LA SEGURIDAD JURÍDICA FRENTE A LOS DELITOS INFORMÁTICOS
LEGAL SECURITY AGAINST CYBERCRIME

Carlos Alcívar Trejo. M.D.C[*]
Gustavo Arturo Domenech Alvarez[**]
Karla Maribel Ortìz Chimbo. Msc[**]

SUMÁRIO: .- Introducción.- Antecedentes históricos.- Los delitos informáticos en el Ecuador.- Análisis legal: Regulación por paises.- Análisis Legal en el Ecuador.- Conclusiones y Recomendaciones.- Referencias.

SUMMARY: .- Introduction.- Historical background.- Computer crime in Ecuador.- Legal Analysis: Regulation by countries.- Legal analysis in Ecuador.- Conclusions and recommendations.- References.

RESUMEN

En el presente artículo, se presenta el problema de los delitos informáticos que pueden ser considerados como crímenes electrónicos, tan graves que pueden llegar a ser un genérico problema para el avance de la informática. Sin embargo este puede tener consigo delitos tan graves como el robo, falsificación de documentos, fraudes, chantajes y malversación de caudales públicos. Un ejemplo muy común es cuando una persona llega a robar información y a causar daños de computadoras o servidores que pueden llegar a ser absolutamente virtuales porque la información se encuentra en forma digital y el daño cada vez se vuelve más grande. Muchas de las personas que cometen este tipo de delitos informáticos tienen diferentes características tales como la habilidad del manejo de los diferentes sistemas informáticos o la realización de y tareas laborales que le facilitan el acceso de carácter simple. También se le puede definir como toda acción culpable por el ser humano quede alguna u otra manera nos lleva a causar un perjuicio a personas que sin necesariamente se beneficien de los distintos tipos de manejo informático ya que los delincuentes que hacen este tipo de delitos nos están quitando la

[*]Catedrático a tiempo completo de la Universidad Tecnológica ECOTEC (Coordinador Académico de la Facultad de Derecho), Catedrático medio tiempo de la Carrera Ingeniería en Sistemas y Networking (Facultad de ciencias matemáticas y físicas). E-mail: carlos.alcivart@ug.edu.ec.

[**] Estudiante de la Carrera de Ingeniería en Networking y Telecomunicaciones. Universidad de Guayaquil. E mail: gustavo.domenecha@ug.edu.ec.

[**] Coordinadora de la Comisión de Evaluación y Acreditación de la Facultad de Filosofía y Catedrática a medio tiempo de la Universidad de Guayaquil, Carrera Ingeniería en Sistemas y Networking (Facultad de ciencias matemáticas y físicas). E mail: karla.ortizch@ug.edu.ec.

posibilidad de ver todo de una manera muy distinta y con distinta me refiera a verla de manera original sin quitarle nada o sin quitarlo de aquel lugar donde siempre se mantuvo.
Palabras clave: Delitos, Amenazas, Seguridad Informática, detección, empresas, información.

ABSTRACT

In this article, the problem of computer crimes that can be considered as electronic crimes so serious that they can become a generic problem for the development of information presented. However this can have him as serious crimes such as theft, forgery, fraud, racketeering and embezzlement of public funds. A common example is when a person comes to steal information and cause damage to computers or servers that can become quite virtual because the information is in digital form and the damage becomes increasingly larger. Many of those who commit this type of cybercrime have different features such as the ability of handling different computer systems or performing work tasks and which facilitate access by single character. It can also be defined as any culpable action by humans remains some way or another leads to cause us harm to people without necessarily benefit from the various types of computer management and criminals who do this type of crime are we removing the ability to see everything in a very different way and with different concerns me see it in an original way without taking anything or without removal from the place where he always stayed.
Keywords: Crime, Threats, Security, Detection, companies information.

1. INTRODUCCIÓN

Un delito informático o ciberdelito es toda aquella acción antijurídica y culpable, que se da por vías informáticas o que tiene como objetivo destruir y dañar ordenadores, medios electrónicos y redes de Internet. Debido a que la informática se mueve más rápido que la legislación, existen conductas criminales por vías informáticas que no pueden considerarse como delito, según la “Teoría del delito”, por lo cual se definen como abusos informáticos (los tipos penales tradicionales resultan en muchos países inadecuados para encuadrar las nuevas formas delictivas (Acevedo, 2010), y parte de la criminalidad informática. La criminalidad informática consiste en la realización de un tipo de actividades que, reuniendo los requisitos que delimitan el concepto de delito, sean llevados a cabo utilizando un elemento informático (Cuervo, 2008).

Los delitos informáticos son aquellas actividades ilícitas que: (a) Se cometen mediante el uso de computadoras, sistemas informáticos u otros dispositivos de comunicación (la informática es el medio o instrumento para realizar un delito); o (b) Tienen por objeto causar daños, provocar pérdidas o impedir el uso de sistemas informáticos (delitos informáticos).

Los también conocidos como Ciberdelitos como lo señala Téllez (2004, p. 7) que son actitudes contrarias a los intereses de las personas en que se tiene a las computadoras como instrumento o fin (concepto atípico) o las conductas atípicas, antijurídicas y culpables en que se tiene a las computadoras como instrumento o fin (concepto típico).

Mucha información es almacenada en un reducido espacio, con una posibilidad de recuperación inmediata, pero por complejas que sean las medidas de seguridad que se puedan implantar, aún no existe un método infalible de protección (Pecoy, 2012).

La criminalidad informática tiene un alcance mayor y puede incluir delitos tradicionales como el fraude, el robo, chantaje, falsificación y la malversación de caudales públicos en los cuales ordenadores y redes han sido utilizados como medio. Con el desarrollo de la programación y de Internet, los delitos informáticos se han vuelto más frecuentes y sofisticados.

