derecho Penal se ve superado por la realidad, realidad que indica su desactualización como protector social y la necesidad de una reforma. Es aquí donde los códigos –y esto vale para todos- quedan vetustos y se ven superados por las circunstancias de hecho[8].

[5] Tradicionalmente se ha caracterizado al delito informático como aquél que está íntimamente ligado no sólo a la informática sino también a los bienes jurídicos relacionados con las tecnologías de la información: datos, programas, documentos electrónicos, dinero electrónico, información, etc.
[6] Estas características, fueron las que los legisladores argentinos tuvieron en cuenta para brindar un marco de protección legal a la información que poseían tanto las personas físicas como jurídicas al sancionar, en febrero de 1997, la denominada "Ley de Confidencialidad".
[7] No es otra cosa que la consagración de un principio básico del Derecho Penal liberal.

Las nuevas modalidades delictivas y las nuevas formas de comisión de delitos anteriores, que por diferentes razones se hace difícil perseguirse penalmente, son sentidas por la sociedad como criminógenas. Dentro de estas últimas, por citar solo un caso, una estafa es una estafa se haya cometido con papel o con un computador.

A continuación expondremos sobre algunas de las más modernas conductas no punidas por la ley[9] y sobre los sujetos que las cometen y que son entendidas por el derecho comparado como delitos informáticos.

1) Hacking.

La palabra "hacking" proviene del inglés "hack" que significa "hachar" y es el término que se utilizaba para describir la manera en que los técnicos telefónicos arreglaban las cajas descompuestas: a los golpes. Se denomina "hacking" en la jerga informática a la conducta de entrar a un sistema de información sin autorización, es decir violando las barreras de protección establecidas a tal fin.

El sujeto que realiza esta actividad es llamado hackers, muy rara vez se conoce su nombre verdadero y en mucho casos actúa y firma en grupo.

La actividad de hackear un sistema puede tener diferentes finalidades y alcances. Así, en la mayoría de los casos el romper el sistema o eliminar los pasos de seguridad de un sistema tiene por objeto ver, fisgonear el contenido y la información protegida, otras veces extraer copias de la información y muy raramente destruir o cambiar los contenidos de la información.

Respecto de esta ultima situación, es decir las entradas ilegales que tienen por objeto destruir el sistema, a esto se llama cracking y a los sujetos que lo realizan se los identifica como crackers. Esta es una expresión idiomática que se puede traducir como quebrar, es decir vencer las barreras de seguridad y romper lo que hay detrás de ellas.

En cualquiera de ambos casos, lo que caracteriza las andanzas de los sujetos es su entrada ilegal al sistema, entendiendo el concepto de entrada ilegal como la entrada de toda aquella persona que no tiene los password o no los ha conseguido por los caminos normales.

---

[8] Para el caso de la legislación argentina –por ejemplo- donde más se ha notado este fenómeno de desactualización normativa es en el Código de Comercio el cual se encuentra vacío de contenido. De la misma manera, el Código Penal aún preveé figuras tan absurdas como la del duelo.

[9] La Ley 19223 que tipifica en Chile delitos informáticos no ha sido muy afortunada. Cuenta con múltiples errores de forma y de fondo fundamentalmente. Entre ellos, algunos delitos que tipifica como "nuevos" son delitos computacionales únicamente, impone penas muy altas, no es coherente en su redacción, no se incorpora al cuerpo del Código Penal y no tipifica delitos informáticos muy comunes como el hacking o el fraude informático, por ejemplo.

2) Phreaking.

La actividad de phreaking es, sin duda, la más común de todas las llamadas actividades ilícitas informáticas.

Sin embargo es aquí donde se denota con máxima claridad las dificultades que se presentan al intentar dar una única definición de delitos informáticos y computacionales, tal como expondremos a continuación.

El phreaking –tanto así como quien lo desarrolla- es considerado un delito informático por la generalidad de los autores en la rama. Pero el phreaking es la actividad de obtener ventajas de las líneas telefónicas a los efectos de no pagar los costos de comunicación. Es decir que básicamente se trata de encontrar el medio para evitar pagar por el uso de la red telefónica ya sea ésta pública o privada, digital o inalámbrica.

Dentro de esta categoría se engloban las tarjetas de conteo[10], las blue box, los war-dialer, etc.

Pero adviértase que para estas actividades raramente se usa el computador, salvo para coordinar o elaborar los chips de tarjeta. Esta actividad es esencialmente extra PC, es telefónica, es más bien de ingeniería en electrónica y no de ingeniería en sistemas.

Esta simple sutileza no parece ser advertida por demasiados colegas que engloban a todas las actividades, es como confundir el hurto de ganado con el hurto de camiones de ganado.

Ello no quita que tales actividades están emparentadas, pues si se revisa en Internet[11] se verá que allí donde hay páginas de tipo “under” conviven los hackers y los phreakers sin inconvenientes y coadyuvándose los unos a los otros.

3) Carding.

Se llama carding a la actividad de cometer un fraude o una estafa con un número de tarjeta de crédito.

