Fd-Rie
Formación docente
revista iberoamericana de educación

Proceso de formación en tipificación en el código orgánico integral penal para los delitos cibernéticos

Training process in criminalization in the comprehensive organic criminal code for cybercrime

Processo de treinamento em criminalização no abrangente código criminal orgânico para crimes cibernéticos

Patricia Rodas Soto
Master. Instituto Superior Tecnológico Vicente Rocafuerte, prodas@itsvr.edu.ec , Guayaquil – Ecuador, https://orcid.org/0000-0002-3255-9226

Elizabeth Loor
Master. Instituto Superior Tecnológico Vicente Rocafuerte, eloor@itsvr.edu.ec , Guayaquil, Ecuador, https://orcid.org/0000-0002-5583-7444

Recibido 15 enero 2017 – Aceptado 04 diciembre 2017

Formación docente - revista iberoamericana de educación
http://www.revista-iberoamericana.org/index.php/es/index

e-ISSN: 2737-632X

Vol – 1 No. 1, enero – diciembre 2018
Pags 42 - 79

Resumen. Actualmente las computadoras se utilizan no sólo como equipos de soporte a diferentes diligencias humanas, sino como medio obtener información, a su vez la informática está presente en casi todos los campos de la vida moderna. El presente artículo aborda los delitos informáticos que logran ser considerados como crímenes electrónicos, tan graves que consiguen llegar a ser un genérico problema para el avance de la informática. Estos delitos tienen consigo lo que es fraude, robo, falsificación (documentos), etc. El ejemplo más claro es cuando una persona sea hombre o mujer consigue robar información y causar daños de servidores o computadores que llegan ser la mayoría virtuales para la información está de forma digital cuyo daño cada vez se vuelve más grande. Podemos apreciar, el

análisis de las acciones realizadas por parte de diversos países para regular esta incidencia en las redes digitales y a su vez dar recomendaciones para que los usuarios puedan adoptar para mejorar su experiencia mientras navegan en esta red. En la investigación realizada tenemos como puntos clave el realizar una investigación bibliográfica del arte de los delitos informáticos en el Ecuador, quienes lo hemos comparado con la legislación de otros países en la cual se verá que aún tenemos mucho que cambiar. En las conclusiones dadas están que nuestro debería de reestructurar su Código Orgánico Integral Penal(COIP), y el tener más severas para quienes infrinjan las ley el hurto de información, el desvío de dinero, a quienes se les confía el dinero de los usuario, de lo cual es materia de estudio, que no solo sea investigado y sancionado el representante legal si no también el funcionario bancario que dé o accese a la información de la base de datos de las diferentes instituciones financieras en el Ecuador.

Palabras clave: delitos, Delitos Informáticos, Delitos Cibernéticos y Seguridad Informática.

Abstract. Currently computers are used not only as support teams for different human tasks, but as a means to obtain information, in turn, computer science is present in almost all fields of modern life. This article deals with computer crimes that manage to be considered as electronic crimes, so serious that they manage to become a generic problem for the advancement of computer science. These crimes have what is fraud, theft, falsification (documents), etc. The clearest example is when a person is male or female manages to steal information and cause damage to servers or computers that become the virtual majority for information is digitally whose damage becomes increasingly larger. We can appreciate, the analysis of the actions carried out by different countries to regulate this incidence in the digital

networks and in turn give recommendations so that the users can adopt to improve their experience while they navigate in this network.

Keywords: cimes, Computer Crimes, Cybercrime and Computer Security.

