COMENTARIOS CRÍTICOS A LA REFORMA DEL CÓDIGO PENAL QUE INTRODUCE LA LEY 9048 (SOBRE DELITOS INFORMÁTICOS EN EL DERECHO PENAL COSTARRICENSE)

Licda. Elízabeth Guerrero
Prof. Alonso Salazar

Resumen

En el siguiente texto se ahonda someramente en la conceptualización del delito informático y su tipología, para luego centrarse en una serie de Comentarios Críticos respecto a la modificación y creación de ciertos tipos penales que introduce una reforma al Código Penal Costarricense, mediante la promulgación de la Ley 9048 (Sobre Delitos Informáticos).

Abstract

In the following text, first the authors talk about the concept and types of cybercrime, then they focus on a number of Critical Comments regarding the modification and creation of certain types of crimes that introduces a Costa Rican Penal Code reform, by enacting Ley 9048 (Sobre Delitos Informáticos).

Palabras Clave

Delito Informático- Crimen por computadora- Código Penal Costarricense- Ley 9048

Keywords

Computer crime- Computer criminal crimen- Costa Rican Penal Code- Ley 9048

COMENTARIOS CRÍTICOS A LA REFORMA DEL CÓDIGO PENAL QUE INTRODUCE LA LEY 9048 (SOBRE DELITOS INFORMÁTICOS EN EL DERECHO PENAL COSTARRICENSE)

Licda. Elízabeth Guerrero
Prof. Alonso Salazar

Introducción

En las siguientes líneas se pretende aportar una serie de consideraciones críticas con respecto a la reforma del Código Penal que introduce la Ley 9048 (Sobre Delitos Informáticos). Lo anterior en razón de que a nuestro entender se perciben una serie de concepciones erróneas en cuanto a la determinación de las acciones que configuran un "delito informático", favoreciéndose con ello el aumento en la creación de tipos penales innecesarios, así como la aparición de problemas de orden técnico-jurídico que merece la pena destacar.

Delitos Informáticos

En la doctrina –básicamente internacional, aún y cuando hay algunos trabajos de orden costarricense al respecto-, no existe un acuerdo en cuanto al concepto de delito informático[1]. Es con base en lo anterior, que precisar una definición absoluta sobre

1 Téngase en consideración que en la dogmática se tomó primero el concepto „crimen por computadora", como tal hecho delictivo en el cual el instrumento u objetivo del hecho es la computadora. Sieber completó este concepto en forma importante con el concepto de „lesión patrimonial dolosa en el ámbito de la informática". De acuerdo a este concepto, el crimen por computadora contempla todas las lesiones patrimoniales dolosas que estén vinculadas de alguna forma con los datos almacenados en equipos de procesamiento de datos; y como modalidades delictivas se toman en consideración la manipulación de datos (ingreso de datos erróneos, cambio en los datos), el uso ilícito de equipos procesadores de datos (hurto de tiempo o de uso), así como la destrucción de datos (sabotaje de computadora). Esta limitación del crimen por computadora a la violación patrimonial fue criticada por Lampe, ya que diferentes casos conocidos no tuvieron relación alguna con intereses patrimoniales, sino que la violación se dio en relación con otros bienes jurídicos. Desde 1974 se habla de tener que cambiar el concepto „crimen por computadora" a „abuso por computadora", ya que el concepto es lingüísticamente incorrecto, discrimina el procesamiento de datos y solo sirve para efectos clasificatorios y de recopilación de casos. La computadora por si sola no puede ser criminal. Este concepto fue aceptado por Sieber y por los nuevos desarrollos en el ámbito de este tipo de criminalidad. Así, (Salazar Rodríguez, 2008) citando a Bundesministerium der Justiz, Lampe, Sieber, Lindemann citado por Sieber y Fischer. Para nuestros efectos, pese a las consideraciones supra indicadas, nos referiremos al término de delito informático pues ha de parecernos, en su consideración semántica, el que puede abarcar en mayor parte la cantidad de acciones delictivas que se pretenden penalizar mediante el tipo penal.

