El delito informático y su clasificación
The computer crime and classification

David Bolívar Narvaez Montenegro
david_narvaez@outlook.es
UNIANDES

RESUMEN

El delito informático ha sido objeto de análisis y por parte de juristas y expertos en seguridad informática; en base a estos estudios muchas legislaciones del mundo han tipificado varias conductas como cibercrimenes. Sin embargo, no existe una clasificación única del delito informático, lo que ha generado que cada legislación le otorgue un tratamiento diferente, no solo en cuanto a la sanción, si no a la forma de consideración de cada uno de ellos: tanto en las circunstancias de cómo es cometido, como en la forma de investigarlo y procesarlo. Lo dicho lleva a la necesidad de crear una clasificación que intente extraer lo mejor del estudio efectuado por los expertos y lo que el legislador ha tipificado en la normativa penal internacional, abarcando la mayor cantidad de hechos delictuales que pueden ser cometidos con empleo de herramientas informática. De esta forma se ofrecerá al legislador, a la Academia y al lector en general, una nueva consideración de las conductas cibercriminales, que bien pueden ayudar a cualquier legislación a construir un marco adecuado de delitos informáticos, sin dejar en el limbo jurídico hechos que puedan quedar impunes o resultar complejos de sancionar por falta de tipificación expresa.

PALABRAS CLAVE: Legislación de delitos informáticos, derecho, clasificación.

ABSTRACT

Computer crime has been analyzed and by lawyers and security experts; based on these studies many laws in the world have criminalized various behaviors such as cybercrimes. However, there is no single classification of computer crime, which has generated every law gives a different treatment, not only in terms of the sanction, if not the form of consideration of each: both the circumstances how it is made, and how to investigate and prosecute. What this leads to the need to create a classification that attempt to extract the best of study by experts and what the legislator has criminalized in international criminal law, covering the largest number of criminal acts that can be committed with the use of computer tools. Thus the legislator will be offered at the Academy and the general reader, a new consideration of behaviors cybercriminals, which may well help any legislation to build a framework of computer crimes, while in legal limbo events likely go unpunished or be complex sanction for failure to express typing.

KEYWORDS: Computer crime legislation, law, classification

INTRODUCCIÓN

El desarrollo tecnológico ha obligado a las legislaciones del mundo a identificar nuevas formas delictuales no contemplados en los Códigos penales. Ciertamente, teniendo la informática un contexto sumamente basto, la delincuencia ha ideado formas para ejecutar conductas que lesionan significativamente derechos de terceros, y para las cuales las legislaciones interestatales no están del todo preparadas. Por esta razón, la

Recibido: Enero 2015. **Aceptado:** Abril 2015

comunidad internacional, expertos en seguridad informática y juristas destacados han intentado abordar el tema con detenimiento, intentando identificar las conductas criminales ejecutadas con empleo de herramientas informáticas, a fin de que sean plasmadas en cuerpos jurídicos de los Estados.

Efectivamente, aunque existen leyes, Códigos, Convenciones, doctrina, que identifican las conductas lesivas ejecutadas con herramientas informáticas, no existe una clasificación que abarque casi la totalidad de delitos informáticos. Lo cual se evidencia en el tratamiento que la mayoría de Estados le dan al tema, contemplando en unos casos cinco o diez artículos donde se pretende abarcar a todas las conductas referidas, quedando en el limbo muchas que deben que ser acopladas por los operadores de justicia a figuras penales tradicionales. Es por eso, que en el presente artículo científico, se ofrece una clasificación amplia y detallada de los delitos informáticos, surgida posterior a la exhaustiva revista efectuada en el Derecho Comparado y del análisis científico realizado, concluyendo en una clasificación nueva y más amplia de las conductas cibercriminales, que puede servir de base para que cualquier legislación del mundo, la Academia y los doctrinarios adopten, tanto en las legislaciones, en el estudio del Derecho y la Seguridad Informática, y en las obras escritas sobre el tema.

DESARROLLO

El delito informático: definición

Como muchos términos jurídicos, el delito ha sido definido por varios juristas del mundo, quienes han intentado proponer una definición que sirviese para todos los tiempos y en todos los países. Sin embargo, anotamos la efectuada por el destacado penalista español Eugenio Cuello Calón, quien propone una definición que ha sido aceptada mayoritariamente en el seno de la Academia por casi un siglo, y que se refiere al delito como la "acción humana antijurídica, típica, culpable y punible" (Cuello Calón, 1960), y cuyos elementos son:

- El delito es un acto humano.
- Este evento debe lastimar o colocar en riesgo un interés legalmente protegido.
- Ha de ser un acto tipificado.
- El acto ha de ser culpable
- El acto debe estar sancionada por una pena.

De acuerdo a lo expuesto, al delito informático se lo puede definir de la siguiente forma: Acto humano culpable ejecutado con empleo de herramientas informáticas, que lesiona bienes jurídicamente protegidos, y que se encuentra tipificado y sancionado en la norma jurídica.