Existen actividades delictivas que se realizan por medio de estructuras electrónicas que van ligadas a un sin número de herramientas delictivas que buscan infringir y dañar todo lo que encuentren en el ámbito informático: ingreso ilegal a sistemas, interceptado ilegal de redes, interferencias, daños en la información (borrado, dañado, alteración o supresión de data crédito), mal uso de artefactos, chantajes, fraude electrónico, ataques a sistemas, robo de Bancos, ataques realizados por hackers, violación de los derechos de autor, pornografía infantil, pedofilia en Internet, violación de información confidencial y muchos otros.

2. ANTECEDENTES HISTÓRICOS

El término delito informático se acuñó a finales de los años noventa, a medida que Internet se expandió por toda Norteamérica. Después de una reunión en Lyón, Francia, se fundó un subgrupo del grupo de naciones que conforman el denominado “G8” con el objetivo de estudiar los problemas emergentes de criminalidad que eran propiciados por o que migraron a Internet.

El “Grupo de Lyón” utilizó el término para describir, de forma muy imprecisa, todos los tipos de delitos perpetrados en la red o en las nuevas redes de telecomunicaciones que tuvieran un rápido descenso en los costos.

Al mismo tiempo, y guiado por los participantes en el grupo de Lyón, el Consejo Europeo comenzó a diseñar el Tratado sobre Delito Informático[1]

Este tratado, que fuera presentado a la opinión pública por primera vez en el año 2000, incorporó una nueva gama de técnicas de vigilancia que las agencias encargadas de la aplicación de la ley consideraban necesarias para combatir el “delito informático”. ¿Cómo se definió el delito informático? La versión final de ese tratado, aprobada en noviembre de 2001 después de los acontecimientos del 11 de septiembre, no definió el término. Es un término muy amplio referido a los problemas que aumentaron el poder informático, abarataron las comunicaciones y provocaron que haya surgido el fenómeno de Internet para las agencias policiales y de inteligencia. El tratado describe de la siguiente manera las diferentes disposiciones y áreas temáticas en las que se requiere una nueva legislación:

- Delitos contra la confidencialidad, integridad y disponibilidad de los datos y sistemas informáticos.
- Delitos relacionados con las computadoras [falsificación y fraude].

[1] Fuente: http://pcolorador.blogspot.com/2008/04/delitos-informaticos_14.html

- Delitos relacionados con el contenido [pornografía].
- Delitos relacionados con la violación del derecho de autor y los derechos asociados.
- Responsabilidades secundarias y sanciones [cooperación delictiva, responsabilidad empresarial].

3. ANÀLISIS

No hay definición de carácter universal propia de delito informático, no obstante, muchos han sido los esfuerzos de expertos que se han ocupado del tema y, aun cuando no existe una definición con carácter universal, se ha formulado conceptos funcionales atendiendo a realidades nacionales concretas.

En el ámbito internacional se considera que no existe una definición propia del delito informático, pero, al consultar bibliografía, específicamente del español Carlos Sarzana, en su obra Criminalitá e tecnología, los crímenes por computadora comprenden “cualquier comportamiento criminógeno en el cual la computadora ha estado involucrada como material o como objeto de la acción criminógena, o como mero símbolo”.

Dentro de los criterios doctrinales de algunos tratadistas, tenemos a Nidia Callegari define al “delito Informático” como “aquel que se da con la ayuda de la informática o de técnicas anexas”.[2] Rafael Fernández Calvo define al “delito informático” como la realización de una acción que, reuniendo las características que delimitan el concepto de delito, se ha llevado a cabo utilizando el elemento informático o telemático contra los derechos y libertades de los ciudadanos definidos en el título 1 de la Constitución Española”. María de la Luz Lima dice que el “delito electrónico”, “en un sentido amplio, es cualquier conducta criminógena o criminal que en su realización hace uso de la tecnología electrónica ya sea como método, medio o fin y que, en un sentido estricto, el delito informático es cualquier acto ilícito penal en el que las computadoras, sus técnicas y funciones desempeñan un papel, ya sea como método, medio o fin”. Julio Téllez Valdés conceptualiza al “delito Informático” en forma típica y atípica, entendiendo por la primera a “las conductas típicas, antijurídicas y culpables en que se tiene a las computadoras como instrumento o fin” y por las segundas “actitudes ilícitas en que se tiene a las computadoras como instrumento o fin”. Por otra parte, debe mencionarse que se ha formulado diferentes denominaciones para indicar las conductas ilícitas en las que se usa computadoras tales como “delitos informáticos”, “delitos electrónicos”, “delitos relacionados con la computadora”, “crímenes por computadora”, delincuencia relacionada con el ordenador”. Analizando estas determinaciones conceptuales estamos en condiciones de brindar una definición de delito informático: Son todas aquellas conductas ilícitas susceptibles de ser sancionadas por el derecho penal, que hacen uso indebido de cualquier medio Informático implicando actividades criminales.

[2]Publicado el 11 septiembre, 2015 por jaimeanimo , https://elmuraldelaconstitucion.wordpress.com/2015/09/11/delitos-y-fraudes-informaticos/

Generalidades

La criminalidad informática incluye una amplia variedad de delitos informáticos (Pecoy, 2012). El fenómeno se puede analizar en dos grupos:

Informática como objeto del delito. Esta categoría incluye por ejemplo el sabotaje informático, la piratería informática, el hackeo, el crackeo y el DDNS (Denegación de servicio de nombres de dominio).

Informática como medio del delito. Dentro de este grupo se encuentra la falsificación de documento electrónico, cajeros automáticos y tarjetas de crédito, robo de identidad, phreaking, fraudes electrónicos y pornografía infantil.

Crímenes específicos

Sabotaje informático: Implica que el "delincuente" recupere o busca destruir el centro de cómputos en sí (las máquinas) o los programas o informaciones almacenados en los ordenadores. Se presenta como uno de los comportamientos más frecuentes y de mayor gravedad en el ámbito político.

