EL BIEN JURÍDICO TUTELADO DE LA INFORMACIÓN Y LOS NUEVOS VERBOS RECTORES EN LOS DELITOS ELECTRÓNICOS.

EL FRAUDE ELECTRÓNICO

***Alexander Díaz García**

1. INTRODUCCIÓN

Antes de entrar de lleno al planteamiento del meollo del asunto, es indispensable establecer algunos conceptos fundamentales para partir de una base común.

La mayoría de los autores se refieren al tema que hoy nos ocupa, DELITOS INFORMÁTICOS, sin detenerse a reflexionar que, para poder hablar de un delito informático, son necesarios dos presupuestos básicos, uno que la conducta constitutiva del mismo esté tipificada por la Ley y dos, que medie una sentencia condenatoria en la cual el Juez Penal haya declarado probada la existencia concreta de una conducta típica, antijurídica y culpable del delito informático. Hoy trataré en este sagrado recinto de resumir y explicar mi posición del bien jurídico turtelado de la información (almacenada, tratada y transmitida a través de sistemas informáticos), en toda su amplitud, titularidad, autoría, integridad, disponibilidad, seguridad, transmisión, confidencialidad e intimidad, sin perjuicio de que con su vulneración subsidiariamente y en tratandose de intereses colectivos, afecte otros bienes jurídicos como la propiedad generalmente. Les expondré como mi modelo es un decálogo de conductas tipos autónomos y no subordinados ora circunstancias genéricas o específicas de agravación punitiva de otros tipos, como ha sido la costumbre legislativa en el mundo. Igualmente observarán que algunos tipos están en el idiona inglés porque muchos de esas conductas están en ese idioma o su texto original en ese idioma han sido modificados caprichosamente por los hackers y he tratado de darle una aproximación al Español, tornándose bien dificil su castellanizción, no obstante se nos torna obligada por técnicas legislativas colombianas hacerlo.

Finalmente he dejado al libre albedrio del legislador el quantum punitivo de las conductas tipo, pues con base al trabajo legislativo y a la política criminal establecida para el momento, esa Corporación cuenta con cuadros estadísticos, informes y otras fuentes, que permitirán sancionar adecuadamente la conducta informática.

Bien Jurídico

A lo largo de la evolución de la disciplina se han ido distinguiendo diversos conceptos de lo que representa el bien-jurídico.

El concepto dogmático de bien jurídico, acuñado por Birnbaum a mediados del S. XIX, se refiere a los bienes que son efectivamente protegidos por el Derecho. Esta concepción es demasiado abstracta y por ello no cumple con la función delimitadora del *Ius puniendi* que pretendemos revelar en el presente estudio.

Según Von Liszt, y bajo una concepción material del bien jurídico, su origen reside en el interés de la vida existente antes del Derecho y surgido de las relaciones sociales. El interés social no se convierte en bien jurídico hasta que no es protegido por el Derecho.

El concepto político criminal del bien jurídico trata de distinguir el bien jurídico de los valores morales, o sea trata de plasmar la escisión entre Moral y Derecho, que si bien a veces pueden coincidir en determinados aspectos, no deben ser confundidas en ningún caso. Esta concepción del bien jurídico es obviamente fruto de un Estado Social y Democrático de Derecho, y dada su vertiente social, requiere una ulterior concreción de la esfera de actuación del Derecho penal a la hora de tutelar intereses difusos.

El origen del bien jurídico está por tanto, en la pretensión de elaborar un concepto del delito previo al que forma el legislador, que condicione sus decisiones, pretensión característica de una concepción liberal del Estado, que concibe este como un instrumento que el individuo crea para preservar los bienes que la colectividad en su conjunto crea de suma conveniencia proteger.

En otras palabras el bien jurídico es la elevación a la categoría del bien tutelado o protegido por el derecho, mediante una sanción para cualquier conducta que lesione o amenace con lesionar este bien protegido, de esta reflexión se puede decir que el bien jurídico obtiene este carácter con la vigencia de una norma que lo contenga en su ámbito de protección, mas si esta norma no existiera o caduca, éste no deja de existir pero si de tener el carácter de jurídico.

Esta característica proteccionista que brinda la normatividad para con los bienes jurídicos, se hace notar con mayor incidencia en el derecho penal, ya que es en esta rama del derecho en que la norma se orienta directamente a la supresión de cualquier acto contrario a mantener la protección del bien jurídico, por ejemplo el delito de espionaje informático busca sancionar los actos que difunden en forma irregular la información privilegiada industrial o comercial a través de medios electrónicos.

En la actualidad la conceptualización del bien jurídico, no ha variado en su aspecto sustancial de valoración de bien a una categoría superior, la de bien tutelado por la ley, en cuanto a ciertos criterios como el origen, o como el área del derecho que deba contenerlos.

El Derecho penal tiene su razón de ser en un Estado social porque es el sistema que garantiza la protección de la sociedad a través de la tutela de sus bienes jurídicos en su calidad de intereses muy importantes para el sistema social y por ello protegibles por el Derecho penal.

