



Congreso de Colombia  
Proyecto de Ley  
H.S. Luís Humberto Gómez Gallo  
H.R. Carlos Arturo Piedrahita C

Bogota D.C. 06 de Septiembre de 2007

Doctor  
**EMILIO OTERO DAJUD**  
Secretario General  
Senado de la República  
Ciudad

En nuestra condición de Congresistas y en uso del derecho que consagra el artículo 154 de la Constitución Política y 140 de la ley 5 de 1992, me permito poner a consideración del Honorable Congreso, el presente Proyecto de ley “Por medio del cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado “la protección de la información” - y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones”

**PROYECTO DE LEY No.**  
**“Por medio del cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado “la protección de la información” - y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones”**

## **EXPOSICIÓN DE MOTIVOS**

### **1. Introducción:**

Sometemos ante el Congreso de la República el presente proyecto de ley, cuya creación corresponde al Juez Segundo Promiscuo Municipal de Rovira **Alexander Díaz García**<sup>1</sup> quien contó con el aporte intelectual del

---

<sup>1</sup> **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 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. Entre otras.

tratadista Dr. Fernando Velásquez Velásquez y académico de los Drs. Jarvey Rincón Ríos Director de Postgrados de la Facultad de Derecho de la **Universidad Santiago de Cali** y Gabriel Roldán Restrepo Juez Veinte Penal del Circuito de Medellín Coordinador del Comité de Estudios Políticos y Legislativos del Colegio de Jueces y Fiscales de Antioquia.

## **2. Precisiones iniciales:**

En la actualidad han surgido muchos problemas relacionados con el uso de las computadoras, amenazas que afectan negativamente tanto a los individuos como a las empresas. La proliferación de estos instrumentos que se han constituido en la principal herramienta de funcionamiento en casi todos los niveles de convivencia, así como la creación de la red global, ha provocado que cada vez más personas se las ingenien para lucrarse, hacer daño o causar perjuicios a través del uso de estos instrumentos.

Por ello, se pone en consideración del Honorable Congreso de la República de Colombia este proyecto de ley sobre los delitos informáticos, que pretende regular y sancionar una serie de conductas, que sorprendentemente, no son tenidas en cuenta por nuestra Legislación Penal.

Se trata de un decálogo de tipos penales, muchos de ellos con nuevos verbos rectores que sólo se conjugan en las circunstancias informáticas origen del presente estudio.

Antes de entrar a considerar más en detalle los delitos informáticos, se torna obligado exponer el tema sobre la legitimidad del documento electrónico, el dato y, por consiguiente, la información en Colombia, que es a la postre el bien jurídico tutelado susceptible de ser vulnerado, cualquiera que sea el propósito ilegal pretendido por el sujeto activo de la conducta. Lo anterior, permite establecer claras fronteras entre un verdadero delito informático y un hecho punible que ha usado medios electrónicos para su consumación.

La mayoría de los expositores se refieren al tema de los 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 funcionario judicial haya declarado probada la existencia concreta de una conducta típica, antijurídica y culpable del delito informático, lo que permite colegir sin profundas elucubraciones que la conducta informática socialmente reprochable es atípica en Colombia.

Así las cosas, es necesario precisar y explicar en qué consiste el bien jurídico tutelado 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 tratándose de intereses colectivos, afecte otros bienes jurídicos como la propiedad generalmente. Así mismo, se debe mostrar cómo el decálogo de conductas aquí propuesto está constituido por tipos autónomos y no subordinados por circunstancias genéricas o específicas de agravación punitiva de otros tipos, como ha sido la costumbre legislativa en el mundo. Igualmente, se debe tener en cuenta que algunas de las expresiones utilizadas aparecen en idioma inglés porque muchas de esas conductas están en esa lengua o porque su texto original en ese idioma ha sido modificado caprichosamente por los llamados “hackers”, lo que obliga a utilizar locuciones castellanas que de forma más o menos aproximada permita tipificar las susodichas conductas.