Existe un sinnúmero de actos humanos antijurídicos en los que se emplean sistemas informáticos con diversos propósitos, pero no todos podrían ser considerados como delitos, ya que algunos de ellos, bien podrían ser tipificados como meras contravenciones, tomando en cuenta la gravedad de la infracción y/o el daño causado. Por esta razón, el empleo correcto del término a criterio del autor, es el de *"infracciones informáticas"*, en vez de *"delitos informáticos"*; ya que existen acciones que pueden causar daños mayores, como la transacción fraudulenta de depósitos

Recibido: Enero 2015. **Aceptado:** Abril 2015

bancarios, o actos informáticos con menos significación que el anterior como el daño causado al hardware por la introducción de un dispositivo extraíble contagiado con un malware.

El delito informático en el contexto internacional.

Las normas establecidas por las legislaciones del mundo tienden a proteger bienes jurídicos como la vida, integridad, bienes de las personas, etc. Dentro de este contexto, la protección de datos procesados es fundamental, más si se considera que los mismos reposan en ordenadores digitales que resultan fácilmente vulnerables al ataque delincuencial -especialmente la información relativa al patrimonio e intimidad de las personas-. Por esta razón, es indispensable que la protección de la información digital sea analizada desde la óptica del Derecho Comparado, para conocer el tratamiento que los Estados le han dado al tema, a fin de que las conductas criminales que tienden ilegalmente a apropiarse o hacer mal uso de la información digital, sean tipificadas como delitos independientes.

En el Derecho Internacional, existen antecedentes vinculados directamente con la lucha contra delitos ejecutados con la informática, así encontramos la Convención para la Protección y Producción de Fonogramas de 1971, que surge debido al incremento de la reproducción no autorizada de fonogramas y por el perjuicio que ocasiona a los intereses de los autores, de los artistas intérpretes o ejecutantes y de los productores de fonogramas.

Posteriormente, en 1974 se celebra el Convenio sobre la Distribución de Señales Portadoras de Programas Transmitidas por Satélite, que surge por la inexistencia de normas con alcance mundial que impidan la distribución de señales portadoras de programas y transmitidas mediante satélite, por distribuidores a quienes esas señales no estaban destinadas; así como por la probabilidad de que este vacío complique el uso de las comunicaciones a través de satélite.

Por otro lado, hallamos la Convención sobre la Propiedad Intelectual, firmado en Estocolmo el 14 de julio de 1967 y enmendado el 28 de septiembre de 1979, para fomentar la protección de la propiedad intelectual en todo el mundo mediante la cooperación de los Estados.

Existieron también, desde la década de los setenta, estudios referidos al uso doloso de herramientas informáticas, entre los que destacamos por su importancia a dos:

1.- El desarrollado por la Organización de Cooperación y Desarrollo Económico en 1983, estudio relativo a la armonización interestatal de las normas jurídicas penales, para combatir el uso prohibido de los programas de computación; y,

2.- El desarrollado en 1992 por La Asociación Internacional de Derecho Penal durante una reunión formal que se efectuó en la ciudad alemana de Wurzburgo, en 1992.

En 1990 la Organización de las Naciones Unidas, en el Octavo Congreso sobre Prevención del Delito y Justicia Penal, celebrado en Cuba, ciudad de La Habana, abordó la problemática naciente del delito informático, concluyendo que la criminalidad informática era producto del mayor empleo del proceso de datos en las economías y burocracias de los distintos Estados, y que por esta razón aumentaban

Recibido: Enero 2015. **Aceptado:** Abril 2015

considerablemente la comisión de ciberdelitos. Así mismo, la Organización de Naciones Unidas ha procedido a reconocer oficialmente tres tipos de delitos informáticos:

1. Fraudes cometidos mediante manipulación de computadoras.
2. Manipulación de los datos de entrada.
3. Daños o modificaciones de programas o datos computarizados.

Sin embargo, el hecho más significativo y que sirvió de inspiración para la mayoría de legislaciones del mundo, por cuanto aborda directamente al crimen informático, es el realizado el 23 de noviembre de 2001 en Hungría, cuando el Consejo de Europa en Estrasburgo, elaboró un documento vinculante frente a los delitos informáticos, a través de la concertación de las leyes internas, y comprometiendo la cooperación de los Estados para la investigación de los mismos. Este acuerdo interestatal se denominó “Convención de Cibercriminalidad”, que fue aprobada y ratificada por 30 Estados; mientras que 16 solo firmaron -quedando pendiente la ratificación correspondiente- . En la actualidad, varios países de Sudamérica consideran la posibilidad real de adherirse al mismo; entre los que consta la República del Ecuador. Sin duda alguna el “Convención de Cibercriminalidad”, es el único acuerdo interestatal que aborda la mayor cantidad de áreas sobre ciberdelincuencia, entre la que se cuenta:

- Acceso ilícito,
- Interceptación ilícita,
- Atentados contra la integridad de los datos,
- Atentados contra la integridad del sistema,
- Abuso de equipos e instrumentos técnicos,
- Falsedad informática,
- Estafa informática,
- Infracciones relativas a la pornografía infantil,
- Infracciones vinculadas a los atentados a la propiedad intelectual y a los derechos afines.