Pero no hay que olvidar que existen bienes jurídicos que no son amparados por el Derecho penal por ser intereses sólo morales y por ello sabemos que no todos los bienes jurídicos son bienes jurídico-penales y debemos distinguirlos.

Bienes jurídico-penales

Un Estado social y democrático de Derecho debe amparar sólo las condiciones de la vida social en la medida en que éstas perturben las posibilidades de participación de los individuos en el sistema social. Por tanto los bienes jurídicos serán jurídico-penales sólo si revisten una importancia fundamental, o sea cuando las condiciones sociales a proteger sirvan de base a la posibilidad de

participación de los individuos en la sociedad. En un Estado democrático cabe destacar la importancia de la participación de los individuos de vivir en sociedad confiando en el respeto de la propia esfera de libertad individual por parte de los demás.

Otra característica esencial de los bienes jurídico-penales es la necesidad de protección de los mismos, o sea que a través de otros medios de defensa que requirieran menos intervención y por tanto fueran menos lesivos no se logre amparar satisfactoriamente el bien.

El bien jurídico nace de una necesidad de protección de ciertos y cambiantes bienes inmanentes a las personas como tales, esta protección es catalizada por el legislador al recogerlas en el texto constitucional, de la cual existirían bienes cuya protección será cumplida por otras ramas del derecho, es decir que no todos los bienes jurídicos contenidos en la constitución tienen una protección penal, existen bienes jurídicos de tutela civil, laboral, administrativa etc. Aquellos bienes jurídicos cuya tutela sólo y únicamente puede ser la tutela penal, son los denominados bienes jurídicos penales; al determinar cuales son los bienes jurídicos que merecen tutela penal, siempre se tendrá en cuenta el principio de tener al derecho penal como ultima ratio o última opción para la protección de un bien jurídico ya que este afecta otros bienes jurídicos a fin de proteger otros de mayor valor social. De otro lado es claro que no aparece otro factor que se revele como más apto para cumplir con la función limitadora de la acción punitiva, pues como hemos observado sólo los bienes jurídicos de mayor importancia para la convivencia social y cuya protección por otras ramas del derecho hagan insuficiente la prevención que cualquier transgresión los afecte.

Principio de la Intervención Mínima de la Actuación Punitiva del Estado.

Es el principio que restringe el campo de la libertad y que mediante la pena, priva de derechos fundamentales o condiciona su ejercicio, por una parte, debe ser el último de los recursos (*ultima ratio)* de los que el mismo tiene a su disposición para tutelar los bienes jurídicos y, por otra parte, debe ser lo menos gravoso posible para los derechos individuales, mientras resulte adecuado para alcanzar los fines de protección que se persiguen. Ello significa que:

1) El Derecho Penal sólo es aplicable cuando para la protección de los bienes jurídicos se han puesto en práctica otras medidas no represivas, que pueden ser, por ejemplo, de carácter laboral, administrativo o mercantil, y ellas han resultado insuficientes; por tanto, sería desproporcionado e inadecuado comenzar con una protección a través del Derecho Penal.

2) El Estado debe graduar la intervención sancionadora administrativa y penal, de modo que siempre que sea posible alcanzar el amparo del bien jurídico mediante el recurso a la potestad sancionadora de la Administración, debe preferir ésta a la penal, por ser menos gravosa, al menos para las conductas menos dañosas o menos peligrosas.

Se debe entender entonces que el carácter subsidiario del Derecho Penal frente a los demás instrumentos del ordenamiento jurídico y, así mismo, su carácter fragmentario, en cuanto no tutela todos los ataques a los bienes jurídicos relevantes sino únicamente los más graves o más peligrosos.

El Derecho Penal sólo es aplicable cuando para la protección de los bienes jurídicos se han puesto en práctica otras medidas no represivas, que pueden ser, por ejemplo, de carácter laboral, administrativo o mercantil, y ellas han resultado insuficientes; por tanto, sería desproporcionado e inadecuado comenzar con una protección a través del Derecho Penal.

2. NATURALEZA JURÍDICA DEL BIEN JURÍDICO TUTELADO DE LA INFORMACIÓN

Para algunos el delito informático es sólo la comisión de delitos mediante el uso de los computadores, pues considera que en realidad no existe un bien jurídico protegido en el delito informático, porque en realidad no existe como tal dicha conducta. Esto no es más que una nueva forma de ejecución de conductas que afecta bienes jurídicos que ya gozan de protección por el derecho penal.

Otros opinan que estos delitos tienen un contenido propio, afectando así un nuevo bien jurídico. La Información diferenciando los delitos computacionales y los delitos informáticos propiamente dichos.

