UNIVERSIDAD Rafael Belloso Chacín

Revista Electrónica de Estudios Telemáticos

TÉLÉMATIQUE

ANÁLISIS CRÍTICO A LA TIPICIDAD PREVISTA EN ALGUNOS ARTÍCULOS DE LA LEY ESPECIAL CONTRA DELITOS INFORMÁTICOS VENEZOLANA

(Critical analysis to the typical in some articles of the special law against computer science crimes venezuelan)

Logreira Rivas, Carmen Isabel[*]
Universidad Rafael Belloso Chacín - Venezuela

Fuentes Pinzón, Fernando José[**]
Universidad Rafael Belloso Chacín - Venezuela

RESUMEN

El presente trabajo procura el estudio de la Ley Especial Contra Delitos Informáticos publicada en la Gaceta Oficial Nº 37.313 del 30 de noviembre del 2001, a través de la tipificación de sus delitos, partiendo de un análisis crítico a la misma, con el propósito de servir como observaciones en una futura modificación del presente instrumento legal o en una probable incorporación al Código Penal reformado.

Palabras Clave: Delitos informáticos, Ley Especial Contra Delitos Informáticos, Tipicidad.

ABSTRACT

The present work tries the study of the Special Law Against Computer science Crimes published in the Official Newspaper Nº 37,313 of the 30 of November of the 2001, through the standardisation of its crimes, starting off of a critical analysis for the same, in order to serve like observations in a future modification as the present legal instrument or in a probable incorporation the reformed Penal Code

Key words: Computer science crimes, Special Law Against Computer science Crimes, Typical.

[*] Licenciada en Educación, mención: Informática y Matemática (UCAT). Magíster en Informática Educativa (URBE). Magíster en Docencia para la Educación Superior (UNERMB). Doctorado en Ciencias Gerenciales (URBE). Doctorado en Educación (URBE). PPI nivel I Nº 6846. Profesora Titular de la Facultad de Ingeniería URBE. Profesora Contratada de la Facultad de Humanidades y Educación LUZ. E-mail: clogreira@urbe.edu, clogreira@hotmail.com.

[**] Abogado (LUZ). Especialista en Propiedad Intelectual (ULA). PPI nivel I Nº 8142 Profesor Agregado de la Facultad de Ciencias Jurídicas y Políticas (URBE). Autor de los libros Guía del Inventor Universitario (2000), Derechos Intelectuales (2006) y Marco Legal de la Informática y la Computación (2007). E-mail: ffpve@hotmail.com, ffve@yahoo.com.

Depósito Legal: PPX200002ZU2142 / ISSN:1856-4194. Volumen 7 Edición No 2 – Año 2008

INTRODUCCIÓN

La Ley Especial Contra Delitos Informáticos publicada en la Gaceta Oficial Nº 37.313 del 30 de noviembre del 2001, si bien en su momento constituyó una novedad en el área penal, cuando se realiza un análisis profundo a la misma, aparecen una serie de errores y omisiones por parte del legislador, que el presente trabajo procura exponer, con el propósito de enmendar la misma o aclarar al intérprete los delitos tipificados.

1. Sobre la tipicidad

Para la existencia del delito, es necesaria la conjunción de varios elementos básicos, según la Teoría General del Delito y a decir de autores clásicos en la materia como Jiménez (1980) y Mendoza (1986), estos elementos pueden resumirse en siete: acción, tipicidad, antijuricidad, imputabilidad, culpabilidad, condicionalidad objetiva y punibilidad. De estos, es la tipicidad entendida como la descripción de una conducta por medio de la norma penal para que sea considerada como delito, es el más perfectible y delicado de estos, por ser precisamente, el freno a la pretensión punitiva del Estado, y constituir la primera defensa al respeto de los derechos humanos.

Tal es su transcendencia que fue previsto en el Artículo 1 del Código Penal (1961 reformado en el 2005), de la siguiente manera: “Nadie podrá ser castigado por un hecho que no estuviese expresamente previsto como punible por la ley”, al igual que en la Constitución de la República Bolivariana de Venezuela, en su Artículo 49 numeral 7, el cual expresa: “Ninguna persona podrá ser sancionada por actos u omisiones que no fueren previstos como delitos, faltas o infracciones en leyes preexistentes”. Sin embargo, su estudio no puede ser realizado sin tomar en cuenta dos elementos adicionales para la constitución del delito, por lo menos normativamente hablando, estos son: la antijuricidad y la culpabilidad.

En la legislación venezolana existen conductas tipificadas como delitos desde hace años, las cuales son aplicables al área de la informática, por ejemplo, las normas penales previstas por la Ley sobre Derecho de Autor (1993), o las relativas a la difamación e injuria contempladas en el Código Penal (1964). Ahora bien, también es cierto que figuras delictuales típicas previstas por el Código Penal venezolano (que data de 1964, con su respectivas reformas, siendo la última publicada en Gaceta Oficial Nº 5.768 Extraordinaria del 13 de abril del 2005) y otras leyes con normas penales, al ser previstas de manera cerrada, no permiten al juez hacer una interpretación extensiva para abarcar las nuevas modalidades de las mismas cuando se utilizaran medios informáticos o electrónicos, por ello, era necesario una reforma al Código Penal o la promulgación de una ley que previera estas adaptaciones a supuestos ya penados y previsto por normas anteriores, como a las nuevas conductas producto de estas tecnologías.

Ahora, en el propio ordenamiento jurídico, puede existir una conducta tipificada, y sin embargo, existir al mismo tiempo una norma que permita o justifique dicha

Depósito Legal: PPX200002ZU2142 / ISSN:1856-4194. Volumen 7 Edición No 2 – Año 2008

acción, de tal manera que la misma acción no fuese punible, en ese caso, la conducta estudiada no sería antijurídica y por ende, no sería considerable delito.

Un ejemplo de ello, lo constituye la reproducción no autorizada de una obra protegida por el derecho de autor, supóngase un programa de computación, al ser introducida en la memoria de la computadora para su ejecución. Se ha cometido la conducta prevista por la norma penal, sin embargo, otro artículo de la misma ley establece entre las excepciones al derecho exclusivo de reproducción, la copia en la memoria interna de la computadora del software para su posterior ejecución, en virtud de esto, dicha conducta a pesar de ser una acción debidamente tipificada y ejecutada por un sujeto, no es antijurídica y como consecuencia de ello, no es considerable delito.