Piratería informática: La piratería informática consiste en la violación ilegal del derecho de autor. Según la definición que en su artículo 51 brinda el ADPIC (Acuerdo sobre los aspectos de los Derechos de Propiedad Intelectual) son aquellas "mercaderías que lesionan el derecho de autor". La piratería es una de las modalidades de reproducción técnica (la otra es la reprografía-reproducción burda del original cuya apariencia dista mucho de la auténtica), que implica la elaboración de una copia semejante al original, con la intención de hacerla pasar por tal.

Existen dos modalidades que se incluyen como piratería informática a saber:

El hurto de tiempo de máquina: consiste en el empleo del computador sin autorización, y se pretende aludir a situaciones en que un tercero utiliza indebidamente recursos de la empresa en que trabaja o un sujeto autorizados se vale de tales prestaciones informáticas en un horario no permitido, utilizándolas parra su provecho sin contar con permiso para ese uso fuera de hora.

La apropiación o hurto de software y datos: en este caso el sujeto accede a un computador ajeno o a la sesión de otro usuario, retirando archivos informáticos, mediante la ejecución de los comandos copiar o cortar, para luego guardar ese contenido en un soporte propio.

Cajeros automáticos y tarjetas de crédito

Conductas mediante las cuales se logra retirar dinero del cajero automático, utilizando una tarjeta magnética robada, o los números de la clave para el acceso a la cuenta con fondos.

Robo de identidad

Luego de obtener los datos personales de un individuo, se procede a realizar todo tipo de operaciones para provecho del victimario, fingiendo ser la persona a la que se extrajo su información sensible. Encuadra como delito de estafa. Si el actuar del sujeto

activo comporta dar a conocer datos personales ajenos contenidos en base de datos a las que por su empleo tiene acceso, entonces por expreso mandato legal la figura aplicable es la de revelación de secreto profesional.

Phreaking

Es la metodología más antigua dentro de los denominados ciberdelitos, consiste en ingresar en las redes de telecomunicaciones para realizar llamadas telefónicas a larga distancia utilizando la cuenta ajena. Resulta ser una modalidad primitiva de hacking.

Sujetos agente y paciente

Muchas de las personas que cometen los delitos informáticos poseen ciertas características específicas tales como la habilidad para el manejo de los sistemas informáticos o la realización de tareas laborales que le facilitan el acceso a información de carácter sensible.

En algunos casos la motivación del delito informático no es económica sino que se relaciona con el deseo de ejercitar, y a veces hacer conocer a otras personas, los conocimientos o habilidades del delincuente en ese campo.

Muchos de los "delitos informáticos" encuadran dentro del concepto de "delitos de cuello blanco", término introducido por primera vez por el criminólogo estadounidense Edwin Sutherland en 1943. Esta categoría requiere que: (1) el sujeto activo del delito sea una persona de cierto estatus socioeconómico; (2) su comisión no pueda explicarse por falta de medios económicos, carencia de recreación, poca educación, poca inteligencia, ni por inestabilidad emocional. Son individuos con una gran especialización en informática, que conocen muy bien las particularidades de la programación de sistemas computarizados, de forma tal que logran un manejo muy solvente de las herramientas necesarias para violar la seguridad de un sistema automatizado (Pecoy, 2012).

El sujeto pasivo en el caso de los delitos informáticos puede ser individuos, instituciones crediticias, órganos estatales, etc. que utilicen sistemas automatizados de información, generalmente conectados a otros equipos o sistemas externos. Víctima puede ser cualquier persona física o jurídica que haya establecido una conexión a Internet (ya que es la principal ventana de entrada para estas conductas), una conexión entre computadoras, o que en definitiva cuenta con un sistema informático para el tratamiento de sus datos (Pecoy, 2012).

Para la labor de prevención de estos delitos es importante el aporte de los damnificados que puede ayudar en la determinación del modus operandi, esto es de las maniobras usadas por los delincuentes informáticos.

4. LOS DELÌTICOS INFORMÀTICOS EN EL ECUADOR

Quito, 13 de junio del 2015.- Transferencia ilícita de dinero, apropiación fraudulenta de datos personales, interceptación ilegal de datos, pornografía infantil, acoso sexual, entre otros, se denuncian en las diferentes Unidades de la Fiscalía.[3]

[3] Publicado el 11 septiembre, 2015 por jaimeanimo

Internet abrió el paso a esas nuevas formas de delincuencia común y organizada que pone en riesgo la información privada, la seguridad en la navegación y de las instituciones públicas y privadas.

La Dirección de Política Criminal de la Fiscalía General del Estado registró 626 denuncias por delitos informáticos desde el 10 de agosto del 2014 -cuando entró en vigencia el Código Orgánico Integral Penal (COIP)- hasta el 31 de mayo del 2015. A partir del COIP se tipifica este tipo de delitos.

En el COIP se sancionan los delitos informáticos, cuyos actos se comenten con el uso de tecnología para violentar la confidencialidad y la disponibilidad de datos personales. Estos actos que se registran a través de la Internet son: fraude, robo, falsificaciones, suplantación de identidad, espionaje, clonación de tarjetas de crédito, entre otros.

Según el fiscal provincial de Pichincha, Wilson Toainga, las investigaciones referentes a los delitos informáticos se realizan de forma técnica y demanda tiempo para establecer la responsabilidad de aquellos que quebrantan la ley sentados frente a un monitor.

El fiscal Edwin Pérez, especialista en delitos informáticos, indicó que en Ecuador existen dificultades durante la investigación de delitos propiciados por el uso de la tecnología, por cuanto la información cruzada a nivel de redes sociales o cuentas de correos electrónicos no se encuentra en el país.