Y finalmente una tercera corriente considera que los delitos informáticos deben ser observados desde un punto de vista triple:

Como fin en si mismo, pues el computador puede ser objeto de la ofensa, al manipular o dañar la información que este pudiera contener;

Como medio: Como herramienta del delito, cuando el sujeto activo usa el ordenador para facilitar la comisión de un delito tradicional

Como objeto de prueba: Los computadores guardan pruebas incidentales de la comisión de ciertos actos delictivos a través de ellos

El bien jurídico ha sido y será la valoración que se haga de las conductas necesarias para una vida pacífica, recogidas por el legislador en un determinado momento histórico–social; es la razón de que a nuestro entender el bien jurídico en esencia no desaparece, solo cambia en cuanto al ámbito de protección que lo sujeta, el desarrollo de esta institución jurídica pasa por momentos totalmente distintos ya que los mismos son producto de las necesidades propias del desarrollo de la sociedad, hay que tener en claro que estos no se originan al crear una norma, su existir es previo a la misma; esto es, en un primer momento, el primer paso para la protección de un bien de suma importancia para el conjunto social, la selección de estas necesidades valoradas socialmente y luego positivizadas sea en las páginas de una constitución o de algún convenio internacional, será el segundo paso de nuestra construcción, para una vez terminado la nueva categoría de bienes a protegerse, determinar cuales son verdaderamente materia de protección penal. Los bienes

jurídicos expresan necesidades básicas de la persona y los procesos de relación social, de instituciones, sistemas y de su participación.

El bien jurídico se justifica como categoría límite al poder punitivo del Estado, un obstáculo capaz de impedir arbitrariedades, distorsiones o confusiones en la elaboración de la estructura penal; las funciones de garantía son inherentes al bien jurídico penal y se vincula a la relación individuo-Estado. Bajo el mecanismo de garantía resulta posible denunciar todos los elementos que amenacen o avasallen a la persona en su relación con el Estado. Las funciones de interpretación de la norma penal, conducirá siempre al bien jurídico, en cuya sede se pueden establecer criterios esclarecedores o correctivos de los alcances de la protección a fin de evitar distorsiones en la comprensión del contenido de los bienes jurídicos en concreto.

Resulta importante la definición de los elementos fundamentadores del bien jurídico penal. Por regla general, no todo es considerado "bien jurídico penal" y por el contrario, sólo algunos comportamientos pasarán a ser calificados como tales en virtud del lus necessitatis, que se conecta con el principio de reserva de la ley penal.

De la punibilidad

Finalmente dejo en completa libertad al Señor Legislador, pues no la establezco, la tasación punitiva, tanto en penas aflictivas de la libertad como de penas pecuniarias, pues es el Congreso de la República el que más conoce y mejor a través del trabajo de campo de investigaciones, las estadísticas del impacto que produce el delito electrónico en la sociedad de la información y así establecerá la correspondiente política criminal para atacar este flagelo.

Como sugerencia final establezco lo prudente que se torna denunciar todo comportamiento doloso informático al Centro de Denuncias de Delitos en Internet el IC3, su site está en wwww.ic3.gov, en donde cualquier persona podrá poner en conocimiento los hechos ilícitos electrónicos.

3. ANÁLISIS DOGMÁTICO DE LOS DELITOS ELECTRÓNICOS DEL PROYECTO

ARTÍCULO PRIMERO: ESPIONAJE INFORMÁTICO. El que se apodere, interfiera, fugue, transmita, copie, modifique, destruya, utilice, impida o recicle datos de valor para el tráfico económico de la industria o comercio, incurrirá en prisión de a años y multa de …….smmlv.

Elementos Estructurales del Delito:

Sujeto Activo: El sujeto activo de la conducta es indeterminado, pues no se hace ninguna calificación al respecto.

Sujeto Pasivo: El sujeto pasivo son los industriales o comerciantes, oficiales o particulares, que manejen esta clase de información.

Objeto Jurídico: El objeto jurídico en principio es la información privilegiada industrial o comercial.

Objeto Material: El objeto material de la conducta es la transmisión de la información privilegiada.

Conducta: Los verbos rectores de las conductas son apoderar, interferir, fugar, transmitir, copiar, modificar, destruir, utilizar, impedir y reciclar.

Comentario: El tipo pretende proteger la información privilegiada industrial o comercial que no debe salir de la órbita de su titular o encargado de manipular. Se castiga la falta de sigilo o confidencialidad de los profesionales, responsable o encargado de los ficheros de los datos automatizados empresariales.

ARTÍCULO SEGUNDO: ACCESO ILEGÍTIMO A SISTEMAS INFORMÁTICOS. El que haga uso de los medios informático o de telecomunicaciones y sus soportes de información, programas y sistemas operativos, de aplicaciones de seguridad, poniendo en riesgo la confidencialidad, seguridad, integridad y disponibilidad de la información que se procesa, intercambia, reproduce, conserva o tramite, incurre en pena de prisión de a años de prisión y multa de …….smmlv

Parágrafo: Si los hechos descritos en el artículo anterior se cometen en redes o sistemas estatales, gubernamentales, de organizaciones comerciales o educativas, nacionales, internacionales o de país extranjero, la sanción es de a años de prisión y multa de smmlv

Elementos Estructurales del Delito:

Sujeto Activo: No es calificado o indeterminado.

Sujeto Pasivo: Cualquier persona que sea dueña de un sistema de procesamiento de información,

Objeto Jurídico: La confidencialidad, seguridad, integridad y disponibilidad de la información

Objeto Material: La conducta protege el acceso ilegal a sistemas de información y protección de su contenido.