### **3. Los bienes jurídicamente tutelados:**

A lo largo de la evolución del Derecho penal se han distinguido diversos conceptos de bien-jurídico. En efecto, la noción acuñada por Birnbaum a mediados del S. XIX, se refiere a los bienes que son efectivamente protegidos por el Derecho; esta concepción, sin embargo, es demasiado abstracta y por ello no cumple con la función delimitadora del *Ius puniendi* que persigue un derecho penal de inspiración democrática.

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.

A su turno, el concepto político criminal del bien jurídico trata de distinguir el bien jurídico de los valores morales, o sea busca 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 de la noción de bien jurídico está, por tanto, en la pretensión de elaborar un concepto del delito previo al que forma el legislador, que condicione sus decisiones, de la mano de una concepción liberal del Estado, para la cual este es un instrumento que el individuo crea para preservar los bienes que la colectividad en su conjunto quiera 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 ello se infiere 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 ámbito del Derecho penal, ya que en esta rama del orden jurídico más que en ninguna otra 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, pues, 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. Sin embargo, no debe olvidarse que existen bienes jurídicos que no son amparados por el Derecho penal por ser intereses sólo morales, por lo cual no todos los bienes jurídicos son bienes jurídico-penales.

#### **4. Los 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, pues también 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 cuáles 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 se deben proteger los bienes jurídicos de mayor importancia para la convivencia social y cuya protección por otras ramas del derecho hagan insuficiente la prevención que cualquier trasgresión los afecte.

### **5. Principio de la intervención mínima de la actuación punitiva del estado.**

Es el axioma que restringe el campo de la libertad del ciudadano y que, mediante la pena, priva de derechos fundamentales o condiciona su ejercicio; por ello, 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 Derecho Penal tiene carácter subsidiario frente a los demás instrumentos del ordenamiento jurídico y, así mismo, posee 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.

## **6. Naturaleza jurídica del bien jurídico tutelado de la información.**

Para algunos, el delito informático representa sólo la comisión de otros delitos mediante el uso de las computadoras, pues se considera que en realidad no hay un bien jurídico protegido en este caso, pues se parte del presupuesto de que dicha conducta no existe como tal. Otros, por el contrario, opinan que estos delitos tienen un contenido propio, afectando así un nuevo bien jurídico “La Información”, gracias a lo cual diferencian los delitos computacionales y los delitos informáticos propiamente dichos.

Finalmente, una tercera corriente considera que los delitos informáticos deben ser observados desde un punto de vista triple: como fin en sí mismos, pues el computador puede ser objeto de la ofensa, al manipular o dañar la información que este pudiera contener; como medio, esto es, como herramienta del delito, cuando el sujeto activo usa el ordenador para facilitar la comisión de un delito tradicional; y, finalmente, como objeto de prueba: los computadores guardan pruebas incidentales de la comisión de ciertos actos delictivos cometidos 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; por ello, el concepto de bien jurídico no desaparece, solo cambia en cuanto al ámbito de protección que lo sujeta. El desarrollo de esta institución jurídica, pues, pasa por momentos totalmente distintos dado que ellos son producto de las necesidades propias del desarrollo de la sociedad; ellos, en consecuencia, no se originan al crear una norma sino que su existir es previo a la misma.

El bien jurídico se justifica, entonces, 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. Por ello, bajo el mecanismo de garantía resulta posible denunciar todos los elementos que amenacen o avasallen a la persona en su relación con el Estado. La función 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.

## **7. El delito informático.**

En tales condiciones, el artículo 269A del Proyecto pretende proteger la información privilegiada industrial, comercial, política o militar relacionada con la seguridad del Estado. Se castiga, pues, la falta de sigilo o confidencialidad de los profesionales, responsables o encargados de los ficheros de los datos automatizados.

En el artículo 269B, los verbos rectores empleados se deducen de las locuciones ingresar, usar ilegalmente información sin estar autorizado. Esta actividad se conoce como White hacking, porque los autores de esas conductas quieren demostrarle al sistema de seguridad en donde acceden 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. Este comportamiento es, sin duda, uno de los delitos informáticos, de mayor ocurrencia, puesto que el hacker al realizar otros comportamientos informáticos, ingresa abusivamente al sistema informático, con lo cual su actuar va asociado a otras conductas punibles.