“Los grandes proveedores de las redes sociales y generadores de los sistemas informáticos como Google, Facebook, Yahoo, entre otros, tienen los bancos de datos de sus usuarios en Estados Unidos, y solicitar esa información puede demorar meses”, dijo el fiscal Pérez.

Un inconveniente para la investigación radica en que Ecuador no cuenta con convenios internacionales que faciliten el cruce de datos informáticos -como los que existe entre Estados Unidos y Europa-. Por ello, hay complicaciones en detectar las cuentas o las direcciones IP desde las que se habría realizado el ataque o la sustracción de información personal ante las formalidades y la virtualidad de los procesos puede tardarse meses.

Uno de los casos de delito informático se registró en mayo del 2014, Diana (nombre protegido) se preguntaba: “¿Cómo consiguieron mis datos?”. Solo recuerda que ingresó sus datos para realizar una compra por Internet, porque se ofrecían descuentos en productos de belleza. Lo único cierto es que la persona que usó su información le endeudó en 2.500 dólares, a través de débitos de su tarjeta. Su caso es investigado por la Fiscalía.

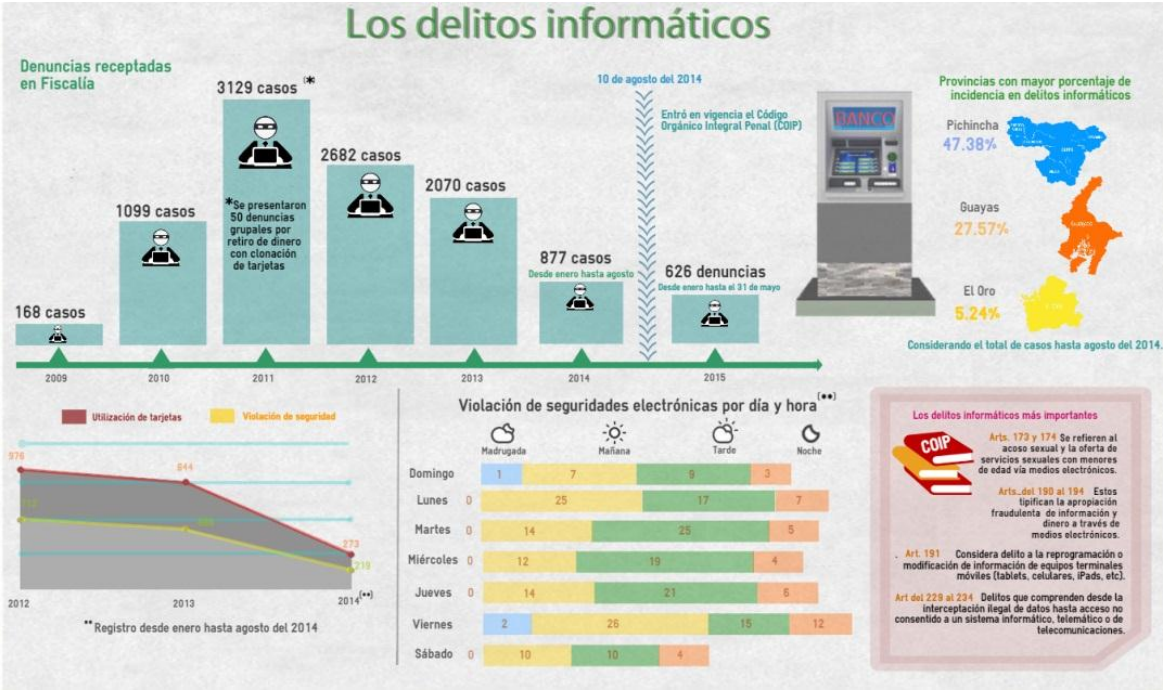
En el caso de Diana, si hubiese estado vigente el COIP y se descubriera a la persona que robó sus datos, este podría recibir una pena de uno a tres años de cárcel.

---

https://elmuraldelaconstitucion.wordpress.com/2015/09/11/delitos-y-fraudes-informaticos/

La persona que sustrajo la información de Diana compró por Internet dos celulares, una memoria externa y una tablet. La joven tiene una deuda que paga en cuotas mínimas porque su sueldo no le alcanza para cubrir más montos.

Ahora, con la aplicación del COIP, también se sancionan delitos por apropiación ilegal de datos almacenados en teléfonos inteligentes y tablets. En este, en su artículo 191 sanciona con una pena privativa de libertad de uno a tres años.



Fuente: Fiscalía General del Estado de Ecuador[4]

5. ANÀLISIS LEGAL: Regulación por países

Argentina

Conforme a la ley vigente[5], Argentina sancionó el 4 de junio del 2008 la Ley 26.388 (promulgada de hecho el 24 de junio de 2008) que modifica el Código Penal a fin de incorporar al mismo diversos delitos informáticos, tales como la 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, daño informático agravado e interrupción de comunicaciones.

Dentro de las definiciones vinculadas a la informática, tenemos que en el nuevo ordenamiento se establece que el término "documento" comprende toda representación de actos o hechos, con independencia del soporte utilizado para su fijación, almacenamiento, archivo o transmisión (art. 77 Código Penal).

[4] Publicado el Sábado, 13 Junio 2015, http://www.fiscalia.gob.ec/index.php/sala-de-prensa/3630-los-delitos-inform%C3%A1ticos-van-desde-el-fraude-hasta-el-espionaje.html
[5] Modificación al Código Penal sobre la incorporación de los Delitos Informáticos (Argentina) http://infoleg.mecon.gov.ar/infolegInternet/anexos/140000-144999/141790/norma.htm

Los términos "firma" y "suscripción" comprenden la firma digital, la creación de una firma digital o firmar digitalmente (art. 77 Código Penal).