Conducta: El verbo rector está dado por la palabra ingresar, usar ilegalmente información sin estar autorizado.

Comentario: Se le conoce en el medio como White hacking, porque quieren demostrarle al sistema de seguridad en donde acceden y lo capaces que son. En el Ethical hacking no es admisible esta conducta, toda vez que se sugiere un contrato para hacer esta clase de asaltos informáticos.

ARTÍCULO TERCERO: BLOQUEO ILEGÍTIMO A SISTEMAS INFORMÁTICOS: El que, sin estar facultado, emplee medios tecnológicos que impidan a persona autorizada acceder a la utilización lícita de los sistemas o redes de telecomunicaciones, incurre en sanción de a años de prisión y multa de ……..smmlv.

Parágrafo: Si el bloqueo genera riesgo a la seguridad nacional la pena se aumentará de una tercera parte a la mitad.

Elementos Estructurales del Delito:

Sujeto Activo: No calificado e indeterminado

Sujeto Pasivo: Cualquier persona

Objeto Jurídico: La información en general

Objeto Material: Va dirigida a la protección de los sistemas informáticos

Conducta: Los verbos rectores de la conducta son impedir o bloquear.

Comentario: Se le conoce también como extorsión informática, pues el delincuente bloquea el sistema hasta cuando no se le cancele una suma de dinero. El caso más patético es el caso de Hackers turcos y eslovenos tomaron como rehén la página de un club de fútbol colombiano Tienen tomada la web del Envigado FC, un equipo de la segunda división. El portavoz de la institución aseguró que no pagarán el rescate y que ya están trabajando en otro dominio. Aunque explicó: "Esto nos cortó el contacto con empresarios del extranjero que entraban al sitio a ver los videos de los jugadores que estaban disponibles". También se conoce de personas que por alguna razón de confianza han logrado acceder a cuentas de correo electrónicos y que luego por alguna indisposición se distancian éstas pero siguen conociendo de las claves de acceso, modifican éstas e impiden que el titular de la cuenta la abra, realizando diversos comportamientos, incluso difamar del titular de la dirección electrónica. Recordemos el caso de la novia que se distancia de su pareja y aquella conociendo el password de su email accede al correo y le modifica la contraseña para luego comenzar a difamar de la titular de la cuenta a todos los corresponsales o contactos que están registrados.

Artículo Cuarto: Uso de Virus (software malicioso). El que produzca, trafique, adquiera, distribuya, venda, envíe, introduzca o extraiga del territorio nacional virus (software malicioso) u

otros programas de computación de efectos dañinos, incurre en sanción de privación de libertad de a años y multa de ……smmlv.

Parágrafo: La pena prevista en este artículo se aumentará hasta en la mitad si la conducta se realizare por empleado o contratista del propietario del sistema informático o telemático o por un servidor público con provecho para sí o para un tercero.

Elementos Estructurales del Delito:

Sujeto Activo: Cualquier persona, no cualificado.

Sujeto Pasivo: Cualquier persona

Objeto Jurídico: Proteger el software

Objeto Material:

Comentario: Aldo B. Castelar, en su trabajo comentarios sobre EL LIBRO DE LOS VIRUS de Mark Ludwig, publicado en http://www.ubik.com.ar/vr/vr15/black.htm, realiza algunas reflexiones que se tornan interesantes conocerlas y que me permito transcribirlas. "Se escribieron muchos libros sobre los virus, pero pocos tan famosos y polémicos como éste. En vez de explicar cómo librarse de los virus, este explica cómo hacerlos. Para saber cuál es el tono general de este libro, hay que leer la cita bíblica que lo precede: 'Y Dios vio que era bueno. Y Dios los bendijo, diciendo "Sean fructíferos y multiplíquense." Génesis 1:21,22. Esto ya nos dice todo sobre el libro. Por otro lado, la contratapa dice "Advertencia. Este libro contiene código fuente completo de virus informáticos vivos, los que pueden ser extremadamente peligrosos en las manos de personas incompetentes. Usted puede ser responsable legalmente por el mal uso de estos virus, aún si este mal uso no fue intencional. No intente ejecutar ningún código de este libro a menos que esté bien versado en programación a bajo nivel para computadoras personales, y esté trabajando en un sistema cuidadosamente controlado y aislado."

La obra se desarrolla entre estas dos frases: Constantemente explica cómo se hacen los virus, cómo funcionan, pero advierte que el mal uso de la información presentada puede ser peligrosa. El autor, Mark Ludwig, sabe que mucha gente está esperando que los virus presentados en el libro causen problemas para hacerlo responsable, e intenta cubrirse como puede. De todas formas, en Estados Unidos está garantizado por la constitución el derecho a publicar cualquier clase de literatura, por más peligrosa que pueda ser considerada la información publicada. El libro está dedicado a explicar en la forma más sencilla y didáctica posible cómo hacer un virus, desde los más sencillos hasta los un poco más sofisticados. No explica técnicas muy novedosas, pero una persona puede aprender a programar un virus con este libro, sin duda. Se le ha criticado mucho que contiene muchos errores, y es cierto, pero la claridad con que explica los conceptos hace que cualquiera pueda corregir esos errores con algunos conocimientos de assembler.