En el Contexto iberoamericano, desde inicios de los noventa se vio la necesidad de abrir el debate del delito informático que había empezado a tipificarse en legislaciones de mayor avanzada -como la estadounidense y la europea-. De los países latinoamericanos, Chile y España fueron de los primeros Estados que tipificaron ciertas conductas criminales ejecutas con empleo de herramientas informáticas, hasta llegar a la actualidad, con Estados cuya normativa -en muchos casos- está a la par de varias legislaciones europeas; tal es el caso de la legislación venezolana, mexicana, entre otras.

A continuación detallamos la realidad en cuanto a la tipificación de delitos informáticos en los países hispanos cuya legislación ofrece más avances sobre el tema:

Argentina: Este país se sumó a diversas legislaciones del mundo que tipifican conductas cibercriminales, cuando el 4 de junio del 2008 sancionó la Ley 26.388, República de Argentina (2008) que reforma los artículos 77, 128, 153, 155, 157, 173, 183,197 y el epígrafe del Capítulo III, del Título V, del Libro II, además que se derogan

Recibido: Enero 2015. **Aceptado:** Abril 2015

el artículo 78 bis y el inciso 1º del artículo 117 bis del Código Penal, incluyendo las siguientes conductas cibercriminales: interrupción de comunicaciones, daño informático agravado, distribución y tenencia con fines de distribución de pornografía infantil, violación de correo electrónico, acceso ilegítimo a sistemas informáticos, daño informático y distribución de virus.
Esta normativa sienta la base legal para que los jueces puedan sancionar conductas delictuales que las encuadraban -en un tipo de adaptación jurídica- en un delito ya tipificado.

Brasil: En este Estado, el debate sobre la situación jurídica del delito informático no ha estado a la par de su auge tecnológico y económico. Mientras otras legislaciones con menor desarrollo estipularon una normativa que tipifica y sanciona esta clase de delitos, Brasil tenía que a adaptar las conductas cibercriminales a figuras penales tradicionales ya tipificadas.

Tuvo que acontecer un hecho que conmocionó considerablemente la sociedad brasileña para que el gobierno tome en serio el debate y la necesidad de crear una ley que tipifique con más amplitud este tipo de delitos. Éste fue el acaecido a la conocida actriz brasileña Carolina Dieckmann, cuyas fotos fueron publicadas en internet por un sitio especializado en celebridades Egotastic, sin su autorización. Lo acontecido a Dieckmann hizo que la autoridad ejecutiva y legislativa tome medidas jurídicas urgentes que protejan a la población de este tipo de ataques, llevando a la presidenta de Brasil, Ec. Dilma Rousseff, a firmar dos leyes que reforman el Código Penal, tipificando y sancionando varios delitos electrónicos. El proyecto fue aprobado por la Cámara de Representantes el 7 de noviembre del 2012; y en el que se tipifican los siguientes, (República de Brasil, 2012).

- El acceso no autorizado a ordenadores, conectados o no a internet, mediante la violación de sus mecanismos de seguridad
- El robo de contraseñas y contenidos de correos electrónicos o
- Hacer caer intencionalmente un Website
- La invasión de dispositivos electrónicos ajenos con el "fin de obtener, cambiar o destruir datos o informaciones".
- La producción y distribución de dispositivos que permitan invadir teléfonos inteligentes o tabletas electrónicas.
- La obtención ilegal de datos bancarios por vías electrónicas

La normativa también amplía a los medios electrónicos la prohibición de contenidos racistas.

Una de la falencias que expertos en seguridad informática y juristas han detectado en esta Ley, es la falta de precisión en los términos que se emplea en la misma: de acuerdo con la ley, incurre en delito la persona que accede a un ordenador superando un mecanismo de seguridad, sin embargo no especifica lo que se considera un mecanismo de seguridad.

Colombia: En la nación colombiana, el debate de los delitos informáticos desembocó en el 2009 en la promulgación de la Ley 1273, por una iniciativa del reconocido Juez

Recibido: Enero 2015. **Aceptado:** Abril 2015

Alexander Díaz García, en la que se crea nuevos tipos penales relacionados con delitos informáticos y la protección de la información, amparando un nuevo bien jurídico protegido al que se denominó **"**De la Protección de la información y de los datos", y que se halla dividido en dos capítulos : "De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos" y "De los atentados informáticos y otras infracciones", (República de Colombia, 2009).

Las conductas tipificadas son: daño informático**,** acceso abusivo a un sistema informático, obstaculización ilegítima de sistema informático o red de telecomunicación, interceptación de datos informáticos, uso de software malicioso, violación de datos personales, suplantación de sitios web para capturar datos personales*,* hurto por medios informáticos y semejantes y transferencia no consentida de activos.

México: En México, a nivel federal, los delitos informáticos constan tipificados en el libro Segundo Título Noveno, en los artículos 210 y 211 bis, 1 a 7e, del Código Penal Federal desde 1999; sin embargo que a nivel local Sinaloa fue la primera jurisdicción en tipificar los delitos informáticos en 1982, estipulándose delitos como el cracking, hacker, crackers, ciberpunk, spam, entre otros.