Resumo. Atualmente, os computadores são usados não apenas como equipamento de suporte para diferentes tarefas humanas, mas como um meio de obter informações, por sua vez, a computação está presente em quase todos os campos da vida moderna. Este artigo trata de crimes de computador que conseguem ser considerados crimes eletrônicos, tão graves que se tornam um problema genérico para o avanço da ciência da computação. Esses crimes têm consigo o que é fraude, roubo, falsificação (documentos), etc. O exemplo mais claro é quando uma pessoa é um homem ou uma mulher que rouba informações e causa danos a servidores ou computadores que se tornam a maioria virtual da informação em formato digital, cujo dano se torna cada vez maior. Podemos apreciar a análise das ações realizadas por vários países para regular essa incidência nas redes digitais e, por sua vez, dar recomendações para que os usuários adotem para melhorar sua experiência enquanto navegam nessa rede. Na pesquisa realizada, temos como pontos-chave a realização de uma investigação bibliográfica da arte do crime de computador no Equador, que a comparou com a legislação de outros países, na qual se verá que ainda temos muito a mudar. Nas conclusões apresentadas, devemos reestruturar seu Código Penal Orgânico Abrangente (COIP) e ter mais severidade para quem infringe a lei o roubo de informações, o desvio de dinheiro, a quem é confiado o dinheiro dos usuários, dos quais é uma questão de estudo, que não apenas o representante legal seja investigado e sancionado, mas também o funcionário bancário que fornece ou acessa as informações do banco de dados das diferentes instituições financeiras do Equador.

Palavras-chave: crimes, Crime Eletrônico, Crime Cibernético e Segurança Informática.

INTRODUCCIÓN

La característica más significativa de la informática reside en que la información ha pasado a convertirse en un valor económico de magnitud primera, ya que desde siempre el individuo ha investigado el cómo almacenar información apreciable para usarla después. (Claudio Magliona Markovicth & Macarena López Medel, 1999)

Según lo señalado por (Luis Camacho Losa, 1987), En todos los aspectos de la actividad humana existen las manipulaciones, el ansia de venganza, el engaño, la codicia, el fraude, en definitiva el delito. Infelizmente es algo ineludible al ser humano y así se puede comprobar a lo largo de la historia.

Un delito informático, es la acción antijurídica y culpable, que se da por vías informáticas con el fin de destruir y dañar medios electrónicos, redes de Internet y ordenadores. Debido a que la informática se mueve de manera más rápida que la legislación, en lo cual existen conductas criminales por vías informáticas que no pueden considerarse como delito, según la Teoría Del Delito, define a los abusos informáticos como los tipos penales tradicionales resultan en muchos países inadecuados para encuadrar las nuevas formas delictivas y parte de la criminalidad informática. (Acevedo Esparza, 2010)

La criminalidad informática radica en la actuación de un tipo de actividad que, reuniendo los requisitos que delimitan la noción de delito, sean llevados a cabo manejando un elemento informático (José Cuervo Alvarez, 2014).

Los ciberdelito es toda actividad ilícita que: (a) Tienen por esencia robo de información, contraseñas, fraude a cuentas bancarias, entre otros o (b) Se cometen mediante el uso de computadoras, sistemas informáticos u otros

dispositivos de comunicación. Tapia-León, M., Rivera Villalta, M. D. C., Luján-Mora, S., & Barros Bastidas, C. I. (2017).

Los ciberdelito como lo señala (Julio Téllez Valdés, 2008), son actitudes inversas a los intereses de las personas en que se tiene a las computadoras como instrumento o fin "concepto atípico" / como las conductas antijurídicas, atípicas y culpables en que se tiene a las computadoras como instrumento o fin "concepto típico".

El tema de los bancos y entidades financieras que han interactuado a través de la web, para que sus clientes actúen en el ciberespacio, con las transacciones económicas y lo pequeños negocios, sean estos a gran o pequeña escala, la comunicación global , y son ellos quienes lideran todos los aspectos actúan por medio del ciberespacio, y cada vez son más las transacciones económicas y los negocios a pequeña, mediana y gran escala que se llevan a cabo directamente a través de este medio de comunicación global (Fernando Miró Llinares, 2012), Rodríguez Morales, A., Barros Bastida, C., & Milanés Gómez, R. (2019).

La información es guardada en un pequeño espacio, con la posibilidad recuperación, pero la criminalidad en el área informática posee un mayor alcance como el robo, fraude, chantaje, malversación y falsificación de recursos públicos en los que redes y ordenadores son los medios utilizados. Con el progreso del Internet y la programación, el tema de los delitos informáticos se ha vuelto más sofisticado y frecuente.