[10] Tarjetas telefónicas caseras que tienen la capacidad de recargarse
[11] Por solo mencionar una de las mejores paginas under en español puede verse www.islatortuga.com

Este concepto que parece simple tiene sus dificultades. Primero no todo fraude con tarjeta de crédito se transforma en carding, así si se roba o se encuentra una tarjeta y es utilizada por otra persona que no es su titular, ello no es carding es solo un fraude.

El carding consiste entonces en usar un número de tarjeta de crédito -ya sea real o creado de la nada mediante procedimientos digitales- para realizar compras a distancia por Internet y efectuar pagos.

El nivel de seguridad en Internet para realizar transacciones económicas no es bueno, por ello existen fugas de información, muchos usuarios de la red ponen su número de tarjeta de crédito para hacer compras, estos números son captados por otras personas que los reutilizan para hacer más compras sin ser los titulares de la tarjeta.

A esta actividad debe agregarse la de generar números válidos de tarjetas de crédito para luego usarlos en compras a distancias. Cuando una empresa de tarjetas asigna una tarjeta numerada a un usuario lo hace a través de un sistema automatizado de creación de números aleatorios. Por ello basta para crear números válidos usar el mismo sistema, ya que cualquier estudiante de ingeniería puede hacer un sistema de cálculo de números aleatorios.

El carding es una de las actividades más riesgosas dentro de las entendidas como delitos informáticos, pues si se quiere recibir lo que se compró hay que ordenar que lo manden a algún sitio, surgiendo el problema de determinar en qué lugar, pues quien compró con un número de tarjeta que no era suyo se arriesga a que en el ínterin lo descubran y al ir a recoger la cosa, lo arresten.

VI.- Perfiles.

Existe cierta corriente de opinión que trata de encasillar a los sujetos que realizan las actividades descritas precedentemente, tratando de dar un perfil criminógeno del mismo.

En la generalidad de los casos tales perfiles terminan siendo meras descripciones que rozan con el neolombrosiano. Nos preguntamos nosotros cómo es posible dar descripciones de los sujetos si no podemos siquiera definir qué es lo que hacen y son sujetos provenientes de culturas tan diferentes como la anglosajona, la hispana, la japonesa, etc.

Así por ejemplo, en el VI Congreso Iberoamericano de Derecho e Informática[12] se ha sostenido que el hackers es un tipo desaliñado, con lenguaje extraño, profesante de religiones oscuras, místicos, inteligentes, faltos de motivación, etc.

Tales descripciones no son sólo inútiles, pues la mitad de la población de Internet reúne al menos tres de las características expuestas con anterioridad, sino que además de ello, ¿a cuántos hackers conocen los autores?, ¿a cuántos han entrevistado o visto detenido? y ¿a cuántos les han hecho informes psicológicos como para determinar sus conductas?.

Creemos firmemente que tales lucubraciones sólo sirven para crear más confusión en un ambiente de por sí confuso, contribuyendo dichos perfiles (de la forma en que se están haciendo) más que a mistificar la figura de personas comunes que tienen un conocimiento avanzado en computación.

VII.- Cuestiones de Jurisdicción y Competencia.

La jurisdicción es entendida por la corriente privatística del Derecho Procesal como la potestad que tiene el Estado de administrar justicia, y más modernamente, como la función pública complementaria y sucedánea de la legislativa que tiene por finalidad resolver conflictos jurídicos mediante un proceso y con autoridad de cosa juzgada. La competencia, en cambio hace alusión a la organización del Estado para ejercer su jurisdicción, o como la define el Código Orgánico de Tribunales chileno es la facultad que tiene cada juez o tribunal para conocer de los negocios que la ley ha colocado dentro de la esfera de sus atribuciones. Tanto la competencia como la jurisdicción son territoriales, no se extienden más allá de sus fronteras y por ende, el Estado argentino, por ejemplo, no puede en principio perseguir penalmente a un ciudadano chileno. Y si bien reconocemos la existencia de tratados de extradición y de colaboración internacional, es claro que la potestad del Estado se limita a su territorio.

Anticipado el tema, surgen los interrogantes para el Derecho Penal Internacional quien deberá resolver las complejas situaciones que se generan a partir del accionar de los delincuentes informáticos teniendo en cuenta que, en la mayoría de los casos, se trata de delitos a distancia[13]. Supongamos que un país cualquiera modifica su código penal e incluye en éste como delito al acceso no autorizado a sistemas de información. Luego, un banco sufre un acceso no autorizado tendiente a obtener una transferencia indebida, se descubre quien accede, pero resulta

[12] Ponencia presentada por los Dres. Ricardo Levene y Alicia Chiaravolletti; libro de Ponencias del VI Congreso Iberoamericano de Derecho e Informática, pág. 123-147.
[13] Todos los actuales tratados y obras sobre la materia, caracterizan al llamado “delito a distancia”, como aquél en el cual la acción tiene lugar en una determinada jurisdicción, mientras que el resultado se produce en otra.

que el violador del sistema es un alemán que vive en Nueva Zelanda y que penetró en el sistema a través de un servidor que se encuentra en los Estados Unidos. La pregunta inevitable es: ¿podría el Estado en cuestión arrogarse la potestad de persecución del delito?