La denominada culpabilidad es un elemento aplicable al sujeto activo, específicamente en su fuero interno, en virtud de estar referida a su intencionalidad de ejecutar o realizar la conducta sancionada por la ley, ya que evalúa la discrecionalidad o la posibilidad de haber actuado de otra manera, evitando la conducta reprochable penalmente, realizada por este sujeto.

La culpabilidad es prevista por el Código Penal (1964 reformado en el 2005) venezolano en su Artículo 61 de la siguiente manera: “Nadie podrá ser castigado como reo de delito no habiendo tenido la intención de realizar el hecho que lo constituye, excepto cuando la ley se lo atribuye como consecuencia de su acción u omisión”.

Pero el concepto de intencionalidad no se ve afectado por la supuesta ignorancia del sujeto activo de estar cometiendo una conducta penalmente sancionada, previendo en ese sentido, el mismo Código Penal (1964 reformado en el 2005), en su Artículo 60: “La ignorancia de la ley no excusa ningún delito ni falta”, por lo cual se constituye en una presunción de conocimiento de la misma, por parte de todos los ciudadanos.

2. Tipos penales susceptibles de perfeccionamiento en la Ley Especial Contra Delitos Informáticos

2.1. Sabotaje o daño a sistemas

Por sabotaje debe entenderse a los daños provocados dolosamente contra las vías de comunicación, bienes o instalaciones de un ejército invasor, un Estado o una empresa rival, con la intención de causar o provocarle atrasos o problemas al mismo. A diferencia de los daños que pueden ser realizados con o sin intención, y que no tienen un sujeto pasivo particular ni mayores consecuencias que los perjuicios directamente causados a las maquinarias o sistemas atacados.

Tradicionalmente, los daños a bienes muebles e inmuebles, han sido previstos por el Código Penal venezolano, de la siguiente manera: “Artículo 473. El que de cualquier manera haya destruido, aniquilado, dañado o deteriorado las cosas,

Depósito Legal: PPX200002ZU2142 / ISSN:1856-4194. Volumen 7 Edición No 2 – Año 2008

muebles o inmuebles, que pertenezcan a otro será castigado, a instancia de la parte agraviada, con prisión de uno a tres meses"

Son tres las características de este delito: (a) Las conductas sancionadas son la destrucción, aniquilación, daño o deterioro; (b) El objeto material sobre el cual se deben ejercen las conductas descritas, son bienes ajenos o pertenecientes a otros; (c) El delito es de acción privada, es decir, es menester la acusación por parte del sujeto pasivo (el agraviado).

La Ley Especial Contra los Delitos Informáticos (2001) venezolana, establece la siguiente figura delictual en relación al Sabotaje:

> Artículo 7. Sabotaje o daño a sistemas. El que destruya, dañe, modifique o realice cualquier acto que altere el funcionamiento o inutilice un sistema que utilice tecnologías de información o cualquiera de los componentes que lo conforman, será penado con prisión de cuatro a ocho años y multa de cuatrocientas a ochocientas unidades tributarias.
>
> Incurrirá en la misma pena quien destruya, dañe, modifique o inutilice la data o la información contenida en cualquier sistema que utilice tecnologías de información o en cualquiera de sus componentes.
>
> La pena será de cinco a diez años de prisión y multa de quinientas a mil unidades tributarias, si los efectos indicados en el presente artículo se realizaren mediante la creación, introducción o transmisión, por cualquier medio, de un virus o programa análogo.

La norma contiene dos delitos distintos: en el primero, el objeto jurídico protegido son los sistemas que utilicen tecnologías de información y los componentes que lo conformen; mientras, que en el segundo, el objeto jurídico protegido es la información o data almacenada en dichos sistemas o en sus componentes.

En este primer supuesto delictual, se pueden dividir en dos las conductas previstas: (a) Aquellas que inutilizan a un sistema que utilice tecnologías de información o alguno de sus componentes, siendo la más representativa de estas, la destrucción del mismo; y (b) Aquellas que dañan, modifiquen o inutilicen al sistema o a sus componentes.

Las acciones solas no bastan para considerarse constituido el delito, sino que será menester un resultado concreto: la inutilización o la alteración en el funcionamiento del sistema o de alguno de sus componentes.

La redacción de la norma, permite tipificar como conductas prohibidas cualquier modificación que logre o permita una alteración (entendida como sinónimo de cambio) en el funcionamiento de un sistema informático, sin importar que medie el consentimiento del dueño o propietario del mismo, o lo que es igual, ha prohibido el ejercicio de la profesión de los técnicos o ingenieros en informática, computación y

Depósito Legal: PPX200002ZU2142 / ISSN:1856-4194. Volumen 7 Edición No 2 – Año 2008

carreras afines. Por ello, la única interpretación aceptable (alejándose de la redacción de la norma) sería que el término alterar se refiera a la perturbación o cambio que afecte negativamente (comprobable por medio de perjuicios derivados de dicha modificación) el funcionamiento del sistema o alguno de sus componentes.

Ahora, la mala praxis legislativa es más notable en el segundo delito previsto, ya que establece como conducta prohibida la destrucción (al tratarse de bienes intangibles, no es posible su destrucción, sino su eliminación o, en su defecto, la acción de borrarlos) y modificación de los datos o informaciones contenidos en un sistema informático, sin excluir al propietario, dueño o autor de dichos bienes intangibles, por ende, cada vez que cualquier persona elimine o modifique una información de la que es propietaria, contenida en un sistema informático del que también es propietario, sería un sujeto activo (y al mismo tiempo pasivo) del presente delito.

La conducta tipificada no condiciona el delito al modo en que se realicen las acciones, sino al objeto material protegido, que no es otro que los datos o informaciones contenidos en un sistema informático o en sus componentes.