Para la abogada Ivonne Muñoz, una de las especialistas más reconocidas en México acerca de ciberdelincuencia, existen por lo menos 200 delitos informáticos tipificados en los distintos Estados de México. La influencia de esta profesional es tal, que la legislación de su país recogió una investigación plasmada en su obra "Delitos Informáticos en México" publicada en el 2006; y cuyo aporte se puede apreciar en la inclusión de 35 nuevos delitos informáticos repartidos en los diferentes Estados mexicanos; siendo los últimos en tipificarse el 28 de marzo del 2012 los siguientes:

1. Revelación de secretos
2. Cracking
3. Hacking; y,
4. *Cyberbullyin*g

Venezuela: Sin duda, en cuanto a delitos informáticos, la legislación venezolana es de las más completas e integrales de Latinoamérica. En este país se considera como bien jurídico "La protección de los sistemas informáticos que contienen, procesan, resguardan y transmiten la información"

El objeto de la Ley venezolana se orienta a la tipificación de las conductas ciberdelictuales intentando salvaguardar los sistemas que empleen tecnologías de información.

Efectivamente, desde el 2001 la República Bolivariana de Venezuela consagra un sinnúmero de infracciones informáticas sancionadas con privación de la libertad. Conductas que a continuación se detallan (República de Venezuela, 2011):

- Acceso indebido.
- Sabotaje o daño a sistemas
- Acceso indebido o sabotaje a sistemas protegidos

Recibido: Enero 2015. **Aceptado:** Abril 2015

- Posesión de equipos o prestación de servicios de sabotaje
- Espionaje informático
- Falsificación de documentos
- Hurto informático
- Fraude informático
- Obtención indebida de bienes o servicios
- Manejo fraudulento de tarjetas inteligentes o instrumentos análogos
- Apropiación de tarjetas inteligentes o instrumentos análogos
- Provisión indebida de bienes o servicios
- Posesión de equipo para falsificaciones
- Violación de la privacidad de la data o información de carácter personal
- Violación de la privacidad de las comunicaciones
- Revelación indebida de data o información de carácter personal
- Difusión o exhibición de material pornográfico
- Exhibición pornográfica de niños o adolescentes
- Apropiación de propiedad intelectual
- Oferta engañosa.

España: España ha considerado una cantidad considerable de delitos informáticos que se hallan tipificados en su Código Penal. Las sanciones se recogen en la Ley Orgánica 10/1995, publicada en el Boletín Oficial del Estado con el número 281, el 24 de noviembre de 1995.

En el referido cuerpo legal se recogen las siguientes conductas delictuales relacionadas a la actividad informática (Ley 10.1995):

España: defraudaciones de fluido eléctrico o análogas, daños informáticos, difusión de material pornográfico, defraudaciones por vía informática, Obstaculización o interrupción del funcionamiento de un sistema informático ajeno, robo inutilizando sistemas específicos de alarma o guarda descubrimiento y revelación de secreto y acceso sin autorización robo afectando sistemas informáticos, estafa empleado herramientas informáticas, defraudaciones por vía informática, receptación y blanqueo de activos, (República de España, 1995).

Chile: El 7 de julio de 1993, Latinoamérica empezó a incluir en su normativa a los delitos informáticos. Chile fue de los primeros Estados en crear una ley que tipificó estos delitos, mediante la Ley 19223 denominada “Ley contra Delitos Informáticos”, (República de Chile, 1993).

Esta ley ofreció en aquella época un aporte significativo en cuanto al bien jurídico que es protegido por la tipificación de los Delitos Informáticos. Aunque no se trata de un cuerpo jurídico completo -para la actualidad- .

Este cuerpo jurídico está compuesto por cuatro artículos que tratan sobre la destrucción o inutilización de un sistema de tratamiento de información. Hecho que puede ser castigado con prisión de un año y medio a cinco. Igualmente se tipifica el apoderamiento, uso o conocimiento indebido, intercepción, interferencia o accesión indebida en un sistema de información.

Recibido: Enero 2015. **Aceptado:** Abril 2015

Es menester destacar que Chile fue de los pioneros no solo en la tipificación de los delitos informáticos, sino en crear entes que se encarguen de su investigación. Efectivamente, el 16 de octubre del año 2000 se crea la Unidad especializada en delitos cometidos vía Internet. Éste ente forma parte de La Policía de investigaciones de Chile, y se encarga de detectar amenazas, estafas, falsificación, pornografía infantil en internet, y todo tipo de conducta informática que lesione derechos de terceros.

Sin embargo de lo efectuado por la Comunidad Internacional, existen criterios que manifiestan que las clasificaciones propuestas resultan incompletas frente a la gran cantidad de conductas cibercriminales que se presentan en el diario vivir de las personas, siendo menester detectar las debilidades detectadas en las clasificaciones planteadas por organismos internacionales y las legislaciones.