(Continúa en la siguiente página)

el delito informático[2] resulta ser una tarea pretensiosa y se escapa de nuestro objeto, preferimos citar algunas que simplemente faciliten al lector la comprensión del tema central de este escrito.

“podemos definir el delito informático como: acción delictiva que realiza una persona, con la utilización de un medio informático o lesionando los derechos del titular de un elemento informático, se trate de máquinas- hardware- o de los programas- software” (Dávara Rodríguez, 1993, citado en (Chinchilla Sandí , Delitos Informáticos. Elementos básicos para identificarlos y su aplicación , 2004))

“[delito informático es] la realización de una acción que, reuniendo las características que delimitan el concepto de delito, sea llevado a cabo utilizando un elemento informático y/o telemático, o vulnerando los derechos del titular de un elemento informático, ya sea hardware o software” (Davara Rodríguez, 1997)

“cualquier conducta ilegal, no ética, o no autorizada que involucra el procesamiento automático de datos y/o la transmisión de datos” (Organización de para la Cooperación Económica y el Desarrollo citada en (Davara Rodríguez, 1997))

“El concepto de abuso por computadora abarca comportamientos ilícitos, éticamente reprochables o prohibidos, en los cuales los datos informáticos son alterados dolosamente, tanto en el procesamiento como en la transmisión de datos. Bajo alteración de datos se entiende el cambio doloso de los mismos (manipulación por computadora), destrucción (sabotaje por computadora), su obtención y uso no autorizados (espionaje por computadora) y conjuntamente el uso no autorizado de equipos de cómputo (hurto de tiempo)” (Salazar Rodríguez, 2008)

De esta manera en un conjugado de todas estas definiciones se tiene que, el delito informático necesariamente se constituye por una acción que es ilícita, delictiva, no autorizada, ni ética cuya comisión recae en dos posibilidades:

(1) La primera, en la comisión de la acción ilícita se utiliza un medio informático, y

2 A modo de aporte al estudio, cabe destacar que antes de 1960 el concepto de „crimen por computadora“ (luego delito informático) casi no se trataba en la dogmática del derecho penal. Al inicio de las discusiones sobre el problema del crimen por computadora por ejemplo en Alemania se cuestionaba, si realmente un crimen como éste existía. Las discusiones sobre el abuso de las computadoras inician en la mayoría de los países en los años 60 con referencia al peligro de los derechos de la personalidad, el cual se define inicialmente en el rubro de la protección de datos, y no bajo el rubro de „crimen por computadora“. En los años 70 el interés aumentó y el crimen por computadora se definió como una nueva forma de criminalidad; en ese entonces se concentraba la ciencia jurídica dentro de los delitos económicos específicos de computadora, p.ej. manipulación por computadora, sabotaje por computadora, hacking por computadora, espionaje por computadora y robo de software. Actualmente el estado de la situación es totalmente diferente. Análisis empíricos no sólo en la República Federal de Alemania, sino también de Australia, Gran Bretaña, Japón, los Países Bajos, Austria, Suiza, Suecia, los Estados Unidos y una investigación de la Comunidad Europea, han ido demostrando la realidad de esta nueva forma de delito. El crimen por computadora aparece como un crimen que requiere de un tratamiento específico. Así, (Salazar Rodríguez, 2008). En las líneas mencionadas se citan autores como Tiedemann, Sieber, Möhrenschlager, Council of Europe y Passim.

(2) La segunda, producto de la comisión de la acción ilícita se afecta o produce un daño sobre dicho medio informático.[3]

Ahora bien, también están quienes consideran la configuración del delito informático desde (1) la perspectiva de la *computadora como objeto del hecho* y (2) la *computadora como recurso para el hecho*. Por un lado se menciona la computadora como objeto del hecho, cuando el delincuente tiene como meta del delito a la computadora, o sea, la intervención del delincuente es específicamente contra la computadora (p.ej. espionaje, sabotaje, daño de bienes, daño de datos). Por otro lado se menciona la computadora como recurso para un hecho, cuando el delincuente utiliza la computadora como recurso de intervención contra un bien jurídico protegido (p.ej. fraude por computadora)[4]. Pero es imperativo aclarar esta diferencia, ya que no todos los hechos en los cuales se utiliza una computadora, deben tomarse como crimen por computadora.