El libro empieza con una introducción que dice que éste es el primero de una serie de tres. El segundo explicará los usos de los virus para simulaciones en investigación para vida artificial, y el tercero hablará sobre los usos militares de los virus. En la introducción habla sobre por qué no se puede hacer ilegal la posesión o la escritura de virus, y hace todo un discurso político sobre el tema. A continuación explica las bases del funcionamiento de los virus, y las herramientas necesarias para hacerlos. El primer virus que empieza a describir es uno llamado Timid, escrito, como todos los otros en el libro, por el mismo Ludwig, con propósito de explicar su funcionamiento. Es un virus muy sencillo, no es residente, y sólo infecta archivos .COM en el directorio actual del disco. Mientras explica cómo funciona su virus, va mostrando el funcionamiento de cada elemento del DOS que usa, cómo encontrar archivos, cómo modificarlos, etcétera. El segundo virus que explica, llamado Intruder, es un infector de .exe. Para explicar su funcionamiento describe con lujo de detalles cómo es el header del .exe y como modificarlo, que es lo más difícil de un virus de este tipo. Este virus ya es más sofisticado porque busca posibles víctimas en otros directorios además del actual. Tampoco es residente, y tiene un mecanismo de protección anti-detección que hace que no infecte archivos cada vez que es ejecutado, como para que sea más difícil saber que algo raro está pasando.

El tercer virus que presenta es el Kilroy, un virus de boot sector. Para presentarnos este virus primero explica cómo funciona un boot sector. El virus es extremadamente simple: se va a reproducir sólo en el momento de botear, no es residente, y ocupa solamente el sector de boteo. En vez de guardar el sector original y ejecutarlo después de él, va a intentar cargar el DOS por su cuenta. Infecta diskettes y discos rígidos. Es un virus extremadamente simple, tan simple que no va a tener prácticamente posibilidades de reproducirse.

El siguiente virus se llama Stealth, y es un virus mucho más complicado. Es de boot sector, residente, y tiene algunas características de stealth. En los diskettes se copia a tres sectores vacíos que marca como malos, y en los discos rígidos se copia al espacio vacío que hay después de la tabla de particiones. Si el virus está en memoria va a implementar un mecanismo de stealth que ocultará el virus de las lecturas al boot sector. Toma la interrupción 13h para infectar los diskettes que se le pongan a su alcance, y para implementar su stealth.

El resto del libro son los códigos fuentes comentados de cada uno de los virus, con instrucciones precisas de cómo cargarlos y hacerlos funcionar. También incluyen los códigos hexadecimales para tipear el virus directamente en forma binaria ejecutable.

Como vemos, no es tan peligroso como lo pintan, ya que el único virus realmente peligroso e infeccioso que trae es el Stealth. Los demás son virus muy sencillos y muy poco infecciosos. De todas formas, mucha gente ha aprendido a hacer virus con este libro, por lo cual debemos tomarlo con mucha precaución. Es simplemente un manual para la creación de virus sencillos, y no es mucho más que eso.

Aldo B. Castelar es consultor en informática en varias empresas, y se desempeña en el campo de las comunicaciones y de la programación a bajo nivel. También es redactor de Virus Report. Ha cursado estudios no formales en filosofía y en literatura. Puede ser contactado en aldo@ubik.to

ARTÍCULO QUINTO: ABUSO DE USO DE MEDIOS INFORMÁTICOS. El que, sin autorización o excediendo la que se le hubiere concedido, con el objeto de procurar un beneficio indebido para si o para un tercero, intercepte, interfiera, use o permita que otra use, un sistema o red de computadoras o de telecomunicaciones, un soporte lógico, programa de computación o base de datos, o cualquier otra aplicación informática o de telecomunicaciones, incurre en sanción de a años de prisión y multad de smmlv

Parágrafo: La pena prevista en este artículo se aumentará hasta en la mitad si la conducta se realizare con el propósito de enviar correos o mensajes no solicitados o autorizados en forma masiva o individual.

Elementos Estructurales del Delito:

Sujeto Activo: No calificado o cualificado

Sujeto Pasivo: El propietario del sistema informático o administrador del mismo, particular o del Estado

Objeto Jurídico: La información

Objeto Material: Los medios informáticos

Conducta: Se consuma con la conjugación de los Verbos Rectores, autorizar en negación o exceder, procurar, usar, permitir, alterar,

Comentario: Dentro de los delitos informáticos, parece que es el de mayor ocurrencia, puesto que el hacker al realizar otras conductas informáticas, ingresa abusivamente al sistema informático, seguramente siempre lo encontraremos en concurso con otras conductas. Aquí se incluye el abuso de spam, flagelo informático que ha generado problemas económicos a los usuarios del correo electrónico, vulnerando también derechos fundamentales como el de la intimidad virtual y el hábeas data a los usuarios de la Internet y de las telecomunicaciones. Recordemos que el spaming se puede realizar mediante el uso masivo de correspondencia electrónica, llamadas telefónicas o avisos en el monitor de los teléfonos móviles.