Los términos "instrumento privado" y "certificado" comprenden el documento digital firmado digitalmente (art. 77 Código Penal).

Delitos contra menores

En el nuevo ordenamiento pasan a ser considerados delitos los siguientes hechos vinculados a la informática:

El artículo 128, señala que será reprimido con prisión de seis (6) meses a cuatro (4) años el que produzca, financie, ofrezca, comercialice, publique, facilite, divulgue o distribuya, por cualquier medio, toda representación de un menor de dieciocho (18) años dedicado a actividades sexuales explícitas o toda representación de sus partes genitales con fines predominantemente sexuales, al igual que el que organizare espectáculos en vivo de representaciones sexuales explícitas en que participaren dichos menores.

Será reprimido con prisión de cuatro (4) meses a dos (2) años el que tuviere en su poder representaciones de las descriptas en el párrafo anterior con fines inequívocos de distribución o comercialización.

Será reprimido con prisión de un (1) mes a tres (3) años el que facilitare el acceso a espectáculos pornográficos o suministrare material pornográfico a menores de catorce (14) años.

Respecto a la protección de la privacidad, el artículo 153 dice que será reprimido con prisión de quince (15) días a seis (6) meses el que abriere o accediere indebidamente a una comunicación electrónica, una carta, un pliego cerrado, un despacho telegráfico, telefónico o de otra naturaleza, que no le esté dirigido; o se apoderare indebidamente de una comunicación electrónica, una carta, un pliego, un despacho u otro papel privado, aunque no esté cerrado; o indebidamente suprimiere o desviare de su destino una correspondencia o una comunicación electrónica que no le esté dirigida.

En la misma pena incurrirá el que indebidamente interceptare o captare comunicaciones electrónicas o telecomunicaciones provenientes de cualquier sistema de carácter privado o de acceso restringido.

La pena será de prisión de un (1) mes a un (1) año, si el autor además comunicare a otro o publicare el contenido de la carta, escrito, despacho o comunicación electrónica.

Si el hecho lo cometiere un funcionario público que abusare de sus funciones, sufrirá además, inhabilitación especial por el doble del tiempo de la condena.

El artículo 153 señala que será reprimido con prisión de quince (15) días a seis (6) meses, si no resultare un delito más severamente penado, el que a sabiendas

accediere por cualquier medio, sin la debida autorización o excediendo la que posea, a un sistema o dato informático de acceso restringido.

La pena será de un (1) mes a un (1) año de prisión cuando el acceso fuese en perjuicio de un sistema o dato informático de un organismo público estatal o de un proveedor de servicios públicos o de servicios financieros.

El artículo 155 bis establece que será reprimido con multa de pesos un mil quinientos ($ 1.500) a pesos cien mil ($ 100.000), el que hallándose en posesión de una correspondencia, una comunicación electrónica, un pliego cerrado, un despacho telegráfico, telefónico o de otra naturaleza, no destinados a la publicidad, los hiciere publicar indebidamente, si el hecho causare o pudiere causar perjuicios a terceros.

Está exento de responsabilidad penal el que hubiere obrado con el propósito inequívoco de proteger un interés público.

El artículo 157 precisa que será reprimido con prisión de un (1) mes a dos (2) años e inhabilitación especial de un (1) a cuatro (4) años, el funcionario público que revelare hechos, actuaciones, documentos o datos, que por ley deben ser secretos.

El artículo 157 bis establece que será reprimido con la pena de prisión de un (1) mes a dos (2) años el que:

1. A sabiendas e ilegítimamente, o violando sistemas de confidencialidad y seguridad de datos, accediere, de cualquier forma, a un banco de datos personales;

2. Ilegítimamente proporcionare o revelare a otra información registrada en un archivo o en un banco de datos personales cuyo secreto estuviere obligado a preservar por disposición de la ley.

3. Ilegítimamente insertare o hiciere insertar datos en un archivo de datos personales.

Cuando el autor sea funcionario público sufrirá, además, pena de inhabilitación especial de un (1) a cuatro (4) años.

En cuanto a los delitos contra la propiedad, el artículo 173 inciso 16 señala que (Incurre en el delito de defraudación)...El que defraudare a otro mediante cualquier técnica de manipulación informática que altere el normal funcionamiento de un sistema informático o la transmisión de datos.

El artículo 183 del Código Penal señala que, Incurre en el delito de daño, en la misma pena incurrirá el que alterare, destruyere o inutilizare datos, documentos, programas o sistemas informáticos; o vendiere, distribuyere, hiciere circular o introdujere en un sistema informático, cualquier programa destinado a causar daños.

El artículo 184 del Código Penal, que eleva la pena a tres (3) meses a cuatro (4) años de prisión, señala que si mediare cualquiera de las circunstancias siguientes):

Inciso 5: Ejecutarlo en archivos, registros, bibliotecas, museos o en puentes, caminos, paseos u otros bienes de uso público; o en tumbas, signos conmemorativos, monumentos, estatuas, cuadros u otros objetos de arte colocados en edificios o lugares públicos; o en datos, documentos, programas o sistemas informáticos públicos; Inciso 6: Ejecutarlo en sistemas informáticos destinados a la prestación de servicios de salud, de comunicaciones, de provisión o transporte de energía, de medios de transporte u otro servicio público.

Respecto a los delitos contra las comunicaciones, el artículo 197 señala que será reprimido con prisión de seis (6) meses a dos (2) años, el que interrumpiere o entorpeciere la comunicación telegráfica, telefónica o de otra naturaleza o resistiere violentamente el restablecimiento de la comunicación interrumpida.
Delitos contra la administración de justicia

El Artículo 255 establece que será reprimido con prisión de un (1) mes a cuatro (4) años, el que sustrajere, alterare, ocultare, destruyere o inutilizare en todo o en parte objetos destinados a servir de prueba ante la autoridad competente, registros o documentos confiados a la custodia de un funcionario público o de otra persona en el interés del servicio público. Si el autor fuere el mismo depositario, sufrirá además inhabilitación especial por doble tiempo.