Ahora bien, la identificación de ambas posibilidades nos conecta simultáneamente con la perspectiva del *delito informático como medio y como fin*. Esta es precisamente la clasificación de los delitos informáticos que propone Téllez Valdés, misma que es expuesta por (Chinchilla Sandí, 2004) así:

- *Delitos informáticos como instrumento o medio*: los cuales se refieren a aquellas conductas criminales que se valen de las computadoras como método, medio o símbolo en la realización del ilícito.

  § En nuestra consideración esto se referiría a la comisión de la acción delictiva por medio del simple “USO DEL ORDENADOR”

- *Delitos informáticos como fin u objetivo*: los cuales se refieren a las conductas criminales que van dirigidas en contra de la computadora, accesorios o programas como entidad física, o bien el sujeto o autor del ilícito obtienen un beneficio perjudicando a un tercero.[5]

  § En nuestra consideración esto se referiría a la comisión de una acción delictiva que produce una “LESIÓN EN EL ORDENADOR”

En relación, agrega (Davara Rodríguez, 1997):

“[p]ara poder encuadrar una acción dolosa o imprudente dentro de este tipo de delitos, el medio por el que se cometan debe ser un elemento, bien o servicio, patrimonial del ámbito de responsabilidad de la informática, y el fin que se persiga deber ser la producción de un beneficio al sujeto o autor del ilícito: una finalidad deseada que causa un perjuicio a otro, a un tercero”

Respecto a dicha clasificación hemos de plasmar nuestra posición. Somos partidarios

3 (Chinchilla Sandí , Delitos Informáticos. Elementos básicos para identificarlos y su aplicación , 2004) citando a Alfredo Sneyers (1990) expone que se incluye dentro de la consideración de medio informático, los ordenadores (computadoras), miniordenadores, microrordenadores, equipos de tratamiento de textos, redes de telecomunicaciones y otros equipos informáticos, software, ficheros de datos y bases de datos.

4 (Salazar Rodríguez, 2008) citando a Kaiser.

5 El subrayado y la cursiva son suplidos

de la configuración de un delito informático únicamente en cuanto al fin, pues es nuestro considerar que el elemento o medio informático utilizado no debe ser el factor determinante para que una conducta ilícita se configure como un delito informático. Esto no quiere decir que no se puedan configurar otras figuras delictivas, empero no susceptibles de ser consideradas "delitos informáticos". Nos explicamos con un ejemplo sencillo:

> **Ejemplo.** Para la tutela del bien jurídico vida, a la luz de la normativa penal costarricense, nuestro legislador toma en consideración la lesión a dicho bien y la condición de quien realiza la acción, de ahí que la tipifica en homicidio simple[6] o calificado[7], partiendo de la misma acción penal "quien haya dado muerte a una persona"; sin dar mayor importancia al medio utilizado[8]. Poco relevante resulta entonces que se realice con un martillo, una roca, un cuchillo o un ordenador. Esto quiere decir que siempre lo que se configurará es un homicidio, así es, pues sería irrazonable pensar en un cuerpo legal que determine tipos penales específicos según el medio que se utilice para realizar la conducta ilícita: "homicidio simple o calificado con martillo, homicidio simple o calificado con roca,… Si un sujeto utiliza su ordenador para alterar otro ordenador que alimenta un respirador de un sujeto hospitalizado, ¿existe una sanción superior a la acción de homicidio, por haber sido cometido a través de un medio informático? Simplemente la acción es homicidio por provocar una lesión contra el bien jurídico vida.