ARTÍCULO SEXTO: DAÑO INFORMÁTICO. El que destruya, altere o inutilice un sistema de tratamiento de información o sus partes o componentes lógicos o impida, altere, obstaculice o modifique su funcionamiento, sufrirá la pena de prisión de a años y multa de ……smmlv.

La pena se aumentará de una tercera parte a la mitad cuando:

1. El propósito o fin perseguido por el agente sea de carácter terrorista
2. Como consecuencia de la conducta del agente sobreviniere daño común
3. El acto dañoso se ejecute sobre entidad estatal
4. Si la conducta se realizare por empleado o contratista del propietario del sistema informático o telemático, o por un servidor público con provecho para si o para un tercero.

Elementos Estructurales del Delito:

Sujeto Activo: Cualquier persona indeterminado

Sujeto Pasivo: Aquel que sufre el daño patrimonial por la acción delictiva

Objeto Jurídico: El objeto jurídico es el valor de la información dañada en soporte lógico o físico, podríamos pensar en el terrorismo informático.

Objeto Material: Su propósito es proteger la información, como bien incorpóreo y los dispositivos que lo soportan.

Conducta: La conducta está definida por tres verbos rectores destruir, alterar inutilizar.

Comentario: Para mi parecer, muy en contrario a muchos autores, considero que la información en el delito de daño informático si puede tangibilizarse, toda vez que la información si puede se objeto del delito de hurto, como también de daño, pese a lo incorpóreo de la substancia. Incluso esta conducta es extensiva para los programadores que insertan en sus programas virus con el objeto de autodestruirse o destruir soporte lógico en donde se monta, so pretexto de ejecutarse sin licencia. ¿Justicia por sus propias manos?

ARTÍCULO SÉPTIMO: ESTAFA ELECTRÓNICA. El que, con ánimo de lucro, y valiéndose de alguna manipulación informática o artificio semejante, consiga la transferencia no consentida de cualquier activo en perjuicio de un tercero, incurrirá en prisión, siempre que no constituya un delito grave, de a años y al pago de una multa de …….smmlv.

Elementos Estructurales del Delito:

Sujeto Activo: No calificado e indeterminado.

Sujeto Pasivo: Persona natural o jurídica

Objeto Jurídico: La información económica

Objeto Material: El traslado de bienes que pasan de ser parte del patrimonio del agente o de un tercero.

Conducta: Está delimitada por el término de manipulación informático o modificación de la información patrimonial.

Comentario: En principio esta conducta se ha considerado como un modus operandi. Tenemos que diferenciar el comportamiento de estafa logrado a través de medios informáticos, con la estafa electrónica que se refiere a la modificación de la información económica o patrimonial

ARTÍCULO OCTAVO: SUPLANTACIÓN DE SITIOS WEB PARA CAPTURAR DATOS PERSONALES (PHISHING). El que diseñe, desarrolle, trafique, venda, ejecute, programe, envíe páginas electrónicas (web site) también llamado Phishing, enlaces (links), ventanas emergentes (pop up) o modifique el sistema de resolución de nombres de dominio, de manera que cuando el usuario crea que está accediendo a su banco u otro site personal o de confianza en Internet, realmente está accediendo a una IP diferente, también llamado pharming; con el fin de inducir, convencer a los consumidores a divulgar información personal o financiera, incurrirá en prisión de a años, siempre que no constituya conducta de mayor gravedad y al pago de una multad de …..smmlv.

La conducta se agravará de una tercera parte a la mitad, si para consumarlo, el phisher ha reclutado Phishing mulas en la cadena del delito.

Elementos Estructurales del Delito:

Sujeto Activo: Calificado e indeterminado

Sujeto Pasivo: Preferiblemente personas que manejan el e-bank

Objeto Jurídico: Datos personales financieros

Objeto Material: Pone en peligro la integridad de la información sensible del usuario con graves consecuencias patrimoniales la mayoría de las veces.

Conducta: El tipo se consuma con el diseño de página (s) falsa (s) de la entidad atacada; el imputado debe registrar ese site falso, en el medio se le denomina camada, con un dominio similar al de la entidad. Logrado el registro del nombre de dominio se debe ubicar el alojamiento en hosting. Luego el delincuente remite correo masivo spam (lanza la carnada) a una base de datos que seguramente ha adquirido en el mercado negro. Seguidamente caerán incautos, pues muchas

personas no diferencian fácilmente entre un site legítimo y uno falso; el afectado ingenuamente suministra su información, incluyendo datos de acceso y contraseñas bancarias. El delincuente captura estos datos y procede a realizar las operaciones bancarias electrónicas y ordena las transferencias a cuentas de tercero.