Continuando con el análisis del Artículo 7 de la Ley Especial Contra Delitos Informáticos, en su párrafo tercero se establece un delito dependiente, que consiste en el uso de medios informáticos para cometer cualquiera de las conductas previamente estudiadas (del mismo artículo), específicamente, el empleo de un virus, el cual se entiende como: “Programa o segmento de programa indeseado que se desarrolla incontroladamente y que genera efectos destructivos o perturbadores en un programa o componente del sistema” (Ley Especial Contra Delitos Informáticos, Artículo 2 Ordinal m), o programa análogo. En ese sentido, si la creación, introducción o transmisión de este, causa la inutilización o alteración en el funcionamiento del sistema, sus componentes o los datos o informaciones (en este último supuesto sería la destrucción, daño, inutilización o modificación) contenidos en el mismo, se debe considerar constituido el delito.

Es de hacer notar, que la ley especial no establece en su articulado, si los delitos previstos, son de carácter público o privado, es decir, si son perseguibles sólo por acusación de la parte agraviada, o si son competencia de la Fiscalía General de la República, bastando la denuncia del hecho.

Para las conductas previstas en el artículo “in comento” existe una atenuante y una agravante. La primera consiste en la realización de las conductas previstas, sin la intención de ello, es decir, cuando falte el dolo en el sujeto activo, será aplicable el Artículo 8, que expresamente prevé: “Sabotaje o daño culposos. Si el delito previsto en el artículo anterior se cometiere por imprudencia, negligencia, impericia o inobservancia de las normas establecidas, se aplicará la pena correspondiente según el caso, con una reducción entre la mitad y dos tercios”.

Mientras, que el agravante es previsto por el Artículo 9, de la siguiente manera:

Depósito Legal: PPX200002ZU2142 / ISSN:1856-4194. Volumen 7 Edición No 2 – Año 2008

> Acceso indebido o sabotaje a sistemas protegidos. Las penas previstas en los artículos anteriores se aumentarán entre una tercera parte y la mitad cuando los hechos allí previstos o sus efectos recaigan sobre cualquiera de los componentes de un sistema que utilice tecnologías de información protegido por medidas de seguridad, que esté destinado a funciones públicas o que contenga información personal o patrimonial de personas naturales o jurídicas.

2.2. Falsificación de documentos

El tipo tradicional es previsto por el Código Penal (1964 reformado en el 2005), de la siguiente forma:

> Artículo 321. El individuo que hubiere falsificado o alterado, total o parcialmente, alguna escritura, carta u otro género de papeles de carácter privado, de modo que haciendo él, u otro, uso de dichos documentos, pueda causarse un perjuicio al público o a particulares, será castigado con prisión de seis a dieciocho meses.

La conducta es la falsificación o alteración de un documento previamente creado, con la condicionante que el uso del mismo sea capaz de generar consecuencias en contra de particulares o del público en general.

Por documento, si bien el Código Penal no lo define, Grisanti (2000: 1060), citando a Cabanellas establece que puede entenderse como:

> (…) instrumento, escritura, escrito con que se prueba, confirma o justifica alguna cosa o, al menos, que se aduce con tal propósito (ómisis) en la acepción más amplia cuando consta por escrito o gráficamente; así lo es tanto un testamento, un contrato firmado, un libro o una carta, como una fotografía o un plano; y sea cualquiera la materia sobre la cual se extienda o figure, aunque indudablemente predomine el papel sobre todas las demás.

Una vez comprendido el antecedente del tipo previsto por la Ley Especial Contra los Delitos Informáticos venezolana, se puede analizar detalladamente la conducta ilícita penada por la norma, la cual esta contemplada en el Artículo 12, de la siguiente manera:

> Falsificación de documentos. El que, a través de cualquier medio, cree, modifique o elimine un documento que se encuentre incorporado a un sistema que utilice tecnologías de información; o cree, modifique o elimine datos del mismo; o incorpore a dicho sistema un documento inexistente, será penado con prisión de tres a seis años y multa de trescientas a seiscientas unidades tributarias.

El primer elemento a determinar es la definición de documento, el cual es entendido por la misma Ley Especial contra Delitos Informáticos como: “Documento: registro incorporado en un sistema en forma de escrito, video, audio o cualquier otro

Depósito Legal: PPX200002ZU2142 / ISSN:1856-4194. Volumen 7 Edición No 2 – Año 2008

medio, que contiene data o información acerca de un hecho o acto capaces de causar efectos jurídicos" (Artículo 2 Ordinal e).

Una vez establecido el objeto material protegido, será menester el análisis de las conductas sancionadas, las cuales difieren de la prevista por el Código Penal.

Cualquier persona (sujeto activo) que realice por primera vez un documento (es decir, que lo cree), o bien que lo modifique o elimine, cuando se encuentre incorporado de cualquier forma a un sistema que utilice tecnologías de información, sin que sean necesarios el perjuicio de un tercero o el beneficio propio, estaría cometiendo este delito. Esta conducta demuestra claramente la inoperatividad de muchas de las normas penales previstas por esta ley, ya que la creación o modificación de documentos es una tarea rutinaria y lícita (previa a la promulgación de esta norma, por supuesto), por ende, la aplicación textual de la misma haría imposible el uso de procesadores de palabras o demás herramientas que permitan la creación, modificación o eliminación de documentos por medio del uso de la tecnología de la información, sin considerar la posibilidad que quien realice dicha conducta sea el propio autor o titular de dicho documento.

Con respecto a la segunda conducta prevista por este artículo, referida a la incorporación a un sistema que utilice tecnologías de la información de un documento inexistente, es de resaltar que si el documento fuese efectivamente inexistente no podría ser incorporado. Interpretando la norma, la intención del legislador debió ser la de condenar la incorporación de documentos nuevos, por quien no tenga derecho a ello, en un sistema que utilice tecnología de información.

El mismo artículo prevé dos agravantes: la primera cuando el sujeto activo haya actuado para procurarse algún beneficio, bien para sí mismo, como para un tercero (aumenta la pena entre un tercio y la mitad); la segunda, si la conducta prevista ha ocasionado un perjuicio para cualquier persona distinta a los sujetos activos (la pena aumenta de la mitad a dos tercios).