Este cuestionamiento, es uno en un millón, basta con analizar cada tipo penal introduciendo la utilización de un medio informático para su comisión y plantearse la misma pregunta, para así arribar al mismo problema: "la acción penal no se define por el medio utilizado sino por el fin perseguido y la lesión causada". Existen tipos penales

6 Código Penal de Costa Rica. Homicidio simple. ARTÍCULO 111.- Quien haya dado muerte a una persona, será penado con prisión de doce a dieciocho años. (Así reformado por el artículo 1 de la ley Nº 7398 de 3 de mayo de 1994)

7 Código Penal de Costa Rica. Homicidio calificado. ARTÍCULO 112.- Se impondrá prisión de veinte a treinta y cinco años, a quien mate: 1) A su ascendiente, descendiente o cónyuge, hermanos consanguíneos, a su manceba o concubinario, si han procreado uno o más hijos en común y han llevado vida marital, por lo menos durante los dos años anteriores a la perpetración del hecho. 2) A uno de los miembros de los Supremos Poderes y con motivo de sus funciones. 3) A una persona menor de doce años de edad. 4) A una persona internacionalmente protegida, de conformidad con la definición establecida en la Ley N.º 6077, Convención sobre la prevención y el castigo de delitos contra las personas internacionalmente protegidas, inclusive agentes diplomáticos, de 11 de agosto de 1977, y otras disposiciones del Derecho internacional. 5) Con alevosía o ensañamiento. 6) Por medio de veneno suministrado insidiosamente. 7) Por un medio idóneo para crear un peligro común. 8) Para preparar, facilitar, consumar u ocultar otro delito o para asegurar sus resultados o procurar, para sí o para otro, la impunidad o por no haber logrado el fin propuesto al intentar otro delito. 9) Por precio o promesa remuneratoria. 10) A un miembro de los cuerpos policiales del Estado, municipal y de las demás fuerzas de policía públicas, cuya competencia esté prevista por ley, siempre que sea en ejercicio, por causa o en razón de sus funciones. (Así adicionado el inciso anterior por el artículo 1° de la ley N° 8977 del 3 de agosto del 2011, "Calificación de los delitos cometidos contra la integridad y vida de los policías en el ejercicio de sus funciones") (Así reformado por el artículo 1°, punto 1., aparte a) de la Ley de Fortalecimiento de la Legislación contra el Terrorismo, N° 8719 de 4 de marzo de 2009)

8 Salvo ciertas excepciones como el uso de veneno o de medio idóneo para crear un peligro, situaciones que en todo caso se clasifican como calificantes del mismo tipo penal, sin necesidad de la creación de un tipo penal en específico como sería "homicidio con veneno". Ver artículos 111 y 112 del Código Penal costarricense.

que no por el hecho de ser cometidos con la intervención de un elemento informático deben tipificarse como un delito informático. Más adelante con cada comentario profundizaremos en esta idea.

Como primera precisión entonces tenemos que constituyen sólo delitos informáticos aquellas acciones que se dirijan (su fin sea) a causar una lesión o perturbación en la operación del ordenador, y como segunda precisión introducimos que esta afectación debe recaer específicamente sobre el software del ordenador, no así sobre el hardware.[9]

Por lo tanto se constituirían en acciones que abarca el delito informático:

1) La manipulación en los datos e informaciones contenidas en los archivos y soportes físicos informáticos ajenos[10], incluyendo sus cuatro fases:

a) Almacenamiento de los datos

b) Procesamiento de los datos

c) Retroalimentación (feedback) con resultados intermedios de los datos

d) Transmisión de los resultados del proceso, ya sea en el mismo ordenador a ficheros de destino, ya sea por medio de comunicaciones o acceso a periféricos en los que se depositan

2) El acceso a los datos y/o utilización de los mismos por quien no está autorizado para ello

3) La introducción de programas o rutinas en otros ordenadores para destruir información, datos o programas, así como también el sabotaje de computadoras mediante "Bombas lógicas"[11]

4) La agresión a la privacidad mediante el procesamiento de datos personales con fin distinto al autorizado, lo que podríamos denominar "espionaje por computadoras"