De las debilidades del conjunto de las legislaciones del mundo

Una vez analizada la realidad jurídica de algunos Estados, se debe precisar que las debilidades que se detallan a continuación, obedece a la insuficiente tipificación en la legislación internacional; sin perjuicio del estudio que sobre el tema se ha efectuado en el en el ámbito doctrinario. Con el antecedente expuesto, anotamos las debilidades identificadas en cuanto a la clasificación de los delitos informáticos en el contexto internacional:

- Las figuras delictuales del acceso indebido, el daño informático y la interceptación de datos no son abordados tomando en cuenta cada una de las circunstancias como puede ejecutado. Es decir, no se establecen penas de acuerdo al daño que causen.
- En cuanto al delito informático en el sistema financiero, no se toma en cuenta al ataque que cause la suspensión del servicio -afectando el sistema informático-.
- La vulneración al derecho a la intimidad y al honor no es abordada con detenimiento ni se considera las circunstancias cómo fue cometida, ya sea por disponer indebidamente de imágenes, video o audio de terceros; o por afirmaciones falsas que desdigan de una persona.
- En cuanto a las conductas criminales que afectan al conjunto social: existen algunas que atacan individualmente a las personas, y otros que efectivamente atacan al mismo tiempo al conglomerado social. Entre estas conductas delictuales tenemos aquellas que provocan pánico o afectan a la población, sea por irrogar afirmaciones falsas y/ o inoportunas, por paralizar servicios públicos, o por difundir colectivamente videos, imágenes o grabaciones de violencia extrema, como ejecuciones y mutilaciones reales publicados en la Web, o aquellos que incitan al cometimiento de conductas reñidas con la ley.
- En el tratamiento de la pornografía infantil no se considera la creación, edición, publicación, o descargas de imágenes o dibujos animados que sugieran prácticas sexuales de personas que no han cumplido su mayoría de edad. Se ha concluido a nivel doctrinario que no es lo mismo utilizar con fines pornográficos a seres humanos que si existen, que emplear imágenes o dibujos animados irreales de contenido sexual.
- El tratamiento a la usurpación de identidad en redes sociales es casi nulo, más si consideramos que la misma se puede efectuar con la apertura de cuentas

Recibido: Enero 2015. **Aceptado:** Abril 2015

usando la identidad de terceros, con el apoderamiento indebido de cuentas, o usando indebidamente imágenes fotográficas que no corresponden al usuario de la misma.

- El hostigamiento psicológico es casi nulo dentro de la clasificación de los delitos informáticos. Hostigamiento que puede configurarse como cyberbulling o acoso.
- Las disposiciones de la legislación internacional y la doctrina, no consagran la instrucción dolosa que brinda una persona a otra en el manejo de sistemas informáticos para cometer delitos.

Con los antecedentes referidos, resulta indispensable desarrollar una nueva y minuciosa clasificación de conductas delictuales ejecutadas con herramientas informáticas, en un ejercicio que ofrezca un marco ciberdelictual completo y preciso, que extraiga lo mejor de legislaciones de mayor avanzada que la nuestra, y de reconocidas posiciones doctrinarias.

Clasificación de los delitos informáticos

A continuación procedemos a compilar en una sola clasificación las conductas cibercriminales tipificadas en las legislaciones, o detalladas en la doctrina:

TÍTULO I

Del acceso indebido

Cuando una persona sin autorización o excediendo sus privilegios, ingrese o haga uso de un sistema de información.

1.1.- Del acceso indebido simple: Cuando una persona accede indebidamente a un sistema de información, con la intención de hurgar la información contenida, sin sacar utilidad de la misma ni de beneficiar a un tercero.

1.2 Del acceso indebido con dolo: Cuando una persona accede indebidamente a un sistema de información, con la intención de hacerse de la información contenida, para sacar provecho personal, perjudicar a una persona, o beneficiar a un tercero.

1.3 Del acceso indebido con vulneración de seguridades: Cuando una persona accede indebidamente, empleando cualquier medio informático que vulnere o se apodere de la seguridad de un sistema informático.

1.4 Del acceso indebido sin vulneración de seguridades: Cuando una persona accede indebidamente a un sistema de información, aprovechándose del descuido o negligencia del titular del sistema informático y/o del funcionario bajo cuya responsabilidad recaiga su seguridad y/o custodia

1.5 Del acceso indebido a sistemas informáticos secretos del Estado.- Cuando el acceso indebido, sea simple, doloso, con o sin vulneración de seguridades, se efectúe en sistemas informáticos que contengan información destinada a funciones públicas o que contenga información personal o patrimonial de personas naturales o jurídicas, o se trate de información reservada del Estado o que pueda comprometer su seguridad interna o externa, o afecten sus relaciones internacionales.

TÍTULO II

Recibido: Enero 2015. **Aceptado:** Abril 2015
Universidad Regional Autónoma de los Andes UNIANDES

Daño a sistemas informáticos.-

Daño es la destrucción, alteración o modificación ejecutada por una persona en un sistema informático

2.1 Daños a particulares

2.1.1 De los daños a sistemas informáticos con dolo.- Cuando el daño a sistemas informáticos se efectúe con premeditación y/o con la clara intención de hacerlo, considerando las siguientes circunstancias:

a) Cuando el daño ocasione perjuicios económicos en el sistema informático

b) Cuando a más del perjuicio económico ocasionado en el sistema informático, provoque otros perjuicios o se afecte intereses de un tercero.