Si el hecho se cometiere por imprudencia o negligencia del depositario, éste será reprimido con multa de pesos setecientos cincuenta ($ 750) a pesos doce mil quinientos ($ 12.500).

Delito sobre los Sistemas Informáticos' El 15 de noviembre de 2012, la Fiscalía General de la CABA dictó la Resolución 501/12, a través de la cual, creó como prueba piloto por el término de un año, el Equipo Fiscal Especializado en Delitos y Contravenciones Informáticas, que actúa con competencia única en toda la Ciudad Autónoma de Buenos Aires, con el fin de investigar los delitos informáticos propiamente dichos, y aquellos que se cometen a través de internet que por su complejidad en la investigación o su dificultad en individualizar a los autores, merecen un tratamiento especializado. Existen diferentes delitos informáticos en eucl es objeto el sistema informático, tales como Delito de Daño: La ley 26388 incorpora como segundo párrafo del art. 183 CP "En la misma pena incurrirá el que alterare, destruyere o inutilizare datos, documentos, programas o sistemas informáticos, o vendiere, distribuyere, hiciere circular o introdujere en un sistema informático, cualquier programa destinado a causar daño

En cuanto al delito agravado, la ley 26388 agrega dos nuevas agravantes al art. 184 CP: 5) "ejecutarlo en archivos, registros, bibliotecas, o en datos, documentos, programaso sistemas informáticos públicos"; 6) "ejecutarlo en sistemas informáticos destinados a la prestación de servicios de salud, de comunicaciones, de provisión o transporte de energía, de medios de transporte u otro servicio. público".[6]

[6] http://delitosinformaticos.fiscalias.gob.ar/wp-content/uploads/2014/02/CyberCrime-Informe-Final-2013-flip.pdf

Uruguay

El Estado uruguayo aprobó en el año 2007 la ley Nº 18.237 denominada EXPEDIENTE ELECTRÓNICO cuyo único artículo autoriza el uso de expediente electrónico, de documento electrónico, clave informática simple, firma electrónica, firma digital y domicilio electrónico constituido en todos los procesos judiciales y administrativos que se tramitan ante el Poder Judicial, con idéntica eficacia jurídica y valor probatorio que sus equivalentes convencionales. Se hace referencia a esta ley porque es evidente que será de amplio tratamiento para el caso de los delitos informáticos, puesto que las conductas que autoriza pueden ser objeto de un ciberdelito.

Los delitos informáticos no son de tratamiento específico por la legislación uruguaya, puesto que no existe una ley de ilícitos informáticos (no puede haber delito sin ley previa, estricta y escrita que lo determine - principio de legalidad-), ni tampoco un título específico relativo a los mismos en el Código Penal uruguayo. Se tratará de otorgar una vez más, la participación que al Derecho Penal corresponde dentro del ordenamiento jurídico, como último remedio a las conductas socialmente insoportables, que no pueden ser solucionadas por la aplicación de otro proveimiento jurídico que no se la aplicación de la sanción más gravosa de todo el sistema.

Colombia

En Colombia el 5 de enero de 2009, el Congreso de la República de Colombia promulgó la Ley 1273 “Por medio del cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado –denominado “De la Protección de la información y de los datos”- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones”[7]

Dicha ley tipificó como delitos una serie de conductas relacionadas con el manejo de datos personales, por lo que es de gran importancia que las empresas se blinden jurídicamente para evitar incurrir en alguno de estos tipos penales.

No hay que olvidar que los avances tecnológicos y el empleo de los mismos para apropiarse ilícitamente del patrimonio de terceros a través de clonación de tarjetas bancarias, vulneración y alteración de los sistemas de cómputo para recibir servicios y transferencias electrónicas de fondos mediante manipulación de programas y afectación de los cajeros automáticos, entre otras, son conductas cada vez más usuales en todas partes del mundo. Según estadísticas, durante el 2007 en Colombia las empresas perdieron más de 6.6 billones de pesos a raíz de delitos informáticos.

De ahí la importancia de esta ley, que adiciona al Código Penal colombiano el Título VII BIS denominado "De la Protección de la información y de los datos" que divide en dos capítulos, a saber: “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”.

[7] Ley de protección de la información y de los datos (Colombia)
http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34492

En Colombia existen instituciones de educación como UNICOLOMBIA que promueven capacitaciones en temas relacionados con Delitos Informáticos, el mejor manejo y uso de la prueba digital, establecer altos estándares científicos y éticos para Informáticos Forenses, Llevar a cabo investigación y desarrollo de nuevas tecnologías y los métodos de la ciencia del análisis forense digital e Instruir a los estudiantes en diversos campos específicos sobre nuevas tecnologías aplicadas a la informática Forense, la investigación científica y el proceso tecnológico de las mismas.

España

En *España*, los delitos informáticos son un hecho sancionable por el Código Penal en el que el delincuente utiliza, para su comisión, cualquier medio informático. Estas sanciones se recogen en la Ley Orgánica 10/1995, de 23 de noviembre en el BOE número 281, de 24 de noviembre de 1995. Éstos tienen la misma sanción que sus homólogos no informáticos. Por ejemplo, se aplica la misma sanción para una intromisión en el correo electrónico que para una intromisión en el correo postal.

El Tribunal Supremo emitió una sentencia el 12 de junio de 2007 (recurso Nº 2249/2006; resolución Nº 533/2007) que confirmó las penas de prisión para un caso de estafa electrónica (phishing).