Según (Alain Ambrosi, Valérie Peugeot & Daniel Pimienta, 2005) la terminología delito informático se recalcó 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 fin de estudiar los problemas emergentes de criminalidad que eran propiciados por o que migraron a Internet. El Grupo

de Lyón manejó el término para describir, de forma muy aproximada, 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. 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:

- Título 1 - Delitos contra la confidencialidad, integridad y disponibilidad de los datos y sistemas informáticos.
- Título 2 - Delitos relacionados con las computadoras (falsificación y fraude).
- Título 3 - Delitos relacionados con el contenido (pornografía).
- Título 4 - Delitos relacionados con la violación del derecho de autor y los derechos asociados.
- Título 5 - Responsabilidades secundarias y sanciones (cooperación delictiva, responsabilidad empresarial).

Según (Ricardo Levene & Ricardo Levene, 2005) de las conductas delictivas que pueden generar el gran avance tecnológico, sobre todo en el campo de la informática por lo cual se analizara el estudio del arte.

Delito Informático involucra acciones criminales que un primer momento los países han tratado de incluir en figuras típicas de carácter tradicional, tales como hurto, sabotaje, falsificaciones, fraudes, estafa, perjuicios, robo, etc., sin embargo, se debe recalcar que el uso ilícito de las computadoras es lo que ha propiciado la necesidad de regulación por parte del derecho.

Universalmente se considera que el delito Informático no posee una definición exacta, sin embargo muchos han sido las energías de peritos que se han ocupado del tema, y aun cuando no existe un concepto con carácter universal, se han expresado nociones funcionales atendiendo a realidades nacionales concretas.

Según Carlos Sarzana, en su obra criminalitá e tecnología, los crímenes por computadora alcanzan cualquier comportamiento criminógeno en el cual la computadora ha estado involucrada como material o como objeto de la acción criminogena, o como mero símbolo.

Según Nidia Callegari define al delito informático como aquel que se da con la ayuda de la informática o de técnicas anexas.

Según Rafael Fernández precisa el delito Informático como la realización de una acción que, reuniendo las características que delimitan el concepto de delito, se ha llevado a cabo utilizando en elemento informático o telemático contra los derechos y libertades de los ciudadanos definidos en el título 1 de la Constitución Española.

Según 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"

Según Julio Tellez referencia al delito informático en forma atípica y típica, pensando por la primeras actitudes ilícitas en que se tienen a las computadoras como instrumento o fin y por las segundas conductas típicas, antijurídicas y culpables en que se tienen a las computadoras como instrumento o fin.

Se han expresado diversas denominaciones para indicar las conductas ilícitas en las que se usa a la computadora, tales como delitos electrónicos, delitos informáticos, delitos relacionados con la computadora, delincuencia relacionada con el ordenador y crímenes por computadora", delincuencia relacionada con el ordenador.

Según Julio Tellez clasifica a los delitos informáticos en base a dos criterios como fin u objetivo o instrumento o medio.

- Como instrumento o medio: Se tienen a las conductas criminógenas que se valen de las computadoras como método, medio, o símbolo en la comisión del ilícito.
- Como fin u objetivo: En ésta categoría se enmarcan las conductas criminógenas que van dirigidas en contra de la computadora, accesorios o programas como entidad física.
    - Los que utilizan la tecnología electrónica como método (conductas criminógenas en donde los individuos utilizan métodos electrónicos para llegar a un resultado ilícito).
    - Los que utilizan la tecnología electrónica como medio (conductas criminógenas en donde para realizar un delito utilizan una computadora como medio o símbolo).
    - Los que utilizan la tecnología electrónica como fin (conductas criminógenas dirigidas contra la entidad física del objeto o máquina electrónica o su material con objeto de dañarla).