2.1.2 Daños a sistemas informáticos con culpa.

- Cuando una persona dañe un sistema informático por un acto de imprudencia, negligencia, impericia o inobservancia de normas básicas de manejo del sistema informático o de limpieza de dispositivos extraíbles. Considerando las circunstancias de los literales a) y b)

2.2 Daños a sistemas informáticos del Estado

2.2.1 De los daños a sistemas informáticos con dolo.- Cuando el daño a sistemas informáticos de una entidad estatal se efectúe con premeditación y/o con la clara intención de hacerlo, considerando las siguientes circunstancias:

a) Cuando el daño ocasione perjuicios económicos únicamente en el sistema informático.
b) Cuando el daño a más del perjuicio referido en el literal a), ocasione otros perjuicios, o cause afectación irreparable en la información del Estado y/o de los particulares, o comprometa la seguridad interna o externa.

2.2.2 Daños a sistemas informáticos con culpa.- Cuando una persona dañe un sistema informático de una entidad estatal por un acto de imprudencia, negligencia, impericia o inobservancia de normas básicas de manejo del sistema informático o de limpieza de dispositivo extraíbles. Considerando las circunstancias de los literales a) y b). Agravándose su situación jurídica si a su cargo estuvo el cuidado o custodia del sistema informático afectado.

TÍTULO III

Del registro indebido de pulsaciones

La persona que mediante el empleo de un dispositivo o programa informático o software se encargue de registrar todo lo que un tercero escriba al utilizar un teclado.

TÍTULO IV

Del Sistema Financiero

4.1 La transferencia ilícita de fondos.- El que sin estar autorizado haga uso de cualquier medio informático para transferir fondos a nombre propio o de un tercero, sea dentro de la misma institución financiera, o de una institución financiera a otra.

Recibido: Enero 2015. **Aceptado:** Abril 2015

4.2 La transferencia de fondos ilícitos.-: El que sin estar autorizado use cualquier medio informático para acceder a la cuenta de clientes de una Institución Financiera, para transferir fondos ilícitos.

4.3 De la captación ilegítima de datos.- El que mediante el empleo de cualquier medio informático, engañe a los clientes para sacar su información confidencial, sea contraseñas o información detallada sobre tarjetas inteligentes u otra información bancaria, para obtener provecho personal o para beneficiar a un tercero.

4.4 Reproducción, tenencia, uso y comercialización indebida de tarjetas inteligentes.- El que con el empleo de medios informáticos y sin estar autorizado, reproduzca tarjetas inteligentes de terceros. Incurriendo también en este delito las personas que las posean injustificadamente; las usen o comercialicen.

4.5 Sabotaje informático.- El que con empleo de cualquier medio tecnológico, impida el funcionamiento de una institución financiera, afectando su sistema informático. Agravándose la situación jurídica del responsable, de acuerdo al perjuicio económico ocasionado a los clientes y a la misma institución.

TÍTULO V

De los delitos contra la intimidad y el honor

Cuando sin autorización alguna, y valiéndose de herramientas informáticas, publique, mire o descargue en redes telemáticas, imágenes, videos y/o grabaciones, que violen el derecho a la intimidad de una persona.

Delito contra la intimidad.

5.1 Cuando una persona publique o descargue en redes telemáticas imágenes, videos o grabaciones reales de actos privados de un tercero, que afecten su imagen ante terceros.

5.2 Cuando una persona suba, mire o baje en redes telemáticas imágenes, videos o grabaciones de partes íntimas del cuerpo, vida sentimental, sexual, o estado de salud de otra persona.

Delitos contra el honor

5.3 Cuando una persona suba en redes interconectadas imágenes, videos o grabaciones de un tercero que tienda a ridiculizar su imagen y/o causarle burla social.

5.4 Cuando una persona injurie a un tercero, mediante imágenes, videos y/o grabaciones, subidas y/o publicadas en redes interconectadas.

TÍTULO VI

De los delitos informáticos de afectación social

6.1 Terrorismo informático.- Cuando una persona empleando medios informáticos, difunda en redes telemáticas noticias falsas o rumores infundados que causen pánico en la población.

Recibido: Enero 2015. **Aceptado:** Abril 2015
Universidad Regional Autónoma de los Andes UNIANDES

6.2 Sabotaje de servicios públicos.- Cuando una persona mediante el empleo de cualquier herramienta informática, obstruya o interrumpa la atención o abastecimiento de servicios públicos.

6.3 Transmisión de contenidos violentos.-Cuando una persona sin estar autorizada, publique, ofrezca, reproduzca o descargue videos, imágenes o grabaciones con contenido de significada violencia u odio.

6.4 Instigación: El que empleando medios informáticos, difunda imágenes, videos y/o grabaciones que inciten al cometimiento de actos reñidos con la ley.

TÍTULO VII

Delitos informáticos contra la propiedad intelectual

7.1 Apropiación indebida.- La persona que empleando medios informáticos violente seguridades y/o contraseñas de sistema de hardware o software, para sustraer información concerniente a propiedad industrial y/ o derechos de autor.

7.2 De la copia no autorizada.- La persona que empleando medios informáticos, reproduzca y/o distribuya copias de obras que se hallen protegidas por el derecho de autor, así como su transmisión al público o su puesta a disposición en redes interconectadas, sin la autorización de los propietarios legítimos.