En el artículo 269C el verbo rector de la conducta es el impedir el acceso a los sistemas informáticos; este comportamiento se conoce también como extorsión informática, pues el delincuente bloquea, asedia, o acorrala el sistema hasta cuando no se le cancele una suma de dinero. El caso más patético es el caso de Hackers turcos y eslovenos que tomaron como rehén la página de un club de fútbol colombiano, el Envigado FC, un equipo de la segunda división. Sin embargo, 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 de éstas pero siguen conociendo de las claves de acceso, modifican éstas e impiden que el titular de la cuenta las abra, realizando diversos comportamientos, incluso difamar del titular de la dirección electrónica, como sucede con los novios que terminan la relación pero abusan de los secretos que, en pareja, guardaron, difundiendo en la red.

El 269D se refiere al uso de virus o software malicioso, una conducta muy generalizada en la red.

A su turno, el artículo 269E prevé como punible el abuso de medios informáticos, mediante la introducción de verbos rectores como "intercepte", "interfiera", "use" o "permita que otro use". Ello, es consecuencia de que en materia de delitos informáticos es frecuente que el hacker al realizar otras conductas informáticas, ingrese abusivamente al sistema informático, por lo cual suele realizar un concurso de conductas punibles. 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. Recuérdese que el spamming se puede realizar mediante el uso masivo de correspondencia electrónica, llamadas telefónicas o avisos en el monitor de los teléfonos móviles. También, es muy común el comportamiento denominado denegación de servicio DDos (Distributed Denial Of Service Attack) que permite bloquear un servidor por múltiples ataques.

En lo que respecta al artículo 269F, debe decirse que se refiere a la protección de la destrucción de la información, bien que aún no ha sido clasificado por la doctrina, como mueble o inmueble, siendo necesario tipificarlo por tan sue generis circunstancia. Incluso, esta conducta es extensiva para los programadores que insertan en sus programas virus con el objeto de autodestruirse o destruir el soporte lógico en donde se monta, so pretexto de ejecutarse sin licencia. Este comportamiento se agrava cuando el fin perseguido es de carácter terrorista, cuando la conducta del agente sobreviniere daño común, si recae sobre bienes estatales, o cuando interviene un servidor público con provecho para si o para un tercero.

El artículo 269G se refiere a la estafa electrónica, la que no puede ser subsumida en la estafa clásica, pues los verbos rectores son diferentes; en efecto, debe recordarse que en aquella (la clásica), la inducción se realiza en humano, en cambio en el delito informático no se puede inducir o mantener a otro en error por medio de artificios o engaños, pues las máquinas no son susceptibles de inducción al error, pues se debe manipular la información para lograr la transferencia de activos en forma ilegal. En principio, esta conducta se ha considerado como un modus operandi. Debe, pues, distinguirse el comportamiento de estafa logrado a través de medios informáticos, de la estafa electrónica que se refiere a la modificación de la información económica o patrimonial.

En tratándose del Phishing, regulado en el artículo 269H, debe decirse que la conducta pone en peligro la integridad de la información sensible del usuario con graves consecuencias patrimoniales la mayoría de las veces. El tipo se consume con el diseño de página (s) falsa (s) de la entidad atacada; el imputado debe registrar ese site falso, que en el medio se le denomina como "carnada", 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 laborar 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 esta descripción típica, pues, 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 pseudo-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, lo hace con la finalidad de obtener lucro incurre en una conducta ya 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 (artículo 327).

Finalmente, 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 EE. UU. 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".

Para describir la conducta punible de falsedad en el artículo 269I, se emplean los verbos rectores borrar, alterar, suprimir, modificar e inutilizar. La norma pretende proteger todo tipo de documentos privados o públicos que tengan carácter probatorio. Hoy, la mayoría de las transacciones en comercio electrónico se hace en este formato y son muy pocas las oportunidades que se registran en soporte papel. Piénsese, por ejemplo, en la transacción que realiza un comerciante Colombiano con zapatos Italianos y, a través de accesos ilegales al sistema, logra modificar las condiciones de la transacción; por ejemplo, que el vendedor asuma el IVA, los valores de la transacción, que modifique el catálogo de productos, etc.