2.3. Hurto Informático

El delito de hurto es previsto por el Código Penal venezolano (1964 reformado en el 2005), de la siguiente manera: "Artículo 451. Todo el que se apodere de algún objeto mueble, perteneciente a otro para aprovecharse de él, quitándolo, sin el consentimiento de su dueño, del lugar donde se hallaba, será penado con prisión de seis meses a tres años".

El objeto jurídico protegido es la propiedad, y en su caso, la tenencia o posesión. Mientras, el objeto material (es decir, aquel sobre el cual se ejecuta una acción o conducta antijurídica) es una cosa mueble ajena. No se entrará a discutir si el concepto de bien mueble incluye a los bienes inmateriales, sino lo que se pretende es entender los elementos esenciales del delito, para posteriormente analizar los supuestos de hurto previstos por la Ley Especial sobre Delitos Informáticos

Depósito Legal: PPX200002ZU2142 / ISSN:1856-4194. Volumen 7 Edición No 2 – Año 2008

venezolana (2001), y su correspondencia con las normas penales de los demás países iberoamericanos.

El sujeto activo es indiferente, es decir, cualquier persona que realice la acción antijurídica prevista por la norma, sin que se establezcan cualidades particulares al sujeto. Igualmente, el sujeto pasivo es indiferente, basta con que haya estado el bien en su posesión o tenencia, cuando ha sucedido el desapoderamiento, independientemente que sea el propietario o no.

La acción consiste en el apoderamiento, es decir, en la capacidad del sujeto activo de disponer o mantener (aunque sea por un período de tiempo muy corto) un señorío de facto sobre el bien despojado. Entonces, será necesario el despojo o desapoderamiento del sujeto pasivo, y la constitución de apoderamiento del sujeto activo, para que pueda entenderse como consumado el delito. Un ejemplo de ello, sería que el sujeto activo del delito obtiene un bien mueble (digamos, un celular), con el propósito de disponer de él, pero al intentar sacarlo de una tienda, suena la alarma y el delincuente es detenido a sólo metros de la salida, entonces, si bien a sucedido un desapoderamiento de una cosa mueble ajena, consistente en la remoción del bien del sitio donde estaba, sin el consentimiento del dueño, con la intencionalidad de aprovecharse del mismo, no ha existido un apoderamiento, ya que no ha tenido realmente disponibilidad sobre el bien, ya que ha sido perseguido inmediatamente por el sujeto pasivo, conservando este una precaria condición de señorío sobre el bien en cuestión, que es restituida completamente al ser recuperado el bien. En este supuesto, ha existido tentativa de hurto, que al igual que el hurto consumado, es una conducta sancionable.

Entendido los elementos básicos del delito de hurto genérico, pasemos a estudiar la norma prevista por la legislación especial (2001) sobre la materia:

> Artículo13.- Hurto. El que a través del uso de tecnologías de información, acceda, intercepte, interfiera, manipule o use de cualquier forma un sistema o medio de comunicación para apoderarse de bienes o valores tangibles o intangibles de carácter patrimonial sustrayéndolos a su tenedor, con el fin de procurarse un provecho económico para sí o para otro, será sancionado con prisión de dos a seis años y multa de doscientas a seiscientas unidades tributarias.

Antes de entrar a analizar los elementos que componen este delito, se deben comprender dos conceptos novedosos contenidos en su redacción, los cuales son: tecnologías de información y sistema, ambos definidos por el Artículo 2 Ordinal a de la misma ley.

> Tecnología de Información: rama de la tecnología que se dedica al estudio, aplicación y procesamiento de data, lo cual involucra la obtención, creación, almacenamiento, administración, modificación, manejo, movimiento, control, visualización, distribución, intercambio, transmisión o recepción de información en forma automática, así como el desarrollo y uso del

Depósito Legal: PPX200002ZU2142 / ISSN:1856-4194. Volumen 7 Edición No 2 – Año 2008

> "hardware", "firmware", "software", cualesquiera de sus componentes y todos los procedimientos asociados con el procesamiento de data.

Entonces, toda aquella tecnología que permita el uso de la información en forma automática, será considerada como tecnología de información, siendo las acciones descritas en la definición (obtención, creación, manejo, visualización, entre otras), funciones típicas de esta. Igualmente, del concepto se desprende la extensión del término para abarcar cualquier bien (tangible como intangible) que permita el cumplimiento de sus funciones.

Ahora bien, sistema, es definido en su Artículo 2 Ordinal b de la Ley como:

> Sistema: cualquier arreglo organizado de recursos y procedimientos diseñados para el uso de tecnologías de información, unidos y regulados por interacción o interdependencia para cumplir una serie de funciones específicas, así como la combinación de dos o más componentes interrelacionados, organizados en un paquete funcional, de manera que estén en capacidad de realizar una función operacional o satisfacer un requerimiento dentro de unas especificaciones previstas.

Pues sistema será entonces, todo aquel proceso que permita el trabajo coordinado de un bien (físico o inmaterial) con otros bienes (tangibles o intangibles) basados en la tecnología de información, siempre y cuando, dicha coordinación permita el cumplimiento de una función específica. Dentro de este concepto se abarcan, tanto a las computadoras como a los sistemas (software) operativos, pasando por las redes (tanto hardware como programas de computación) que permitan la coordinación de los recursos y procedimiento informáticos.

Una vez comprendidos estos dos conceptos, se tratarán de analizar los elementos que componen este tipo de delito, aunque la redacción de la norma atente contra estos propósitos.

El objeto jurídico protegido es la tenencia o posesión, no la propiedad, ya que no existe en toda la norma ninguna referencia a la misma. El objeto material lo constituyen bienes o valores tangibles o intangibles de carácter patrimonial, que estén en tenencia o posesión de un sujeto distinto al sujeto activo.

El primer punto a destacar es la pluralidad en el objeto material (bienes o valores), es decir, que si el hurto ha sido sobre un bien individual solamente (sólo se ha hurtado un bien o un valor), ¿sería aplicable dicha norma?. En el supuesto del hurto genérico del Código Penal no existe esta duda, porque por cada cosa mueble se estaría realizando un hurto, pero en esta norma pareciera ser un requisito que sean como mínimo dos bienes o valores (ya que no existe una previsión de un objeto material en singular), por lo cual, no sería aplicable a aquel sujeto que haya hurtado sólo un bien o un valor tangible o intangible de carácter patrimonial.