7.3 De la captación y reproducción no autorizada.- El que empleando medios informáticos capte y reproduzca sin autorización, imágenes y/o audio de medios de comunicación.

TÍTULO VIII

De la Estafa Informática

La persona que a través de medios informáticos, utilice engaños para que un tercero trasfieran a su nombre o el de un tercero, fondos o activos.

TÍTULO IX

Interceptación de datos informáticos

La persona que sin autorización, se apodere de datos informáticos antes de que lleguen a su destino.

9.1 Interceptación simple de datos públicos.- La persona que sin autorización, intercepte datos informáticos del Estado, con la mera intención de hurgar en ellos; sin sacar provecho económico para sí o para un tercero, y sin que los divulgue

9.2 Interceptación de datos públicos con afectación.- La persona que sin autorización, intercepte datos informáticos del Estado, con la intención de sacar provecho económico para sí o para un tercero; o, con la intención de divulgar información reservada y que pueda comprometer la seguridad interna y/o externa, la estabilidad política dentro del país como a nivel internacional

9.3 Interceptación simple de datos informáticos de particulares.- La persona que sin autorización, intercepte datos informáticos de particulares, con la mera intención de

Recibido: Enero 2015. **Aceptado:** Abril 2015
Universidad Regional Autónoma de los Andes UNIANDES

hurgar en ellos; sin sacar provecho económico para sí o para un tercero, y sin que los divulgue.

9.4 Interceptación de datos de particulares con afectación.- La persona que sin autorización, intercepte datos informáticos de particulares, con la intención de sacar provecho económico para sí o para un tercero y/o con la intención de divulgar la información apoderada, considerándose agravante si la misma se refiere a la vida sentimental, sexual, estado de salud o preferencia sexual de otra persona.

TÍTULO X

De la Pornografía Infantil

10.1 Cuando una persona cree, edite, publique, ofrezca, abra, posea o descargue desde un software y/o mediante redes interconectadas, contenido sexual de personas menores de dieciocho años.

10.1 Cuando una persona realice, cree, edite, publique, ofrezca, abra o descargue desde un software y/o mediante redes interconectadas, imágenes animadas o similares, de contenido sexual de personas menores de dieciocho años.

TÍTULO XI

De la falsedad

Cuando una persona con empleo de medios informáticos introduzca, altere, borre, o suprima datos de documentos públicos, generando datos no auténticos, con la intención de hacerlos pasar como auténticos.

TÍTULO XII

De los correos no deseados

La persona que mediante el empleo de sistemas informáticos envíe anuncios no solicitados con fines comerciales, a la dirección de correo electrónico de cualquier persona con la que no tenga relación personal, profesional o comercial preexistente; a no ser que el receptor haya expresado previamente su consentimiento o permiso.

TÍTULO XIII

Usurpación de identidad en redes sociales y direcciones electrónicas

11.1 De la apertura de cuentas.- Cuando una persona abra una cuenta en una red social o una dirección electrónica empleando nombres y apellidos de una tercera persona que exista o haya existido, efectuando usos que den a entender que se trata de la persona usurpada.

11.2 Apoderamiento indebido de cuentas.- Cuando una persona se apodere fraudulentamente de una cuenta de red social o dirección electrónica de una persona que exista o haya existido, efectuando usos que den a entender que se trata de la persona despojada del control de su cuenta.

11.3 Uso indebido de imágenes fotográficas.- Cuando en su cuenta de red social o dirección electrónica, haga uso de fotografías de otros u otras personas que existan o hayan existido, como parte de su identificación ante los demás.

Recibido: Enero 2015. **Aceptado:** Abril 2015
Universidad Regional Autónoma de los Andes UNIANDES

TÍTULO XIV

Del hostigamiento Psicológico

12.1 Cyberbullying.- Cuando una persona empleando medios informáticos, amenace, intimide o se burle de otra.

12.2 Acoso informático.- Cuando de manera persistente y/o habitual emplee cualquier medio informático para ejecutar actos considerados de persecución sentimental o sexual a una persona, sin su consentimiento.

TÍTULO XV

De las tecnologías y herramientas informáticas

13.1 Posesión dolosa: cuando una persona sin estar autorizada, se encuentra en posesión de tecnologías y/o herramientas informáticas, para copiar, vulnerar, o eliminar la seguridad de cualquier sistema que utilice tecnologías de información.

13.2 Transferencia dolosa: cuando una persona ofrezca o reciba en donación; ponga en venta o compre tecnologías y/o herramientas informáticas, con la intención de destinarlas a copiar, vulnerar o eliminar la seguridad de cualquier sistema que utilice tecnologías de información.

13.3 Virus informáticos.- La persona que cree, difunda, transfiera, acepte o compre un malware que tenga por objeto alterar el normal funcionamiento de un sistema informático, sin el consentimiento del usuario.

TÍTULO XVI

De la Instrucción Ilícita

Incurre en este delito la persona que enseñe o asesore a un tercero, sobre cómo efectuar uno de los delitos establecidos en la presente clasificación. Exceptuándose la instrucción académica recibida en establecimientos educativos, cuyo objeto no sea el de instruir en el cometimiento de delitos informáticos.