Estas transferencias las realiza mediante spam a través de terceros que se les llaman Phishing mulas, enviando correos de ofertas de trabajo a personas que ansiosas de trabajar realizan cualquier labor para ganarse algunos pesos y mejor si resulta ser muy fácil. Objetivo: Captar intermediarios para recibir el dinero. Actividad: Recibir en su cuenta el dinero procedente de las víctimas, luego éstos envían el dinero al Phisher (delincuente informático) según instrucciones. En este tipo, no se pena al phisher mula (incauto cibernauta casi siempre) que vincula el agente para el éxito del ilícito, pues ha ofrecido su cuenta bancaria o sus servicios en forma espontánea, ante unas supuestas transacciones, como un seudo-representante de la compañía internacional que en el país le han hecho creer, porque si se prueba que éste, el que ha prestado su nombre y cuenta dicha conducta ya está consagrada en nuestro Código Penal, bajo el epígrafe de **Enriquecimiento ilícito de particulares**, consistente en penalizar el que de manera directa o por interpuesta persona obtenga, para sí o para otro, incremento patrimonial no justificado, derivado en una u otra forma de actividades delictivas.

Comentario: Resulta oportuno resaltar que el nombre de Phishing viene de una combinación de **"Phishing"** (en inglés pescar) con las dos primeras letras cambiadas por **"ph"**: la **"p"** de password (contraseña) y la **"h"** de **hacker** (pirata informático). El Anti-Phishing Working Group, organización creada en EEUU para combatir este fraude, asegura que el número y sofisticación del Phishing' enviado a los consumidores se está incrementando de forma dramática y que "aunque la banca online y el comercio electrónico son muy seguros, como norma general hay que ser muy cuidadoso a la hora de facilitar información personal a través de Internet".

ARTÍCULO NOVENO: FALSEDAD ELECTRÓNICA. El que por cualquier medio electrónico, borre, altere, suprima, modifique o inutilice, sin autorización los datos registrados en una computadora, incurrirá en prisión de a años y al pago de una multa de …….smmlv.

Elementos Estructurales del Delito:

Sujeto Activo: Cualquier persona e indeterminada.

Sujeto Pasivo: El conglomerado en general que confían en la credibilidad del contenido de ese documento público electrónico. La determinación del sujeto pasivo es proporcionada por el carácter del Estado al conferir valor probatorio a ciertos documentos.

Objeto Jurídico: La credibilidad pública en soporte electrónico

Objeto Material: La información que crea credibilidad

Conducta: Los verbos rectores son: borrar, alterar, suprimir, modificar e inutilizar.

Comentario: No sólo se realiza con la modificación del dato o información, se refiere al hecho más relevante, que dicha modificación soporte la credibilidad pública dentro del ambiente comercial o jurídico, como lo es un registro civil electrónico o una factura electrónica. La norma pretende proteger todo tipo de documentos privados o publicas que tengan carácter probatorio.

Se piensa que sólo puede haber falsedad cuando se modifica un contenido (información) en soporte papel, pues hoy por hoy, no sólo se puede pensar que el documento electrónico adulterado vaya a ser transformado en uno en soporte papel siempre. Tenemos que recordar que la mayoría de las transacciones en comercio electrónico todo el soporte se hace en este formato y son muy pocas las oportunidades que se registran en soporte papel. Pensemos en la transacción que realiza un comerciante Colombiano en zapatos Italianos y a través de accesos ilegales al sistema logra modificar las condiciones de la transacción, como por ejemplo que el vendedor asuma el IVA, los valores de la transacción, que modifique el catálogo de productos, etc. No todas las veces se imprimen los documentos electrónicos en soporte papel, además esta adulteración logra engañar, virtud de la falsedad para convencer; al lograrse todo esto, creamos un documento ilegítimo y su contenido no es cierto o parcialmente verdadero.

Tampoco podemos pasar por alto además por ser una verdad de perogrullo, que la falsedad no siempre es material o física, vuelvo a repetir, sólo es recordar la destrucción de las cartillas decadactilares que borró el ex-Director de Informática del DAS o los que se han hecho en la Registraduría Nacional del Estado Civil para "desaparecer" a ciudadanos seguro por una alguna suma significativa de dinero. Sería interesante averiguar cuál es el delito que se le está imputando a éste ex-funcionario, hoy sin existir el tipo punible de falsedad electrónica, para no estar violándosele el principio fundamental de legalidad y el derecho al debido proceso.

Finalmente el documento electrónico y por ende su adulteración está contemplado por vía jurisprudencial porque la Corte Constitucional en su sentencia No. C-356 de Mayo 6 de 2003, Magistrado Ponente Dr. Jaime Araujo Rentaría, quien por acción de inconstitucionalidad del ciudadano Manuel Enrique Cifuentes Muñoz demanda la constitucionalidad del artículo 294 de la Ley 599 de 2002 lo estableció.

ARTÍCULO DÉCIMO: VIOLACIÓN DE DATOS PERSONALES. El que sin autorización obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique o emplee datos personales que se encuentren ficheros, archivos, bases de datos o medios semejantes, públicos o privados, con provecho para sí o para un tercero, incurrirá en prisión de a años y multa de …….smmlv

Las penas previstas en este artículo se aumentarán hasta en la mitad si la conducta se realizare por empleado o contratista del propietario del sistema u operador informático o telemático, o por un servidor público, con provecho para sí o para un tercero, igual acontece si la información vulnerada corresponde a un menor de edad.