No todas las veces, pues, se imprimen los documentos electrónicos en soporte papel, además esta adulteración logra engañar, virtud de la falsedad para convencer; al lograrse todo esto, se crea un documento ilegítimo y su contenido no es cierto o parcialmente verdadero.

Tampoco, se puede pasar por alto, por ser una verdad de perogrullo, que la falsedad no siempre es material o física, basta recordar la

destrucción de las cartillas decadactilares que, se dice, borró el ex-Director de Informática del DAS o las vulneraciones que se han hecho en la Registraduría Nacional del Estado Civil para “desaparecer o resucitar” a ciudadanos. Finalmente, téngase en cuenta que el documento electrónico y, por ende, su adulteración, ha sido debatida por vía jurisprudencial porque la Corte Constitucional en su sentencia No. C-356 de Mayo 6 de 2003 lo reconoció pero, ciertamente, esa Corporación no es un ente legislativo.

Para terminar, con la punición de la violación de datos personales que aparece en último lugar en el nuevo artículo 269J, se quiere salvaguardar el derecho protegido a la autodeterminación informativa, un estrecho nexo con valores, como la dignidad humana y el libre desarrollo de la personalidad, así como con otras libertades públicas como la ideológica o la de expresión. La conducta se define con el empleo de los siguientes verbos rectores: autorizar en negación, obtener, compilar, sustraer, ofrecer vender, intercambiar, enviar, comprar, divulgar, modificar o emplear datos sensibles.

En fin, la exposición anterior demuestra la trascendencia que estas conductas ilícitas tiene en el tráfico social por lo que, a la par de convenios internacionales como el de la cibercriminalidad suscrito en Budapest en 2001, el legislador colombiano las debe incluir dentro de su catálogo de prohibiciones. A eso, pues, está enderezado el presente Proyecto de ley que esperamos cuente con la acogida de los H. congresistas.

## **EL CONGRESO DE LA REPUBLICA DE COLOMBIA**

### **DECRETA**

**ARTÍCULO PRIMERO: adicionase el Código Penal con el Título VII BIS denominado “De la Protección de la información”, del siguiente tenor:**

**ARTÍCULO 269A: ESPIONAJE INFORMÁTICO.** El que se apodere, interfiera, transmita, copie, modifique, destruya, utilice, impida o recicle datos informáticos de valor para el tráfico económico de la industria, el comercio, o datos de carácter político y/o militar relacionados con la seguridad del Estado, incurrirá en prisión de seis (6) a diez (10) años y multa de 500 a 2.500 salarios legales mínimos mensuales vigentes.

**ARTÍCULO 269B: ACCESO ILEGÍTIMO A SISTEMAS INFORMÁTICOS.** El que haga uso de los medios informáticos 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 procese, intercambie, reproduzca, conserve o

transmita, incurrirá en pena de prisión de cuatro (4) a ocho (8) años de prisión y en multa de 200 a 1.500 salarios mínimos legales mensuales vigentes.

**Parágrafo:** Si los hechos descritos en el artículo anterior se cometen utilizando redes o sistemas estatales, gubernamentales, de organizaciones comerciales o educativas, nacionales, internacionales, o de país extranjero, la sanción será de seis (6) años a diez (10) años de prisión y multa de 350 a 2.000 salarios mínimos legales mensuales vigentes.

**ARTÍCULO 269C: 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, incurrirá en sanción de cuatro (4) a ocho (8) años de prisión y en multa de 50 a 500 salarios mínimos legales mensuales vigentes.

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

**ARTÍCULO 269D: 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, incurrirá en sanción de privación de libertad de cuatro (4) a ocho (8) años y en multa de 50 a 500 salarios mínimos legales mensuales vigentes.