Según Julio Valdes y María Luz Lima entre otros especialistas sustentan que las personas que realizan los delitos informáticos, son aquellas que poseen ciertas características que no presentan el denominador común de los delincuentes, esto es, los sujetos activos tienen habilidades para el manejo de los sistemas informáticos y generalmente por su situación laboral se encuentran en lugares estratégicos donde se maneja información de carácter sensible, o bien son hábiles en el uso de los sistemas informatizados, aun cuando en muchos de los casos, no desarrollen actividades laborales que faciliten la comisión de este tipo de delitos.

Con el tiempo se ha logrado evidenciar que los autores de los delitos informáticos son muy varios y que lo que los diferencia entre sí es la naturaleza de los delitos cometidos. De esta forma, la persona que entra en un sistema informático sin intenciones delictivas es muy diferente del empleado de una institución financiera que desvía fondos de las cuentas de sus clientes.

El nivel típico de aptitudes del delincuente informático es argumento de discusión ya que para algunos dicho nivel no es indicador de delincuencia informática en tanto que otros aducen que los posibles delincuentes informáticos son personas decididas, listas, motivadas y dispuestas a aceptar un reto tecnológico, características que pudieran encontrarse en un empleado del sector de procesamiento de datos. Barros-Bastidas, C., & Turpo, O. (2020).

Sin embargo, teniendo en cuenta las características ya mencionadas de las personas que cometen los delitos informáticos, estudiosos en la materia los han catalogado como delitos de cuello blanco término introducido por primera vez por el criminólogo norteamericano Edwin Sutherland en el año 1943.

Efectivamente, este popular criminólogo marca un sin número de conductas que considera como delitos de cuello blanco, aun cuando muchas de estas conductas no están tipificadas en los ordenamientos jurídicos como delitos, y

dentro de las cuales cabe destacar las violaciones a las leyes de patentes y fábrica de derechos de autor, el contrabando en las empresas, el mercado negro, las quiebras fraudulentas, la evasión de impuestos, corrupción de altos funcionarios, entre otros.

Por lo cual este criminólogo estadounidense dice que tanto la conceptualización de los delitos informáticos como la de los delitos de cuello blanco no es de acuerdo al interés protegido, Barros Bastidas, C., & Turpo Gebera, O. (2018),

como sucede en los delitos convencionales sino de acuerdo al sujeto activo que los comete. Entre las características en común que poseen ambos delitos tenemos que: el sujeto activo del delito es una persona de cierto status socioeconómico, ni por carencia de recreación, su comisión no puede explicarse por pobreza ni por mala habitación, ni por baja educación, ni por inestabilidad emocional, ni por poca inteligencia.

Con lo que es difícil elaborar estadísticas sobre ambos tipos de delitos. La cifra negra es muy alta; no es fácil descubrirlo y sancionarlo, en razón del poder económico de quienes los cometen, pero los daños económicos son altísimos; existe una gran indiferencia de la opinión pública sobre los daños ocasionados a la sociedad; ésta no considera delincuentes a los sujetos que cometen este tipo de delitos, no los segrega, no los desprecia, ni los desvaloriza, por el contrario, el autor o autores de este tipo de delitos se considera a sí mismos respetables. Otra coincidencia que tienen estos tipos de delitos es que, generalmente, son objeto de medidas o sanciones de carácter administrativo y no privativo de la libertad.

En primera instancia tenemos que distinguir que el sujeto pasivo o víctima del delito es el ente sobre el cual reitera la conducta de acción u omisión que realiza el sujeto activo, y en el caso de los delitos informáticos, mediante él podemos conocer los diferentes ilícitos que cometen los delincuentes

informáticos, que generalmente son descubiertos casuísticamente debido al desconocimiento del modus operandi.

Ha sido improbable estar al tanto sobre la verdadera magnitud de los delitos informáticos ya que la mayor parte de los delitos no son denunciados o no son descubiertos a las autoridades responsables; que sumado al temor de las empresas de denunciar este tipo de ilícitos por el desprestigio y su consecuente pérdida económica que esto pudiera ocasionar, hace que éste tipo de conductas se mantenga bajo la llamada cifra negra o cifra oculta.