Depósito Legal: PPX200002ZU2142 / ISSN:1856-4194. Volumen 7 Edición No 2 – Año 2008

Otro aspecto derivado de estas primeras consideraciones, es que el sujeto pasivo es el tenedor o poseedor de dichos bienes o valores, sin que importe que el apoderamiento haya sido realizado con el consentimiento del propietario o titular. Se observa entonces, que el propietario o titular legítimo podría ser responsable (sujeto activo) de hurto contra el tenedor de mala fe (o el delincuente que lo haya sustraído primeramente), invirtiendo el sentido para el cual fue creado esta figura delictual, por la mala redacción de la norma en concreto.

La acción no consiste en el apoderamiento, sino en el uso de la tecnología informática como herramienta, para apoderarse, por ende, no existirá el delito de tentativa, porque para considerarse consumado el delito, basta con que exista el uso de la informática con la intención de apoderarse (no es necesario que se apodere del bien, como lo exige el Código Penal), mediante la sustracción (esta sí debe ser ejecutada) del bien. En conclusión, se separa notablemente de la acción prevista por el Código Penal, ya que la acción objetiva que determina la consumación del delito es la sustracción, complementada por la intencionalidad del sujeto activo de apodarse del bien o valor para procurarse un beneficio económico.

Ahora bien, el uso de la informática como herramienta para acceder, interceptar, interferir, manipular o usar un sistema o medio de comunicación, con la intención de sustraer un bien o valor, no es sinónimo que dicha sustracción será realizada por medios electrónicos. Un ejemplo de ello sería el uso o intercepción de mecanismos de seguridad bancarios o de otro tipo, para facilitar el acceso físico a un inmueble de donde se sustraen bienes tangibles, aunque dicha conducta (la de interferir con el funcionamiento de un sistema informático) pueda ser subsumida por otro delito (denominado sabotaje o daño a sistemas) que estudiaremos más adelante.

Otro supuesto, es que se acceda por medio del uso de las tecnologías informáticas a un medio o sistema de comunicación para sustraer un bien o valor intangible. Para ello (sustraer un bien intangible) es menester que esté plasmado en un soporte que le dé materialidad al mismo, que pudiesen ser bytes u otros, para permitir una apropiación. Un ejemplo de esto lo constituye un software en creación (en proceso de elaboración) que no tenga copia de respaldo, y que sea sustraído (no copiado), es decir, que se haya tenido acceso a los datos o instrucciones que la componen, guardadas en un computador u otro elemento electrónico, y se hayan transferido dichos archivos para otro computador (sin dejarle copia alguna al tenedor), es decir, se realizó una sustracción y el anterior tenedor ha sido despojado o desapropiado del bien o valor. Con este ejemplo sucede igual que con el anterior, ya que la mera conducta de obtener cualquier información contenida en un sistema informático, es la acción de otro delito previsto en la misma norma, denominado espionaje informático.

2.4. Fraude Informático

La estafa es un delito doloso, en la cual una persona busca un beneficio (propio o no), en perjuicio de un tercero, mediante engaños o valiéndose de un error

Depósito Legal: PPX200002ZU2142 / ISSN:1856-4194. Volumen 7 Edición No 2 – Año 2008

infundado al mismo (al tercero). Previsto por el Código Penal venezolano en su Artículo 462:

> El que, con artificios o medios capaces de engañar o sorprender la buena fe de otro, induciéndole en error, procure para sí o para otro un provecho injusto con perjuicio ajeno, será penado con prisión de uno a cinco años. La pena será de dos a seis años si el delito se ha cometido:
>
> 1. En detrimento de una administración pública, de una entidad autónoma en que tenga interés el Estado o de un instituto de asistencia social.
>
> 2. Infundiendo en la persona ofendida el temor de un peligro imaginario o el erróneo convencimiento de que debe ejecutar una orden de la autoridad.

El delito consiste en el engaño o sorpresa de una persona, para su propio perjuicio, realizado por el sujeto activo utilizando artificios u otros medios capaces de abusar de la buena fe del sujeto pasivo. No se especifican los medios por los cuales se realiza el engaño, la inducción al error o el negocio, así podrá ser por vía telefónica, vía fax, a nivel personal, por medio de apoderado, entre otras.

Esta misma conducta típica se presenta en el caso de las transacciones electrónicas, así, si una persona entra a una librería en línea y compra un producto (pagando con la tarjeta de crédito o por otro medio) y no es entregado el encargo, será una conducta típicamente prevista como estafa, ya que se ha perjudicado al comprador a través de engaños (asegurando que llegaría el producto) a favor de esta empresa, sin embargo, esta figura contractual ya está prevista en otra norma relativa a la oferta engañosa. Sería estafa en el sentido tradicional.

Igualmente, cuando se inscribe a un servicio mensual o semanal, pagadero por medio de la tarjeta de crédito (continuando con ejemplos en línea), que aseguran su actualización y esta no ocurre, se estará en caso de una estafa, ya que se ha engañado al comprador, en su perjuicio y a favor de la empresa que recibe, aunque no exista actualización, el pago. Un caso aun más claro de estafa, sería el ofrecimiento vía Internet (otro caso en línea), de un inmueble en alquiler o venta, cuando la empresa que lo ofrece no tiene ninguna injerencia sobre el mismo y es comprado o arrendado a través de dicho medio informático.

Sin embargo, ninguno de estos ejemplos son aplicables al denominado fraude informático, según la propia ley venezolana. Este está previsto en el Artículo 14 de la Ley Especial Contra los Delitos Informáticos (2001), de la siguiente manera:

> Fraude. El que, a través del uso indebido de tecnologías de información, valiéndose de cualquier manipulación en sistemas o cualquiera de sus componentes o en la data o información en ellos contenida, consiga insertar instrucciones falsas o fraudulentas que produzcan un resultado que permita obtener un provecho injusto en perjuicio ajeno, será penado con prisión de tres a siete años y multa de trescientas a setecientas unidades tributarias.