9 Para comprender más profundamente de este punto véase en este mismo artículo infra, Comentario 3.

10 A saber: (1) Manipulación en el ingreso de los datos a la computadora, (2) Manipulación de datos ingresados a la computadora, (3) Manipulación de Programas, conocida como la famosa "técnica salami", en la que el autor no manipula ni altera los datos de la computadora, sino que por el contrario, la manipulación y/o alteración se genera en el programa. Un ejemplo de este caso, relativamente sencillo es el del empleado bancario, que altera el programa de cálculo de intereses de las cuentas de ahorro, de manera tal que solo los dos primeros dígitos de los decimales, se tomen como intereses y los restantes dígitos se transfieran a una cuenta, por él controlada. De esta manera tan simple, es posible obtener grandes sumas de dinero, pues los cuentahabientes no lo pueden detectar, y (4) Manipulación en los datos que salen de la Computadora o el "Caballo de Troya" que ocurre cuando los datos se transfieren a otra computadora, en los programas de impresión (output), o en programas de actualización, es decir, una vez que los datos son ingresados, ordenados y los procesos de cálculo elaborados, la información final, por lo general se imprime y almacena. Es posible así manipular la información que se imprime y almacena, de manera tal que la alteración no pueda detectarse, durante el procesamiento de datos.

11 Esta forma de criminalidad tiene por objeto la afectación o destrucción tanto del programa, como de los datos almacenados en la computadora, bien puede provocarse un daño al hardware o disco duro, pero la forma más común de comisión es a través del deterioro de los datos almacenados y los programas. Un ejemplo clásico es la intromisión de los denominados virus, que son programas que se almacenan o instalan en determinados sectores del hardware y/o programas de la computadora y que se encargan de destruir la información, inutilizarla o bien producir daños al mismo disco duro, que lo hacen inaccesible y/o inservible.

5) Estafa Electrónica[12]

Bien, sin necesidad de ahondar en estos ejemplos y reafirmando nuestra posición respecto a que, delitos informáticos sólo deben configurarlos aquellas acciones que por su fin se dirijan a la lesión del software del ordenador, procedemos a exponer nuestras críticas a la reforma del Código Penal que introduce la Ley 9048 (Sobre delitos Informáticos).

Comentario 1. Sobre la reforma al delito de extorsión.

CÓDIGO PENAL	REFORMAS AL CÒDIGO PENAL
ARTÍCULO 214.- Extorsión simple. Será reprimido con prisión de dos a seis años, el que para procurar un lucro injusto obligare a otro con intimidación o con amenazas graves a tomar una disposición patrimonial perjudicial para sí mismo o para un tercero.	**ARTÍCULO 214.- Extorsión.** Será reprimido con pena de prisión de cuatro a ocho años (1) al que para procurar un lucro obligue a otro, con intimidación o con amenazas graves, a tomar una disposición patrimonial perjudicial para sí mismo o para un tercero. La pena será de cinco a diez años de prisión cuando la conducta se realice valiéndose de cualquier manipulación informática, telemática, electrónica o tecnológica.(2) *(el subrayado es suplido)

(1) En primera instancia debe apercibirse el aumento injustificado de la pena, de 2 años tanto en su mínimo como en su máximo, sin existir ninguna modificación en la acción sancionada: *"quien para procurar un lucro obligue a otro, con intimidación o con amenazas graves, a tomar una disposición patrimonial perjudicial para sí mismo o para un tercero"*. Pareciera ser ésta únicamente una maniobra legislativa que se vale de la promulgación de esta ley, para imponer una mayor punición a esta acción sin nuevas consideraciones respecto al tipo penal que la justifiquen.

(2) Como segundo punto cabe cuestionarse ¿qué relevancia tiene en la configuración de la acción penal en cuestión, el medio que se utilice? El bien jurídico tutelado respecto a la libre disposición de los actos de un individuo es el mismo, sin que tenga importancia que se haga personalmente o a través de un medio informático o cualquier instrumento de la comunicación.