La ley 111 de Patentes de Invención regula la protección a la propiedad intelectual, la ley Penal 11723 de "La propiedad Científica, literaria y artística" ha modificado los artículos 71, 72, 72 bis, 73 y 74.

El artículo 71 tipifica como conducta ilícita al que de cualquier manera y en cualquier forma defraudare los derechos de propiedad intelectual que reconoce esta ley. El Art. 72 considera casos especiales de defraudación:

a. El que edite, venda o reproduzca por cualquier medio o instrumento, una obra inédita o publicada sin autorización de su autor o derecho-habientes.
b. El que falsifique obras intelectuales, entendiéndose como tal la edición de una obra ya editada, ostentando falsamente el nombre del editor autorizado al efecto.
c. El que edite, venda o reproduzca una obra suprimiendo o cambiando el nombre del autor, el título de la misma o alterando dolosamente su texto.

El Art. 72 bis

a. El que con fin de lucro reproduzca un fonograma sin autorización por escrito de su productor o del licenciado del productor;
b. El que con el mismo fin facilite la reproducción ilícita mediante el alquiler de discos fonográficos u otros soportes materiales;

c. El que reproduzca copias no autorizadas por encargo de terceros mediante un precio.
d. El que almacene o exhiba copias ilícitas y no pueda acreditar su origen mediante la factura que lo vincule comercialmente con el productor legítimo;
e. El que importe las copias ilegales con miras a distribución al público.

El decreto 165/94 (B.O. del 8/2/94) incluyó al software dentro de la Ley de Propiedad Intelectual 11723. También dentro del Código Penal encontraremos sanciones respecto de los delitos contra el honor (109 a 117); Instigación a cometer delito (209), instigación al suicidio (83); estafas (172), además de los de defraudación, falsificación, tráfico de menores, narcortráfico, etc., todas conductas que pueden ser cometidas utilizando como medio la tecnología electrónica

En este sentido habrá que recurrir a aquellos tratados internacionales, que nuestro país es parte y que, en virtud del artículo 75 inc. 22 de la Constitución Nacional reformada en 1994, tienen rango constitucional.

En los últimos años se ha perfilado en el ámbito internacional un cierto consenso en las valoraciones político-jurídicas de los problemas derivados del mal uso que se hace de las computadoras, lo cual ha dado lugar a que, en algunos casos, se modifiquen los derechos penales nacionales.

El GATT, se transformó en lo que hoy conocemos como la Organización Mundial de Comercio (OMC), por consecuencia todos los acuerdos que se suscribieron en el marco del GATT, siguen estando vigentes.

En este sentido Argentina es parte del acuerdo que se celebró en el marco de la Ronda Uruguay del Acuerdo General de Aranceles Aduaneros y Comercio, que en su artículo 10 relativo a los programas de ordenador y compilaciones de datos, se establece que este tipo de programas, ya sean fuente u objeto, serán protegidos como obras literarias de conformidad con el Convenio de

Berna de 1971 para la Protección de Obras Literarias y Artísticas, y que las compilaciones de datos posibles de ser legibles serán protegidos como creaciones de carácter intelectual.

En el Artículo 61 se establece que para los casos de falsificación dolosa de marcas de fábrica o de comercio o de piratería lesiva del derecho de autor a escala comercial se establecerán procedimientos y sanciones penales además de que, los recursos disponibles comprenderán la pena de prisión y/o la imposición de sanciones pecuniarias suficientemente disuasorias.

El convenio de Berna fue ratificado en nuestro país por la Ley 22195 el 17/3/80, La convención sobre la Propiedad Intelectual de Estocolmo, fue ratificada por la ley 22.195 del 8/7/1990, la Convención para la Protección y Producción de Phonogramas de 1971, fue ratificada por la ley 19.963 el 23/11/1972, la Convención Relativa a la Distribución de Programas y Señales, fue ratificada por la ley 24425 el 23/12/1994.