Depósito Legal: PPX200002ZU2142 / ISSN:1856-4194. Volumen 7 Edición No 2 – Año 2008

La conducta, a diferencia de la estafa tradicional, no consiste en abusar de la buena fe de otro, sino que el sujeto sobre el cual se efectúa la conducta, ni siquiera es humano, sino es un sistema o su contenido. Obviamente, el sujeto pasivo es el propietario del sistema o del contenido alterado, o aquel que haya sufrido el perjuicio.

Se observa que las diferencias entre la estafa tradicional y el fraude informático, son impresionantes, ya que, a diferencia del delito tradicional, el sujeto activo no engaña la buena fe de otro, sino que realiza una manipulación de un sistema o de su contenido, para obtener un provecho injusto en perjuicio ajeno. No es necesario que se haya accedido ilegalmente a un sistema o contenido, sino la introducción de instrucciones falsas o fraudulentas que causen ese provecho injusto en perjuicio de otro. Ejemplo: un empleado de un banco o de cualquier institución que tenga acceso al sistema informático, introduce un programa de computación que transfiere un bolívar por cada transacción superior a 1000, a una cuenta particular o de un tercero, lo cual, luego de cierto tiempo de funcionamiento, le ha reportado beneficios considerables, en perjuicio tanto de la institución en la cual trabaja como de los clientes a los cuales les haya cobrado ese bolívar adicional por los servicios que presta la compañía (Fuentes, 2007).

2.5. Violación a la privacidad de las comunicaciones

La privacidad de las comunicaciones en Venezuela, ha sido prevista por la Ley sobre Protección a la Privacidad de las Comunicaciones (Gaceta Oficial N° 34.863 del 16/12/1991), de la siguiente forma: “Artículo 2. El que arbitraria, clandestina o fraudulentamente grabe o se imponga de una comunicación entre otras personas, la interrumpa o impida será castigado con prisión de tres (3) a cinco (5) años”.

El sujeto activo es cualquier persona hacia la cual no está dirigida la comunicación. Los sujetos pasivos serán las partes de la comunicación interceptada o grabada.

La acción consiste en grabar, imponerse, interrumpir o impedir una comunicación ajena, siendo dichas conductas explicadas magistralmente por Fuentes (2007: 277) citando a Arteaga: “Grabar una comunicación implica copiarla, fijarla en cualquier instrumento apto para ello; imponerse de una comunicación supone tomar conocimiento de ella, total o parcialmente; interrumpirla quiere decir hacerla cesar después de iniciada; e impedirla supone que no se permita su inicio”.

La condición de dichas acciones es que sean realizadas arbitrariamente, es decir, sin tener derecho o autorización judicial para ello. Clandestina, en el sentido de ser la grabación o intercepción desconocida por parte de los sujetos de la comunicación (en el supuesto que los medios por los cuales se realiza la comunicación sean de otro y éste condicione el uso del mismo a la posibilidad de acceso a dicha información, como podrían ser los email corporativos, no se consumiría dicho delito), o por medios fraudulentos, lo que debe entenderse como todos aquellos que se emplean en desconocimiento de la ley (es un criterio amplio

Depósito Legal: PPX200002ZU2142 / ISSN:1856-4194. Volumen 7 Edición No 2 – Año 2008

que pretende abarcar los demás supuestos no previstos expresamente), en perjuicio de terceros (en este caso del derecho a la privacidad e intimidad). En los tres supuestos, ha existido la intención de acceder a la comunicación y se han empleado medios para conseguir dicho fin, por ende, ha sido una conducta dolosa por parte del sujeto activo.

Igualmente, existe un antecedente a la conducta tipificada por la Ley Especial Contra Delitos Informáticos (2001), prevista por el Código Penal venezolano (1964 reformado en el 2005), específicamente en su Artículo 186 que establece: "Cualquiera que haya suprimido indebidamente alguna correspondencia epistolar o telegráfica que no le pertenezca, aunque estando cerrada no la hubiera abierto, será castigado con arresto de uno a seis meses". El término suprimir es equiparable a la acción de borrar un mensaje almacenado en un sistema que utilice tecnología de información, prevista por la norma estudiada.

La Ley Especial Contra Delitos Informáticos (2001), ha hecho una adaptación a los anteriores dispositivos legales, al contemplar como delito a la violación de la privacidad de las comunicaciones, lo siguiente:

> Artículo 21. Violación de la privacidad de las comunicaciones. El que mediante el uso de tecnologías de información, acceda, capture, intercepte, interfiera, reproduzca, modifique, desvíe o elimine cualquier mensaje de datos o señal de transmisión o comunicación ajena, será sancionado con prisión de dos a seis años y multa de doscientas a seiscientas unidades tributarias.

Las acciones son el acceso (llamado anteriormente imponerse de una comunicación, y consiste en tomar conocimiento del contenido, bien total o parcial, de una comunicación privada), captura (prevista anteriormente como grabar y consiste en la fijación total o parcial del contenido de la comunicación en materiales tangibles o en archivos digitales que permitan recuperarla), intercepción (significa que no se ha permitido que el mensaje o la comunicación enviada o comenzada llegue a su destino), interferencia (es la acción de perturbar la comunicación), reproducción (previsto en la norma anterior como copia), modificación (consiste en cambiar el contenido, parcial o totalmente, de una comunicación, y puede ser realizada sobre la grabación, el mensaje enviado o en cualquier otro momento técnico donde exista dicha comunicación), desvío (consiste en la intercepción de la comunicación pero con la característica adicional que la misma es reenviada a una dirección o persona distinta a la originalmente prevista) o eliminación (significa borrar, pero dicho término sólo es posible si existe una manifestación física de la comunicación o de la transmisión, siendo aplicable principalmente al mensaje de datos).

Las anteriores acciones pueden ser dolosas (como la modificación, desvío, captura, intercepción, reproducción o eliminación) o culposa, es decir, sin intención o propósito de realizar dicha acción (acceso e interferencia).