**Parágrafo:** La pena prevista en este artículo se aumentará hasta en la mitad, si la conducta se realizare en provecho propio o de un tercero por parte de empleado o contratista del propietario del sistema informático o telemático, o por un servidor público.

**ARTÍCULO 269E: ABUSO DE USO DE MEDIOS INFORMÁTICOS.** El que, sin autorización o excediendo la que se le hubiere concedido, con el fin de procurar un beneficio indebido para sí o para un tercero, intercepte, interfiera, use o permita que otra use un sistema o red de computadoras o de telecomunicaciones, un soporte lógico, un programa de computación o una base de datos, o cualquier otra aplicación informática o de telecomunicaciones, incurrirá en sanción de cuatro (4) a ocho (8) años de prisión y en multa de 50 a 500 salarios mínimos legales mensuales vigentes.

**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.

**ARTÍCULO 269F: 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, incurrirá en pena de prisión de cuatro (4) a ocho (8) años y en multa de 200 a 1000 salarios mínimos legales mensuales vigentes.

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 peligro o daño común.
3. El acto dañoso se ejecute sobre bien de propiedad de una entidad estatal.
4. Si la conducta se realizare en provecho propio o de un tercero, por parte de empleado o contratista del propietario del sistema informático o telemático, o por un servidor público.

**ARTÍCULO 269G: ESTAFA INFORMÁTICA.** 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, siempre que la conducta no constituya delito sancionado con pena más grave, incurrirá en prisión de cuatro (4) a diez (10) años y en multa de 200 a 1000 salarios mínimos legales mensuales vigentes.

**Parágrafo:** La pena prevista en este artículo se aumentará hasta en la mitad, si el monto del activo transferido es superior a 100 salarios mínimos legales mensuales vigentes.

**ARTÍCULO 269H: SUPLANTACIÓN DE SITIOS WEB PARA CAPTURAR DATOS PERSONALES (PHISHING).** El que diseñe, desarrolle, trafique, venda, ejecute, programe o envíe páginas electrónicas (web site), enlaces (links) o ventanas emergentes (pop up), incurrirá en prisión de cuatro (4) a ocho (8) años y en multa de 200 a 1000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con pena más grave.

En las mismas sanciones incurrirá el que, con el fin de inducir, convencer a los consumidores a divulgar información personal o financiera, modifique el sistema de resolución de nombres de dominio, lo que hace al usuario ingresar a una IP diferente en la creencia de que está accediendo a su banco u otro sitio personal o de confianza, siempre que la conducta no constituya delito sancionado con pena más grave.

La pena señalada en los dos incisos anteriores se agravará de una tercera parte a la mitad, si para consumarlo el phisher ha reclutado Phishing mulas en la cadena del delito.

**ARTÍCULO 269I: FALSEDAD INFORMÁTICA.** El que sin autorización para ello y valiéndose de cualquier medio electrónico, borre, altere, suprima, modifique o inutilice los datos registrados en una computadora, incurrirá en prisión de cuatro (4) a ocho (8) años y en multa de 50 a 500 salarios mínimos legales mensuales vigentes.

**ARTÍCULO 269J: VIOLACIÓN DE DATOS PERSONALES.** El que, con provecho para sí o para un tercero y sin autorización, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique o emplee datos personales que se encuentren en ficheros, archivos, bases de datos o medios semejantes, públicos o privados, incurrirá en prisión de cuatro (4) a ocho (8) años y en multa de 50 a 500 salarios mínimos legales mensuales vigentes.

Las penas previstas en este artículo se aumentarán hasta en la mitad, si las conductas se realizaren en provecho propio o de un tercero por parte de empleado o contratista del propietario del sistema u operador informático o telemático, o por un servidor público.

Las mismas sanciones se impondrán al que realice dichas conductas cuando la información vulnerada corresponda a un menor de edad.

**ARTÍCULO SEGUNDO:** La presente ley deroga todas las disposiciones que le sean contrarias y rige desde su promulgación.

De los Honorables Congresistas,

**LUIS HUMBERTO GÓMEZ GALLO**  
Senador de la República

**CARLOS ARTURO PIEDRAHITA**  
Representante a la Cámara