En 1983 la Organización de Cooperación y Desarrollo Económico (OCDE) inició un estudio de la posibilidad de aplicar y armonizar en el plano internacional las leyes penales, a fin de luchar contra el problema del uso indebido de los programas de computación.

Las posibles implicaciones económicas de la delincuencia informática tienen carácter internacional e incluso transnacional, cuyo principal problema es la falta de una legislación unificada que, facilita la comisión de los delitos.

En 1986 la OCDE público un informe titulado Delitos de informática: análisis de la normativa jurídica, donde se reseñaban las normas legislativas vigentes y las propuestas de reforma en diversos Estados miembros y se recomendaba una lista mínima de ejemplos de uso indebido que los países podrían prohibir y sancionar en leyes penales.

En 1992 elaboró un conjunto de normas para la seguridad de los sistemas de información, con intención de ofrecer las bases para que los Estados y el

sector privado pudieran erigir un marco de seguridad para los sistemas informáticos.

En 1990 la Organización de las Naciones Unidas (ONU) en el Octavo Congreso sobre Prevención del Delito y Justicia Penal, celebrado en La Habana, Cuba, se dijo que la delincuencia relacionada con la informática era consecuencia del mayor empleo del proceso de datos en las economías y burocracias de los distintos países y que por ello se había difundido la comisión de actos delictivos.

La ONU ha publicado una descripción de Tipos De Delitos Informáticos, que se transcribe al final ésta sección. En 1992 La Asociación Internacional de Derecho Penal durante el coloquio celebrado en Wurzburgo en 1992, adoptó diversas recomendaciones respecto a los delitos informáticos, entre ellas que, en la medida que el derecho Penal no sea suficiente, deberá promoverse la modificación de la definición de los delitos existentes o la creación de otros nuevos, si no basta con la adopción de otras medidas como por ejemplo el principio de subsidiariedad.

Hay otros Convenios no ratificados aún por nuestro País, realizados por la Organización Mundial de la Propiedad Intelectual (OMPI), de la que nuestro país es parte integrante a partir del 8/10/1980.

En Noviembre de 1997 se realizaron las II Jornadas Internacionales sobre el Delito Cibernético en Mérida España, donde se desarrollaron temas tales como:

- Aplicaciones en la Administración de las Tecnologías Informáticas / cibernéticas.
- Blanqueo de capitales, contrabando y narcotráfico.
- Hacia una policía Europea en la persecución del delito Cibernético.
- Internet: a la búsqueda de un entorno seguro.
- Marco legal y Deontológico de la Informática.

Este tipo de fraude informático conocido también como sustracción de datos, representa el delito Informático más común ya que es fácil de cometer y difícil de descubrir. Este delito no requiere de conocimientos técnicos de informática y puede realizarlo cualquier persona que tenga acceso a las funciones normales de procesamiento de datos en la fase de adquisición de los mismos. Es muy difícil de descubrir y a menudo pasa inadvertida debido a que el delincuente debe tener conocimientos técnicos concretos de informática. Este delito consiste en modificar los programas existentes en el sistema de computadoras o en insertar nuevos programas o nuevas rutinas. Un método común utilizado por las personas que tienen conocimientos especializados en programación informática es el denominado Caballo de Troya, que consiste en insertar instrucciones de computadora de forma encubierta en un programa informático para que pueda realizar una función no autorizada al mismo tiempo que su función normal.

Se efectúa fijando un objetivo al funcionamiento del sistema informático. El ejemplo más común es el fraude de que se hace objeto a los cajeros automáticos mediante la falsificación de instrucciones para la computadora en la fase de adquisición de datos. Tradicionalmente esos fraudes se hacían a partir de tarjetas bancarias robadas, sin embargo, en la actualidad se usan ampliamente equipos y programas de computadora especializados para codificar información electrónica falsificada en las bandas magnéticas de las tarjetas bancarias y de las tarjetas de crédito.