Depósito Legal: PPX200002ZU2142 / ISSN:1856-4194. Volumen 7 Edición No 2 – Año 2008

La mala redacción de la norma, permite que cualquier acceso o interferencia, aunque sea por culpa del sistema informático y no de una conducta del sujeto, sea causal para considerarse consumido el delito, lo cual es totalmente injustificado. Otro aspecto importante derivado de la redacción, es que no prevé la posibilidad de realizar dichas acciones con la autorización de un tribunal competente, por lo cual, podrían las autoridades que se presten a dichas conductas, ser juzgadas, aunque esa acción haya sido determinante para evitar un crimen o acto terrorista. Es de observar que el Artículo 48 de la Constitución de la República Bolivariana de Venezuela (1999) establece con respecto a la posibilidad de grabar comunicaciones y emplearlas como medios probatorios en juicios, lo siguiente:

> Se garantiza el secreto e inviolabilidad de las comunicaciones privadas en todas sus formas. No podrán ser interferidas sino por orden de un tribunal competente, con el cumplimiento de las disposiciones legales y preservándose el secreto de lo privado que no guarde relación con el correspondiente proceso.

2.6. Violaciones a la privacidad de la data o información

La Ley Especial Contra Delitos Informáticos (2001), prevé tres conductas delictivas que protegen un mismo bien jurídico: la privacidad, manifestada en estos supuestos, por medio de la protección al contenido de la data o información almacenada o guardada en un sistema que utilice tecnologías de información o en cualquiera de sus componentes físicos.

Sin embargo, esta protección no es novedosa, aunque sí lo sean, los elementos para acceder a ella y las formas de almacenamiento, manejo y recuperación de la data o información.

Por data, la ley especial entiende en su Artículo 2 Ordinal c, a los: “hechos, conceptos, instrucciones o caracteres representados de una manera apropiada para que sean comunicados, transmitidos o procesados por seres humanos o por medios automáticos y a los cuales se les asigna o se les puede asignar significado”.

El término data, empleado en la ley especial, no es el más acorde para identificar el concepto expuesto, ya que este es entendido por la Real Academia Española (2003), como:

> “1.f. Nota o indicación del lugar y tiempo en que se hace o sucede algo y especialmente la que se pone al principio o al fin de una carta o de cualquier otro documento. 2.f. Tiempo en que ocurre o se hace algo. 3.f. Abertura para desviar de un embalse o de una corriente de agua parte de su caudal. 4.f. Com. En una cuenta, partida o partidas que componen el descargo de lo recibido. 5.f. ant. Permiso por escrito para hacer algo”.

Depósito Legal: PPX200002ZU2142 / ISSN:1856-4194. Volumen 7 Edición No 2 – Año 2008

Por lo que vemos, ninguna de las cinco acepciones contenidas se aproxima al concepto expuesto por la ley especial. Mientras que el término dato(s), es entendido, por la Real Academia Española (2003), como:

> "1.m. Antecedente necesario para llegar al conocimiento exacto de algo o para deducir las consecuencias legítimas de un hecho. 2.m. Documento, testimonio, fundamento. 3.m. Inform. Información dispuesta de manera adecuada para su tratamiento por un ordenador".

Por ello, y empleando las directrices en el uso del castellano propuestas por la Real Academia Española, se opta por el empleo del término dato(s), como el más cercano y acorde, con el concepto expuesto por la ley especial.

Mientras, que el término información consiste en el: "significado que el ser humano le asigna a la data utilizando las convenciones conocidas y generalmente aceptadas" (Ley Especial Contra Delitos Informáticos. Artículo 2 Ordinal d).

La inviolabilidad del contenido de una carta o un telegrama, como medios idóneos (en épocas pasadas) para transmitir datos o informaciones a distancia, son protegidas por normas penales, prevista por el Código Penal venezolano (1964 reformado en el 2005), de la siguiente manera:

> Artículo 185. El que indebidamente abra alguna carta, telegrama o pliego cerrado que no se le haya dirigido, o que indebidamente lo tome para conocer su contenido, aunque no esté cerrado, perteneciendo a otro, será castigado con arresto de ocho a veinte días.
>
> Si divulgando el contenido, el culpable ha causado algún perjuicio, la pena será de quince días a diez meses de arresto.

Con los nuevos medios de comunicación a distancia, que permiten el intercambio de datos e informaciones, la protección penal prevista se hizo insuficiente, por lo cual, en la Ley sobre Protección a la Privacidad de las Comunicaciones (1991), específicamente en el único aparte del Artículo 2 se establece:

> "En la misma pena incurrirá, salvo que el hecho constituya delito más grave, quien revele, en todo o en parte, mediante cualquier medio de información, el contenido de las comunicaciones indicadas en la primera parte de este artículo".

De ambos delitos, se deriva que la protección de dichos datos o informaciones están condicionadas al uso de medios que permitan la comunicación a distancia (cartas, telegramas, teléfonos, internet, etc.). Es en este aspecto, donde efectivamente existe un avance con respecto a las previsiones anteriores, ya que la protección a la data o información no está condicionada al empleo de medios de comunicación a distancia, sino al uso de sistemas de tecnologías de información, lo que incluye, aquellos datos e informaciones que están almacenados, contenidos o

Depósito Legal: PPX200002ZU2142 / ISSN:1856-4194. Volumen 7 Edición No 2 – Año 2008

guardados de manera estacionaria en un sistema informático o en alguno de sus componentes.

La primera conducta a estudiar, es la que lleva una sanción mayor, y en su tipología es más amplia que las demás, siendo prevista por la ley especial de la siguiente manera:

> Artículo 11.- Espionaje informático. El que indebidamente obtenga, revele o difunda la data o información contenidas en un sistema que utilice tecnologías de información o en cualquiera de sus componentes, será penado con prisión de cuatro a ocho años y multa de cuatrocientas a ochocientas unidades tributarias.
>
> La pena se aumentará de un tercio a la mitad, si el delito previsto en el presente artículo se cometiere con el fin de obtener algún tipo de beneficio para sí o para otro.
>
> El aumento será de la mitad a dos tercios, si se pusiere en peligro la seguridad del Estado, la confiabilidad de la operación de las instituciones afectadas o resultare algún daño para las personas naturales o jurídicas como consecuencia de la revelación de las informaciones de carácter reservado.