La intimidación o amenaza sobre el sujeto que recibe la acción afecta de igual manera su libertad, entonces ¿por qué la agravante? Si se apela a características como el método, ¿por qué no? entonces considerar situaciones como: si la intimidación se realiza

12 Es preciso antes señalar que técnicamente no es ninguna estafa, por ausencia de un sujeto pasivo que realice el acto dispositivo, sin embargo se asemeja a la hipótesis de la estafa triangular, la cual supone que el engañado y el estafado son personas diferentes. Sin embargo, en la estafa triangular el engañado tiene la facultad de realizar un acto dispositivo perjudicial para el estafado, de manera que el autor le produce a través de ese engaño, una lesión a su patrimonio y obtiene para sí o para un tercero un beneficio patrimonial antijurídico. En el caso de la aquí denominada "estafa electrónica" lo que el autor hace es "engañar" [utilizamos el término únicamente como una pseudodefinición estipulativa porque claramente no es un engaño, sino una manipulación] a la computadora (que sustituye al sujeto pasivo), y produce con esto que la computadora realice un acto dispositivo perjudicial para un tercero, desde luego, pues para la computadora no puede existir un perjuicio patrimonial en ningún supuesto.

(1) e nos encontramos ante una variación injustificada de la pena que aumento el mínimo a imponer en 3 años, sancionándose la misma

respecto a la pérdida de un familiar, o la afectación de un patrimonio… En estos casos entonces, ¿la acción ilícita de obligar a otro a tomar una disposición patrimonial perjudicial para sí mismo o para un tercero, cambia? ¿Tendríamos que configurar un agravante para cada una de estas hipótesis?

Comentario 2. Sobre la reforma al delito de espionaje.

CÓDIGO PENAL	REFORMAS AL CÒDIGO PENA
ARTÍCULO 288.-Espionaje. Será reprimido con prisión de uno a seis años, el que procurare u obtuviere indebidamente informaciones secretas políticas o de seguridad concernientes a los medios de defensa o a las relaciones exteriores de la Nación. (Así modificada la numeración de este artículo por el numeral 185, inciso a), de la ley No.7732 de 17 de diciembre de 1997, que lo traspasó del 286 al 288)	Espionaje. Será reprimido con prisión de cuatro a ocho (1) años al que procure u obtenga indebidamente informaciones secretas políticas o de los cuerpos de policía nacionales o de seguridad concernientes a los medios de defensa o a las relaciones exteriores de la nación, o afecte la lucha contra el narcotráfico o el crimen organizado. La pena será de cinco a diez años de prisión cuando la conducta se realice mediante manipulación informática, programas informáticos maliciosos o por el uso de tecnologías de la información y la comunicación. (2) *(el subrayado es suplido)

Comentario 3. Sobre la adición al delito de daño agravado.

acción: "la obtención de información cubierta por el secreto estatal". Lo que se realiza es una especial consideración al hecho de que dicha acción afecta la lucha contra el narcotráfico o el crimen organizado, la cual resulta irracional en el tanto los resultados de esta acción no sólo pueden afectar estos aspectos, sino muchos otros relacionados con la política criminal que también deberían en su caso ser considerados.

(2) Esta agravante también resulta innecesaria, dado que el medio que se utilice no altera en nada la conducta penal, la intromisión en la información resguardada por el Estado resulta ser la misma, el tipo penal anterior ya consideraba su protección, no hay porqué considerar el medio que se utilizó para obtenerla. Lo que si debiera de considerarse es si el sujeto se vale de su puesto de poder o confianza para la comisión del delito, pero no del medio que emplee, pues la lesión provocada no cambia. ¿No debería ser más grave la pena si se obtiene la información de una conversación con un funcionario público?..., esto pues estaría no sólo violando el secreto de Estado, sino sus deberes de discreción y confidencialidad con la administración pública.