Aprovecha las repeticiones automáticas de los procesos de cómputo. Es una técnica especializada que se denomina "técnica del salchichón" en la que "rodajas muy finas" apenas perceptibles de transacciones financieras, se van sacando repetidamente de una cuenta y se transfieren a otra.

Las computadoras pueden utilizarse también pare efectuar falsificaciones de documentos de uso comercial. Cuando empezó a disponerse de

fotocopiadoras computarizadas en color a base de rayos láser surgió una nueva generación de falsificaciones o alteraciones fraudulentas. Estas fotocopiadoras pueden hacer copias de alta resolución, pueden modificar documentos e incluso pueden crear documentos falsos sin tener que recurrir a un original, y los documentos que producen son de tal calidad que solo un experto puede diferenciarlos de los documentos auténticos.

Es el acto de borrar, suprimir o modificar sin autorización funciones o datos de computadora con intención de obstaculizar el funcionamiento normal del sistema. Las técnicas que permiten cometer sabotajes informáticos son:

Es una serie de claves programáticas que pueden adherirse a los programas legítimos y propagarse a otros programas informáticos. Un virus puede ingresar en un sistema por conducto de una pieza legitima de soporte lógico que ha quedado infectada, así como utilizando el método del Caballo de Troya.

Se fabrica de forma análoga al virus con miras a infiltrarlo en programas legítimos de procesamiento de datos o para modificar o destruir los datos, pero es diferente del virus porque no puede regenerarse. En términos médicos podría decirse que un gusano es un tumor benigno, mientras que el virus es un tumor maligno. Ahora bien, las consecuencias del ataque de un gusano pueden ser tan graves como las del ataque de un virus: por ejemplo, un programa gusano que subsiguientemente se destruirá puede dar instrucciones a un sistema informático de un banco pare que transfiera continuamente dinero a una cuenta ilícita.

Exige conocimientos especializados ya que requiere la programación de la destrucción o modificación de datos en un momento dado del futuro. Ahora bien, al revés de los virus o los gusanos, las bombas lógicas son difíciles de detectar antes de que exploten; por eso, de todos los dispositivos informáticos criminales, las bombas lógicas son las que poseen el máximo potencial de

daño. Su detonación puede programarse para que cause el máximo de daño y para que tenga lugar mucho tiempo después de que se haya marchado el delincuente. La bomba lógica puede utilizarse también como instrumento de extorsión y se puede pedir un rescate a cambio de dar a conocer el lugar en donde se halla la bomba.

Por motivos diversos: desde la simple curiosidad, como en el caso de muchos piratas informáticos (Hacker) hasta el sabotaje o espionaje informático. Piratas informáticos o Hackers El acceso se efectúa a menudo desde un lugar exterior, situado en la red de telecomunicaciones, recurriendo a uno de los diversos medios que se mencionan a continuación. El delincuente puede aprovechar la falta de rigor de las medidas de seguridad para obtener acceso o puede descubrir deficiencias en las medidas vigentes de seguridad o en los procedimientos del sistema. A menudo, los piratas informáticos se hacen pasar por usuarios legítimos del sistema, esto suele suceder con frecuencia en los sistemas en los que los usuarios pueden emplear contraseñas comunes o contraseñas de mantenimiento que están en el propio sistema.

Esta puede entrañar una pérdida económica sustancial para los propietarios legítimos. Algunas jurisdicciones han tipificado como delito esta clase de actividad y la han sometido a sanciones penales. El problema ha alcanzado dimensiones transnacionales con el tráfico de esas reproducciones no autorizadas a través de las redes de telecomunicaciones modernas. Al respecto, consideramos, que la reproducción no autorizada de programas informáticos no es un delito informático debido a que el bien jurídico a tutelar es la propiedad intelectual.

MATERIALES Y MÉTODOS

Para los recursos fundamentales que se consiguieron alcanzar para el desarrollo del presente trabajo investigativo han sido formados mediante dos

partes, la primera con cierta cantidad de material impreso tales como investigaciones científicas/académicas de tercer/cuarto nivel de educación y libros, en cuanto la segunda parte es mediante una laptop dotada de acceso a internet, por medio del cual se accedió a distintas plataformas de sitio web (fuentes de información digital) sean estas base de datos nacionales/extranjeras, tanto de carácter formal como particular.