CONCLUSIONES

Todas las clasificaciones plasmadas sea en legislaciones o en la doctrina, contribuyen en cuanto a la identificación de las conductas criminales ejecutadas con empleo de medios informáticos. Sin embargo, en la mayoría no se aborda con amplitud todas las circunstancias como pueden ser ejecutadas. Es por eso que la clasificación propuesta en el presente artículo reviste de vital importancia, toda vez que en el ejercicio de investigación y análisis que el autor ha desarrollado, se ha logrado estructurar una clasificación que abarca una gran variedad de hechos cibercriminales, con detalle de las circunstancias de su cometimiento.

Por lo señalado, la clasificación propuesta en el presente artículo científico, puede servir de base y/o fuente de consulta para que el legislador estructure y tipifique en el ordenamiento jurídico nuevas conductas cibercriminales, o amplíe las que se encuentran tipificadas. De igual forma, contribuirá al estudio y análisis del tema en espacios académicos o en el ámbito doctrinal, tanto para profesionales y estudiantes del Derecho como de la informática.

Recibido: Enero 2015. **Aceptado:** Abril 2015
Universidad Regional Autónoma de los Andes UNIANDES

Por otro lado, es necesario que los Estados aúnen esfuerzos, recursos humanos y económicos para combatir este delito, toda vez que la ciberdelincuancia en Estados con poco avance jurídico y tecnológico, le está ganando la batalla a la administración de justicia y a la policía, toda vez que existen conductas informáticas lesivas, que no están tipificadas expresamente como delitos en su ordenamiento jurídico penal.

REFERENCIAS

Carrión, Hugo Daniel. (2001). Presupuestos para la Punibilidad del Hacking. Recuperado el 2 de Mayo de 2015, de: http://usuaris.tinet.cat/acl/html_web/seguridad/tesis/Cap4.pdf

Código Orgánico Integral Penal. (2014). Corporación de Estudios y Publicaciones. Quito. Recuperado el 6 de Abril de 2015, de: http://www.cuenca.gob.ec/biblicuenca/opac_css/index.php?lvl=author_see&id=15614

Convención para la Protección de Producción de Fonogramas. (1990). México, Editorial Dykinson.

Convenio sobre Ciberdelincuencia. Serie de Tratados Europeos. Budapest. (2001). Recuperado el 21 de Abril de 2015, de: http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/ETS_185_spanish.PDF

Cuello, Enrique. (1983). Derecho Penal. Editorial Bosch.

Cuello Calón, Eugenio. (1960). Derecho Penal. México, ed. Nacional.

Ensayo sobre la importancia de evitar delitos informáticos. (s.f.). Recuperado el 6 de Mayo de 2015, de: https://sites.google.com/site/equipo8delitosinformaticos/ensayo-sobre-la-importancia-de-evitar-delitos-informaticos

Legislación y Delitos informáticos-La Información y el Delito (2009). Recuperado el 6 de Mayo de 2015, de: http://www.segu-info.com.ar/legislacion/

Lima de la LUZ, María. (1984). Delitos Electrónicos. México, Ediciones Porrúa.

Moliner, María. (1996). Diccionario de María Moliner. Edición Digital.

Muñoz, Ivonne. (2006). Delitos Informáticos en México. México

Organización Mundial de la Propiedad Intelectual (1974). Convenio sobre la Distribución de Señales Portadoras de Programas Transmitidas por Satélite. Recuperado el 6 de Abril de 2015, de: http://www.wipo.int/treaties/es/text.jsp?file_id=283797

República de Argentina. (2008). Ley 26.388 de Delitos Informáticos en Argentina. Recuperado el 17 de Abril de 2015, de: http://www.taringa.net/post/info/2087099/Ley-26-388---Delitos-Informaticos-en-Arg.html

República de Brasil (2012). Ley de delitos informáticos 12737/12. Recuperado el 21 de Marzo de 2015, de:

Recibido: Enero 2015. **Aceptado:** Abril 2015

http://riquertdelincuenciainformatica.blogspot.com/2013/01/brasil-ley-de-delitos-informaticos.html

República de Chile. (1993). Ley 19223. Recuperado el 13 de Abril de 2015, de: http://www.leychile.cl/Navegar?idNorma=30590

República de Colombia. (2009). Ley 1273. Recuperado el 11 de Mayo de 2015, de: http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html

República de España (1995). Ley Orgánica 10. Recuperado el 6 de Abril de 2015, de: http://noticias.juridicas.com/base_datos/Penal/lo10-1995.html

República de México. (1999). Código Penal Federal. Recuperado el 11 de Mayo de 2015, de: http://info4.juridicas.unam.mx/ijure/tcfed/8.htm?s

República de Venezuela. (2011). Ley Especial Contra los Delitos Informáticos. Recuperado el 3 de Mayo de 2015, de: http://www.oas.org/juridico/spanish/mesicic3_ven_anexo18.pdf

Télles Valdés, Julio. (1996). Derecho Informático. México, McGraw Hill.

Recibido: Enero 2015. **Aceptado:** Abril 2015