A la hora de proceder a su investigación, debido a que una misma acción puede tener consecuencias en diferentes fueros, comenzará la investigación aquel partido judicial que primero tenga conocimiento de los hechos delictivos cometidos a través de un medio informático, si durante el transcurso de la investagación, se encuentra al autor del delito y pertenece a otro partido judicial, se podrá realizar una acción de inhibición a favor de este último para que continue con la investigación del delito.

México

En *México* los delitos de revelación de secretos y acceso ilícito a sistemas y equipos de informática ya sean que estén protegidos por algún mecanismo de seguridad, se consideren propiedad del Estado o de las instituciones que integran el sistema financiero son hechos sancionables por el Código Penal Federal en el título noveno capítulo I y II.

El artículo 167 fr.VI del Código Penal Federal sanciona con prisión y multa al que intencionalmente o con fines de lucro, interrumpa o interfiera comunicaciones alámbricas, inalámbricas o de fibra óptica, sean telegráficas, telefónicas o satelitales, por medio de las cuales se transmitan señales de audio, de video o de datos.

La reproducción no autorizada de programas informáticos o piratería está regulada en la Ley Federal del Derecho de Autor en el Título IV, capítulo IV.

También existen leyes locales en el código penal del Distrito Federal y el código penal del estado de Sinaloa.

Venezuela

Concibe como bien jurídico la protección de los sistemas informáticos que contienen, procesan, resguardan y transmiten la información. Están contemplados en la Ley Especial contra los Delitos Informáticos, de 30 de octubre de 2001.[8]

La ley tipifica cinco clases de delitos: Contra los sistemas que utilizan tecnologías de información: acceso indebido (Art.6); sabotaje o daño a sistemas (Art.7); favorecimiento culposos del sabotaje o daño. (Art. 8); acceso indebido o sabotaje a sistemas protegidos (Art. 9); posesión de equipos o prestación de servicios de sabotaje (Art. 10); espionaje informático (Art. 11); falsificación de documentos (Art. 12). Contra la propiedad: hurto (Art. 13); fraude (Art. 14); obtención indebida de bienes o servicios (Art. 15); manejo fraudulento de tarjetas inteligentes o instrumentos análogos (Art. 16); apropiación de tarjetas inteligentes o instrumentos análogos (Art. 17); provisión indebida de bienes o servicios (Art. 18); posesión de equipo para falsificaciones (Art. 19). Contra la privacidad de las personas y de las comunicaciones: violación de la privacidad de la data o información de carácter personal (Art. 20); violación de la privacidad de las comunicaciones (Art. 21); revelación indebida de data o información de carácter personal (Art. 22). Contra niños y adolescentes: difusión o exhibición de material pornográfico (Art. 23); exhibición pornográfica de niños o adolescentes (Art. 24). Contra el orden económico: apropiación de propiedad intelectual (Art. 25); oferta engañosa (Art. 26).

Estados Unidos

Este país adoptó en 1994 el Acta Federal de Abuso Computacional que modificó al Acta de Fraude y Abuso Computacional de 1986.

En el mes de julio del año 2000, el Senado y la Cámara de Representantes de este país -tras un año largo de deliberaciones- establece el Acta de Firmas Electrónicas en el Comercio Global y Nacional. La ley sobre la firma digital responde a la necesidad de dar validez a documentos informáticos -mensajes electrónicos y contratos establecidos mediante Internet- entre empresas (para el B2B) y entre empresas y consumidores (para el B2C).

Chile

En Chile el 28 de mayo de 1993, se promulgó la ley 19.223 pero no fue hasta la fecha 7 de junio de 1993 que ésta se publicó. Esta ley, tipifica y sanciona los denominados Delitos Informáticos.[9]

Los delitos tipificados en la Ley 19.223 consideran como un bien jurídico la calidad, la pureza e idoneidad de la información que está contenida en cualquier sistema automatizado de tratamiento de la información. Además, no solo se protege el bien mencionado anteriormente sino que también los siguientes:

a. El patrimonio, en el caso de los fraudes informáticos.

[8] Ley Especial de Delitos Informáticos (Venezuela)
http://web.archive.org/web/20140902120028/http://www.tsj.gov.ve/legislacion/ledi.htm
[9] Delitos Informáticos (Chile)
http://www2.udec.cl/contraloria/docs/materias/delitosinformaticos.pdf

b. La privacidad, intimidad y confidencialidad de los datos, en el caso de espionaje informático.
c. La seguridad y fiabilidad del tráfico jurídico y probatorio, en el caso de falsificaciones de datos probatorios mediante algún sistema o medio informático.
d. El derecho de propiedad sobre la información y sobre los elementos físicos y materiales de un sistema de información, en el caso de los delitos de daños.

6. ANÀLISIS LEGAL EN EL ECUADOR

En cuanto a las políticas públicas para proteger los sistemas informáticos desde el Estado (Codigo Organico Integral Penal – Coip). Nuestra legislación regula penalmente las conductas ilícitas relacionadas con la informática, y es así como en el nuevo Código Orgánico Integral Penal COIP, manifiesta ciertas políticas para la protección de los sistemas informáticos

Los delitos informáticos tipificados en la normativa penal son los siguientes:

A) Art. 202 inciso 1.- Violación de claves o sistemas de seguridad, para acceder u obtener información protegida contenida en sistemas de información

Prisión: Pena específica 6 meses a 1 año; multa de 500 a 1000 dólares.

B) Art. 202.2 Cesión, publicación, utilización o transferencia de datos personales sin autorización

Prisión: Pena específica 2 meses a 2 años; multa de 1000 a 2000 dólares.

C) Art. 262 Destrucción o supresión de documentos o información por empleado público depositario de la misma. Reclusión menor ordinaria: Pena específica 3 a 6 años.