CÓDIGO PENAL	ADICIONES AL CÒDIGO PENAL
ARTÍCULO 229.- Daño agravado. Se impondrá prisión de seis meses a cuatro años: 1) Si el daño fuere ejecutado en cosas de valor científico, artístico, cultural o religioso, cuando, por el lugar en que se encuentren, se hallaren libradas a la confianza pública, o destinadas al servicio, la utilidad o la reverencia de un número indeterminado de personas. 2) Cuando el daño recayere sobre medios o vías de comunicación o tránsito, sobre puentes o canales, sobre plantas de producción o conductos de agua, de electricidad o de sustancias energéticas. 3) Cuando el hecho fuere ejecutado con violencia en las personas o con amenazas. 4) Cuando el hecho fuere ejecutado por tres o más personas. 5) Cuando el daño fuere contra equipamientos policiales.	**ARTÍCULO 229.-** Daño agravado. Se impondrá prisión de seis meses a cuatro años: 1) Si el daño fuere ejecutado en cosas de valor científico, artístico, cultural o religioso, cuando, por el lugar en que se encuentren, se hallaren libradas a la confianza pública, o destinadas al servicio, la utilidad o la reverencia de un número indeterminado de personas. 2) Cuando el daño recayere sobre medios o vías de comunicación o tránsito, sobre puentes o canales, sobre plantas de producción o conductos de agua, de electricidad o de sustancias energéticas. 3) Cuando el hecho fuere ejecutado con violencia en las personas o con amenazas. 4) Cuando el hecho fuere ejecutado por tres o más personas. 5) Cuando el daño fuere contra equipamientos policiales. 6) Cuando el daño recayera sobre redes, sistemas o equipos informáticos, telemáticos o electrónicos, o sus componentes físicos, lógicos o periféricos.(1) *(el subrayado es suplido)

(1) Para la exposición de este comentario antes debemos recurrir a la determinación de lo que se conoce como el software y el hardware de un ordenador, (Davara Rodríguez, 1997) indica que:

“Hardware, es el término con el que se designa a la configuración física de un sistema de un ordenador respecto a todos sus elementos; software, es el soporte lógico de las instrucciones y órdenes (programas) que se dan a un ordenador para que realice un proceso. El software puede ser de tres tipos:

a) Software de base o de sistema, formado por los programas que controlan y guían las funciones del sistema (ordenador).

b) Software de utilidad, formado por diversos programas de utilidad general.

c) Software de usuario o de aplicaciones”.

Así, hemos de considerar que un daño agravado sólo se configura sobre el hardware del ordenador, pues las otras intromisiones al software que pudieren ocasionar su destrucción, inutilización, desaparición o daño de cualquier modo, ya están contempladas en otros tipos penales según el fin que persigan, por lo que su inclusión en esta figura podría significar su doble punición. De ahí también que consideremos, como fue supra indicado, que un delito informático se configura únicamente cuando estamos frente a una acción que produce una lesión sobre el software del ordenador, pues de lo contrario estaríamos precisamente hablando de un daño agravado.

Comentario 4.

Adición del delito de suplantación de identidad y suplantación de páginas electrónicas[13].

ARTÍCULO 230.- Suplantación de identidad. Será sancionado con pena de prisión de tres a seis años quien suplante la identidad de una persona en cualquier red social, sitio de Internet, medio electrónico o tecnológico de información. La misma pena se le impondrá a quien, utilizando una identidad falsa o inexistente, cause perjuicio a un tercero.

La pena será de cuatro a ocho años de prisión si con las conductas anteriores se causa un perjuicio a una persona menor de edad o incapaz.

ARTÍCULO 233.-Suplantación de páginas electrónicas. Se impondrá pena de prisión de uno a tres años a quien, en perjuicio de un tercero, suplante sitios legítimos de la red de Internet.

La pena será de tres a seis años de prisión cuando, como consecuencia de la suplantación del sitio legítimo de Internet y mediante engaño o haciendo incurrir en error, capture información confidencial de una persona física o jurídica para beneficio propio o de un tercero.

En ambos tipos penales no encontramos su justificación para constituirse como delitos informáticos. Pareciera ser que la conexión que se pretende establecer radica en que la suplantación de identidad se realice en cualquier red social, sitio de Internet, medio electrónico o tecnológico de información o que se suplanten sitios legítimos de la red de Internet. Pero, ¿eso qué relación tiene con intromisión en el software de un medio informático? Lo que se pretende proteger sancionando la suplantación es el derecho a la identidad propia y reconocida de cada persona y a la protección de los derechos de autor de quien posea una página de internet, situaciones que no tienen porqué depender del medio a través del cual se violenten.