A fin de brindar alguna solución, hay autores que consideran que el juez penal puede intervenir por la sola circunstancia de que la infracción fue cometida en el territorio de su país. En pocas palabras, es el vínculo del territorio el que justifica la aplicación de la ley penal[14]. Sin embargo, este es sólo el comienzo de un apasionante tema a resolver por los juristas.

VIII.- Algunos casos.

En general, la mayoría de los ataques contra las computadoras ni siquiera se denuncian, algunos se minimizan y otros se niegan. Las razones pueden ser varias: las empresas e instituciones temen perder credibilidad frente a sus clientes si admiten que sus sistemas fueron violados o bien, sencillamente, algunos nunca llegan a enterarse de que sus computadores han sido víctimas de un delito informático.

Sin embargo, y pese a este escaso reconocimiento público, varios hechos han visto la luz sobre todo en países caracterizados por un mayor desarrollo tecnológico.[15] No puede decirse lo mismo de países como la Argentina en donde no se registran demasiados casos de delincuencia con medios informáticos que pasaron por ante los tribunales. La excepción podría ser en algunos aspectos puntuales como las maniobras ilegales con cajeros automatizados o en materia de piratería de software. Por otra parte, y como se vino sosteniendo a lo largo del presente trabajo, la ausencia de una legislación que pueda aplicarse específicamente al tema ha llevado a que "muchas de estas conductas queden sin una adecuada solución jurídico-penal, permaneciendo empantanados en la discusión sobre si las maniobras perpetradas por su intermedio configuran el delito de estafa o el de hurto".[16] Estas consecuencias fueron padecidas en uno de los pocos casos de hacking tratados por la justicia argentina cuando en diciembre de 1995, y tras una intensa investigación, se descubrieron las maniobras de un jóven de 21 años de edad que con su computadora en la Capital Federal logró violar el sistema de seguridad de la marina estadounidense. Sin una ley adecuada, el caso debió ser encuadrado en las clásicas figuras de defraudación e interrupción de las comunicaciones con penas absurdas dada la magnitud del hecho.

---

[14] Al respecto pueden verse las interesantes consideraciones de Michel Vivant a partir del análisis del derecho francés en su artículo "Ciberespacio: Los derechos y el derecho a las redes", en la revista Derecho de la Alta Tecnología, Nº112/113.

[15] Sin duda uno de los casos que mayor notoriedad ha adquirido a nivel mundial alimentado por el interés concitado por la prensa, fue el del norteamericano Kevin D. Mitnick, quién fuera acusado de ingresar sin autorización a decenas de computadoras de empresas, robar miles de expedientes de tarjetas de crédito y una fortuna en software. Curiosamente, Mitnick es una figura idolatrada por los hackers.

En el caso de Chile, luego de la dictación hace 5 años de la Ley 19223, supuestamente tipificadora de delitos informáticos, sólo se han interpuesto 3 querellas las cuales aún no han sido falladas.

IX.- Conclusión.

Luego de estas nociones introductorias a la delincuencia informática podemos establecer como síntesis lo siguiente:

1. Las relaciones entre el delito y la informática se han manifestado de dos formas: en los delitos computacionales, es decir, figuras penales tradicionales en las que se emplea como un especial medio de comisión a las tecnologías de la información; y los delitos informáticos, entedidos como nuevos ilícitos en los que, empleando la informática, se atenta dolosamente contra el soporte lógico de un sistema computacional (datos relevantes y programas).

2. La doctrina generalmente no distingue en forma clara estas diferencias, confundiéndolos, lo que implica dificultades mayores para la determinación de los bienes jurídicos protegidos, las penas y la técnica legislativa a utilizar, por ejemplo.

3. Las clasificaciones dadas por los autores a los delitos informáticos son variadas y diversas, pero frecuentemente se consideran los fraudes cometidos mediante la manipulación de datos o los daños causados a la información digitalizada, entre otros.

4. En cuanto a los sujetos involucrados destaca la necesidad de que la víctima posea información digitalizada de cierto valor. Por otra parte, han surgido nuevos tipos de delincuentes como los hackers, crackers y phreakers.

5. Este tipo de delincuencia informática no reconoce fronteras nacionales y crea dificultades para el Derecho Penal Internacional cuando los delitos son cometidos a distancia gracias a las redes computacionales. Éste, junto con el tema de la delincuencia informática en general, es un reto importante para los juristas si se busca lograr eficacia

[16] Riquert, Marcelo A.; op cit, pág.3.

en la prevención de estas conductas y en la represión de tales delitos, en miras a entregar un Derecho Penal actualizado y concordante con las necesidades del próximo siglo.

Santiago, Chile y Rosario, Argentina

Agosto de 1998.