Elementos Estructurales del Delito:

Sujeto Activo: Cualquier persona e indeterminado

Sujeto Pasivo: El titular de la información sensible

Objeto Jurídico: Los datos sensibles, estos son: cuando afecten a datos de carácter personal que revelen la ideología, religión, Creencias, salud, origen étnico o racial, vida social o conciencia política,

Objeto Material: Guarda el derecho protegido a la audeterminación informativa, un estrecho nexo con valores, como la dignidad humana y el libre desarrollo de la personalidad, así como otras libertades públicas como la ideológica o la de expresión.

Conducta: La conducta está definida por los siguientes verbos rectores: autorizar en negación, obtener, compilar, sustraer, ofrecer vender, intercambiar, enviar, comprar, divulgar, modificar o emplear datos sensibles.

Comentario: Un ejemplo de tantos para este tipo, es el caso del sujeto que envía a múltiples direcciones electrónicas, sin el consentimiento de su ex-novia, unas fotos en donde aparece desnuda, con textos ofensivos, vulnerando la dignidad de aquella. Violando flagrantemente datos sensibles. La protección jurídica de los datos personales representa, en el marco de la evolución del derecho penal comparado, uno de los aspectos más recientes y significativos del esfuerzo por tutelar y garantizar la esfera de los derechos y libertades fundamentales. En este precepto se convierte en delito actividades que antes sólo tenían sanción administrativa o constitucional (Acción de Tutela) Se debe considerar la Ley 221 de 29 de Mayo de 2007, la nueva estatutaria de hábeas data, como también, particularmente deben citarse, entre otras, la resolución 45/95 de 1990 de la ONU, la directiva 95/46/CE del Parlamento Europeo y las "Directrices para la Armonización de la Protección de Datos en la Comunidad Iberoamericana" aprobadas por la Red Iberoamericana de Protección de datos el pasado 4 de mayo en la ciudad de Cartagena.

***Alexander Díaz García.** Abogado de la Universidad Católica de Colombia; Especialista en: Ciencias Penales y Criminológicas de la Universidad Externado de Colombia; Ciencias Constitucionales y Administrativas de la Universidad Católica de Colombia y Nuevas Tecnologías y Protección de Datos de la Escuela de Gobierno y Políticas Públicas de Madrid adscrita al Instituto Nacional de Administración Pública de España. Autor del libro en soporte papel **DERECHO**

INFORMÁTICO ELEMENTOS DE LA INFORMÁTICA JURÍDICA, Editorial Leyer y de los siguientes trabajos de investigación: **EFECTOS JURÍDICOS DE LOS DOCUMENTOS ELECTRÓNICOS EN COLOMBIA**. Estudio de la Ley 527 de 1999. **DESVINCULACIÓN DEL SERVIDOR PÚBLICO POR USO IMPROPIO DEL EMAIL OFICIAL. LA ÉTICA EN EL DERECHO INFORMÁTICO. LA PROTECCIÓN DEL DATO EN EL CONTEXTO JUDICIAL COLOMBIANO. ACCESO RETOS Y REALIDADES DE LA ADMINISTRACIÓN DE JUSTICIA EN COLOMBIA CON EL USO DE LOS MEDIOS ELECTRÓNICOS. ACCESO A LA ADMINISTRACIÓN DE JUSTICIA A TRAVÉS DE LAS NUEVAS TECNOLOGÍAS. DESNATURALIZACIÓN DEL DOCUMENTO ELECTRÓNICO JUDICIAL EN LA APELACIÓN DE LA SENTENCIA EN EL SISTEMA PENAL ACUSATORIO (EL JUICIO ORAL) COLOMBIANO. MANEJO DE DATOS SENSIBLES EN FICHERO CLÍNICOS.** Autor de la primer proceso judicial electrónico tramitado en la Internet, protegiendo los Derechos Fundamentales de Hábeas Data y la Intimidad Virtual, a través de una acción de tutela virtual, violado por abuso de spam. Facilitador de la Escuela Judicial Rodrigo Lara Bonilla, en los módulos de **INTERPRETACIÓN JUDICIAL, JUECES DE PAZ, CONCILIACIÓN EN EQUIDAD PARA JUECES FORMALES Y TRANSVERSALIZACIÓN DE GÉNERO**. Ex-Catedrático de la Escuela de Administración Pública en el Módulo de Contratación Electrónica Estatal y de la Universidad Cooperativa de Ibagué con la materia Informática Jurídica y Asesor Académico de la Universidad de Ibagué Coruniversitaria. Actualmente Asesor Académico de la Dirección de Postgrados de la Universidad Santiago de Cali con los proyectos **JUZGADO VIRTUAL; ESPECIALIZACIÓN, MAESTRÍA Y DOCTORADO EN NUEVAS TECNOLOGÍAS Y PROTECCIÓN DE DATOS.** Y el proyecto de ley **DELITOS ELECTRÓNICOS.** Conferencista del Programa Internacional de Asistencia y entrenamiento en la Investigación Criminal ICITAP del Departamento de Justicia de los Estados Unidos, con el tema delitos electrónicos. Es el titular en la actualidad del Juzgado Segundo Promiscuo Municipal de Rovira Tolima Colombia.