Ahora bien, no estamos aquí afirmando que no debe existir la punición de dichas suplantaciones, sólo apuntamos que estas acciones no tienen razón para ser clasificadas como delitos informáticos, pues con su comisión no se configura ninguna acción que tenga como fin la lesión al software de un ordenador.

Comentario 5.

Adición del delito de narcotráfico y crimen organizado.

Artículo 235.- Narcotráfico y crimen organizado. La pena se duplicará cuando cualquiera de los delitos cometidos por medio de un sistema o red informática o telemática, o los contenedores electrónicos, ópticos o magnéticos afecte la lucha contra el narcotráfico o el crimen organizado.

Este artículo resulta definitivamente injustificable, a no ser que se acepte un matiz político de la ley. De manera prácticamente inexplicable se establece una conexión entre los delitos informáticos y el narcotráfico o el crimen organizado. Pareciera a la

13 La ley 17.613, dispone la modificación de la sección VIII del título VII de la Ley N.º 4573, Código Penal, de 4 de mayo de 1970, y sus reformas; corriendo la numeración de los artículos subsiguientes, de manera que su redacción contemple un “TÍTULO VII […] Sección VIII. Delitos informáticos y conexos

luz de la adición de este artículo como las reformas introducidas en el numeral 288 sobre espionaje[14] que esta ley tiene un gran interés por aumentar la punición de los delitos de narcotráfico y crimen organizado, relacionando su comisión con otras acciones sin que exista un vínculo lógico que les una. Nuevamente señalamos, el bien jurídico tutelado la salud y seguridad pública, es el mismo y su lesión no depende de los medios informáticos utilizados para su organización o configuración.

Ante esta situación caben miles de cuestionamientos, el principal: ¿qué hace un "tipo penal" como el expuesto en el acápite de delitos informáticos y sus conexos? ¿De qué manera está acción vulnera un sistema o medio informático?

Comentarios Finales

La penalización de la utilización de un medio informático en la comisión de un delito puede alcanzarse a través de la determinación de una agravante en el tipo penal, sin necesidad de la creación de un nuevo delito informático. Tal es el caso de la reforma introducida por la ley en análisis al artículo 67 sobre corrupción, en donde se aumenta la pena (cuatro a diez años) "si el actor, utilizando las redes sociales o cualquier otro medio informático o telemático, u otro medio de comunicación, busca encuentros de carácter sexual para sí, para otro o para grupos, con una persona menor de edad o incapaz; utiliza a estas personas para promover la corrupción o las obliga a realizar actos sexuales perversos, prematuros o excesivos, aunque la víctima consienta participar en ellos o verlos ejecutar". Esto, pues resulta razonable una sanción mayor en atención al actual desarrollo de la informática y más aún de la telemática, dado que permiten una propagación masiva de la información.

Así, no puede pretenderse que toda aquella acción que involucre a un medio informático constituya un delito informático. A nuestra consideración estos se configurarán únicamente cuando exista una intromisión o alteración en el software de un ordenador que provoque una lesión sobre el mismo, y que dicha acción sea cometida con ese fin y con el objeto de obtener un beneficio propio con ello.

Si se sigue admitiendo la configuración de un delito penal en cuanto a su medio, en pocos años con el acelerado avance de la informática nuestros códigos penales estarán abarrotados de delitos informáticos, configurándose así un derecho penal de medios y no de fines, perdiéndose la esencia de la protección de cada bien jurídico.

14 Ver Comentario 2.

Bibliografía

Chinchilla Sandí , C. (2004). *Delitos Informáticos. Elementos básicos para identificarlos y su aplicación .* San José: Farben Group Editorial Norma.

Davara Rodríguez, M. Á. (1997). *Manual de Derecho Informático.* Navarra: Aranzadi.

Salazar Rodríguez, A. (2008). *El Delito del Fraude por Computadora de acuerdo al 263a del Código Penal. Tesina para la Universidad de Valencia.* Valencia.

Alonso Salazar Rodríguez (asalazar@salazarabogados.net, Cel: 8833 8624)
Elízabeth Guerrero Barrantes (eguerrero@salazarabogados.net, Cel: 8304 8025)