D) Art. 353. 1 Falsificación electrónica Varias

Pena específica: Depende del tipo de falsificación de acuerdo con los artículos 337 al 353

E) Art. 415.1 Destrucción, alteración o supresión de contenidos de sistema informático o red electrónica Prisión: Pena específica 6 meses a 3 años; multa de 60 a 150 dólares

F) Art. 415.2 Destrucción de infraestructuras físicas necesarias para la transmisión, recepción o procesamiento de mensajes de datos Prisión: Pena específica, 8 meses a 4 años; multa de 200 a 600 dólares

G) Art. 553.2 Los que utilizaren fraudulentamente sistemas de información o redes electrónicas, para facilitar la apropiación de un bien ajeno, o los que procuren la transferencia no consentida de bienes, valores o derechos de una persona, en perjuicio de ésta o de un tercero, en beneficio suyo o de otra persona alterando, manipulando o modificando el funcionamiento de redes electrónicas, programas informáticos, sistemas informáticos, telemáticos o mensajes de datos

Prisión: Pena específica, 6 meses a 5 años; multa de 500 a 1000 dólares; los autores podrán ser colocados bajo la vigilancia especial de la autoridad por 2 años a lo menos y 5 a lo más.

Por ser un estudio exploratorio no se puede ser concluyente con los resultados, sin embargo este análisis muestra un panorama empírico de esta temática en el Ecuador que puede servir como referente para un estudio descriptivo o inferencial. Cabe mencionar que es posible desarrollar varios temas que podrían ser utilizados para futuras investigaciones en base a este artículo. El estudio de otros tipos de evidencia digital tales como: documentos de ofimática, imágenes digitales, ficheros de registros de actividad, memoria volátil, entre otros y su relación con el COIP. Además el rango de años y la fuente de información de los casos podrían ampliarse y así evidenciar si la cobertura de artículos es la misma que contempla este paper. Finalmente, se puede categorizar los casos por provincias para brindar un mejor análisis descriptivo general de la pericia informática en el país.[10]

7. CONCLUSIONES Y RECOMENDACIONES

Conclusiones

Los delitos informáticos se han venido desarrollando con el avance de la tecnología y esto hace mucho más complejo poder llegar con los responsable, tanto en estados unidos como en otros de países estos han tenido mucho más auge, teniendo un impacto en los ciudadanos, afectándolos ya sea económicamente trayendo consigo responsabilidades enormes en cuanto se refiere a deudas con las instituciones, pero no solo así muchos de ellas también han tenido que liderar con la crítica social porque algunas intimidades han sido reveladas.

Una misma acción dirigida contra un sistema informático puede aparejar la violación de varias leyes penales, algunos autores expresan que el "uso de la informática no supone más que un modus operandi nuevo que no plantea particularidad alguna respecto de las formas tradicionales de comisión". Una clara dificultad para la persecución de estos ilícitos, ha sido que el ciudadano no considera delincuente al autor de estos delitos, entre los propios victimarios algunas veces existe una reivindicación que subyace a toda su actividad, como es el caso de los hackers, quienes cuentan con todo una "filosofía" preparada para respaldar su actividad afirmando que propenden a un mundo más libre, que disponga de acceso a todas las obras de la inteligencia, y basándose en ese argumento divulgan las claves que tienen en su actividad.

Dado el carácter transnacional de los delitos cometidos mediante el uso de las computadoras, es conveniente establecer tratados de extradición o acuerdos de ayuda mutua entre los países, que permitan fijar mecanismos sincronizados para la puesta en vigor de instrumentos de cooperación internacional para contrarrestar eficazmente la incidencia de la criminalidad informática. Asimismo, la problemática jurídica de los sistemas informáticos debe considerar la tecnología de la información en su conjunto (chips, inteligencia artificial, nanotecnología, redes, etc.), evitando que la norma jurídica quede desfasada del contexto en el cual se debe aplicar.

[10] Estudio cualitativo de la relación de las leyes y la pericia informática en el Ecuador, http://recibe.cucei.udg.mx/revista/es/vol4-no3/computacion01.html

La importancia de contar con contraseñas robustas para acceder a webs y servicios en Internet, instalar y actualizar un buen antivirus, realizar copias de seguridad, la precaución al utilizar herramientas de almacenamiento en la nube para información importante de la organización, hasta el control parental para proteger el uso de los dispositivos entre los menores, para que las empresas y particulares se protejan ante las amenazas de los ciberdelincuentes.

Recomendaciones

No compartir con otras personas la clave de seguridad para acceder a páginas webs para evitar que pueda ser suplantado por otra persona. Aprender a reconocer las páginas seguras, para no caer en trampas. Entrar solo en páginas con https: No hacer caso ni responder a números, ni mails descomidos. No proporcionar datos personas o familiares. Denunciar las páginas que cometan delitos informáticos. Tomar precauciones para acceder a páginas.

8. REFERENCIAS

Acevedo Esparza, P. J. (2010). *Tecnología e Informática*. Ecuador: . Colegio Técnico Industrial José Elias Puyanaarea

Correa, C; Batto, H; Czar de Zalduendo, S. & Nazar Espeche, F. (1987). “El derecho ante el desafío de la informática”. En *Derecho informático*. Buenos Aires: Depalma. ISBN 950 14 0400 5, p. 295.

Cuervo, J. (2008). “Delitos informáticos: Protección penal de la intimidad”. En *Informática Jurídica*. Publicado en http://www.INFORMÁTICA-jurídica.com/trabajos/delitos.asp

Pecoy, M. (2012a). *Delitos informáticos*. Montevideo: Universidad de Montevideo. ISBN 978 9974 8342 4 8.

Tellez, J. (2004). *Derecho Informático*. 3° ed. Mexico: McGraw-Hill.

Correspondencia: Universidad Privada Antonio Guillermo Urrelo. Jr. José Sabogal N° 913, Cajamarca-Perú.

Recibido: 15/10/2015 **Aprobado:** 30/11/2015