Existen tres conductas prohibidas: (a) La obtención: consistente en la acción de conseguir, que no se basta en el mero acceso, sino que deben ser reproducidos o extraídos dichos datos o informaciones del sistema donde estén contenidos; (b) revelación: consiste en presentar la información o datos obtenidos a una o varias personas determinadas, que no tenían acceso previo a dicho material; o (c) difusión: es la presentación pública de dichos datos o informaciones, como por ejemplo, la publicación en una página web, sin tener un receptor definido, siendo libre (en el sentido de ausente de restricciones) su acceso.

El objeto material sobre el cual debe recaer cualquiera de estas acciones, son los datos o informaciones (independientemente que ésta ya sea conocida por el público receptor) contenidos en un sistema que utilice tecnologías de información (computadoras, celulares, agendas electrónicas, etc.) o en cualquiera de sus componentes (memorias, cd, diskettes, etc). No es un requisito que dichos datos o informaciones, sean efectivamente desconocidos o secretos.

Existen dos agravantes a este delito: (a) Si existe un beneficio para quien realiza la acción o para un tercero; o (b) Si existe perjuicio para el sujeto pasivo (Estado, personas jurídicas y/o naturales) como consecuencia de la revelación de una información reservada (en esta agravante, es menester que dicha información sea secreta o reservada).

Los otros dos delitos se cometen contra un objeto material más limitado, ya que no es sobre cualquier tipo de dato o información, sino sólo aquellas de carácter

Depósito Legal: PPX200002ZU2142 / ISSN:1856-4194. Volumen 7 Edición No 2 – Año 2008

personal. Por el término carácter personal, debe entenderse a todo dato o información relativa a la persona (como historiales financieros, educativos, médicos, legales, etc), e incluye a la vida íntima y/o familiar de la misma.

El primero de ellos, consiste en el apoderamiento, utilización, modificación o eliminación de una información o datos personales de otro (como un inventario de bienes, un historial bancario, un informe médico o sobre sus gustos políticos, ideológicos, religiosos, sociales, sexuales, etc.) o aquellos en los que el sujeto activo tenga algún interés legítimo (por ejemplo: el archivo de notas de una institución educativa, o los antecedentes penales guardados en archivos estatales), que estén incorporadas (almacenadas) en un sistema que utilice tecnología de la información, siempre y cuando, dichas conductas no hayan sido autorizadas por el dueño (el cual no implica que sea la misma persona sobre la que versen los archivos personales) de la información o datos.

Es prevista por el Artículo 20 de la siguiente forma:

> Violación de la privacidad de la data o información de carácter personal. El que por cualquier medio se apodere, utilice, modifique o elimine, sin el consentimiento de su dueño, la data o información personales de otro o sobre las cuales tenga interés legítimo, que estén incorporadas en un computador o sistema que utilice tecnologías de información, será penado con prisión de dos a seis años y multa de doscientas a seiscientas unidades tributarias.
>
> La pena se incrementará de un tercio a la mitad si como consecuencia de los hechos anteriores resultare un perjuicio para el titular de la data o información o para un tercero.

El delito siguiente, es totalmente injustificado al ser una reiteración, ya que el mismo está previsto y sancionado por el artículo 11 (analizado en líneas anteriores), y consiste en revelar la información o los datos obtenidos sin el consentimiento de su dueño o propietario, con la salvedad que en este supuesto específico (el previsto por el Artículo 22), el objeto material es una información o dato personal, mientras que en el supuesto del Artículo 11, el objeto material es cualquier información o dato contenido en un sistema que utilice tecnologías de información. El único tipo penal aplicable de este artículo sería, cuando dicha información o datos revelados hayan sido obtenidos violando la privacidad de las comunicaciones.

> Artículo 22.- Revelación indebida de data o información de carácter personal. El que revele, difunda o ceda, en todo o en parte, los hechos descubiertos, las imágenes, el audio o, en general, la data o información obtenidos por alguno de los medios indicados en los artículos precedentes, aún cuando el autor no hubiese tomado parte en la comisión de dichos delitos, será sancionado con prisión de dos a seis años y multa de doscientas a seiscientas unidades tributarias.

Depósito Legal: PPX200002ZU2142 / ISSN:1856-4194. Volumen 7 Edición No 2 – Año 2008

Si la revelación, difusión o cesión se hubieren realizado con un fin de lucro o si resultare algún perjuicio para otro, la pena se aumentará de un tercio a la mitad.

Conclusiones

La Ley Especial Contra Delitos Informáticos, si bien es cierto que representó un adelanto legislativo en la materia en su momento, también lo es que algunas de sus normas tipo previstas, carecen de una redacción clara y jurídicamente adecuada, lo cual produce como resultado una inseguridad jurídica emanada de los errores en la tipicidad normativa, según se ha demostrado en el análisis críticos a algunos de los delitos por ella previstos, esperando sirva de ayuda, en una futura reforma a la misma.

Referencias bibliográficas

Diccionario de la Real Academia de la Lengua Española. (RAE). (2008). Consultado el día 18 de febrero de 2008 en la página www.rae.es.

Fuentes, F. (2007). *Marco Legal de la Informática y la Computación*. Caracas: Vadell Hermanos.

Grisanti, H. (2000). *Lecciones de Derecho Penal Parte General*. Caracas: Vadell Hermanos.

Jiménez, L. (1980). *La Ley y el Delito*. Buenos Aires: Sudamericana.

Mendoza, J. (1986). *Curso de Derecho Penal Venezolano*. Caracas: Empresa el cojo.

Leyes

Código Penal de 1964, reformado en el 2005 y publicado en Gaceta Oficial Nº 5.768 (Extraordinaria) de fecha 13 de Abril del 2005.

Ley Especial Contra Delitos Informáticos, publicada en la Gaceta Oficial Nº 37.313 del 30 de noviembre del 2001.

Ley Sobre la Protección a la Privacidad de las Comunicaciones, publicada en Gaceta Oficial Nº 34.863 del 16 de diciembre de 1991.

Depósito Legal: PPX200002ZU2142 / ISSN:1856-4194. Volumen 7 Edición No 2 – Año 2008