La metodología que se llevar es una investigación documental, tomando como base lo explicado por (Daniel Behar Rivero, 2008), se apoya en fuentes de carácter documental, esto es, en documentos de cualquier especie. Es transcendental reiterar que en el presente trabajo de investigación se ha examinado un conjunto de documentos informativos, que en lo sucesivo fueron sometidos a una minuciosa lectura y revisión a fines de poder inferir para así poder fundar un esbozo de desarrollo, basado en la conceptualización y descripción concerniente a delitos cibernéticos.

La realización de este trabajo, tras haber escogido el material consultado, está muy bien asociada con la idea de una investigación a nivel descriptivo, y mencionando nuevamente a la obra de (Daniel Behar Rivero, 2008) sirve para analizar cómo es y cómo se manifiesta un fenómeno y sus componentes donde permitirá detallar el fenómeno estudiado básicamente a través de la medición de uno o más de sus atributos.

Asociado a esto la investigación a nivel exploratorio al que se ha previsto limitar, se puede hacer mención a lo definido por (Roberto Hernández Sampieri, Carlos Fernández Collado & María del Pilar Baptista Lucio, 2010), quien establece en su obra que se habla de estudios exploratorios cuando la investigación, se realizan cuando el objetivo es examinar un tema o problema de investigación poco estudiado, del cual se tienen muchas dudas o no se ha abordado antes. Los mismos autores indican que este estudio sirve para preparar el terreno y por lo común anteceden a investigaciones con alcances

descriptivos y que la relación con el objeto de estudio puede hacerse por diversas vías tales como observación directa o indirecta y por medio del análisis preliminar de documentos diversos que traten sobre la temática.

Hasta este punto se ha referido con respecto a la metodología, donde consideramos que es suficiente y que aplica para fundamentar lo afirmado en el resumen aportado.

Es de suma importancia insistir que el acceso a la información digital se efectuó a través de los motores de búsqueda de Google, Google Académico y Scielo. La investigación de dicha información se hizo de manera independiente y casual, teniendo como criterio el vínculo sobre el robo de información como parte de la criminalidad informática, alcanzando a seleccionar del total del material consultado y disponible, sólo el contenido que desde nuestro punto de vista, resultó ser más relevante y adecuado.

Investigación exploratoria en bases de datos de delitos informáticos de diferentes áreas y países. Se desarrolla a partir de esta exploración un análisis culitativo de los mismos.

Para esta investigación, se han hecho uso de métodos cuantitativos mediante una plataforma en internet llamada: Encuestas de Google. (Google Formularios, 2018). Por medio de esta herramienta se entrevisto a 400 personas, la misma que se estableció como tamaño de muestra; debido a que, si mayor es la observación, menos es el error a la hora de la veracidad del artículo científico.

Se ahorró tiempo puesto que el entrevistado sólo tuve que leer las preguntas y responderlas en la plataforma. Aquello se ejecutó a 200 personas, mientras que por otro lado, se realizó 200 encuestas personalmente (en la ciudad de Guayaquil específicamente en la Avenida 9 de octubre) es decir una muestra simple aleatoria (donde cada persona sea hombre o mujer pudo ser seleccionada para entrevistarla al azar).

Esta plataforma, otorgó el número de observaciones representado de manera porcentual e ilustró los datos en barras de Excel, logrando que se pueda obtener una mejor apreciación de los resultados.

Adicionalmente, se reviso el estado del arte de diversos artículos publicados por varias personas, páginas web, libros de autores relacionados con la presente investigación y la investigación de campo.

RESULTADOS

Según (FGE, 2015), 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: clonación de tarjetas de crédito, fraude, falsificaciones, espionaje, suplantación de identidad, robo, 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.

El mismo fiscal dijo que 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.

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.

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.

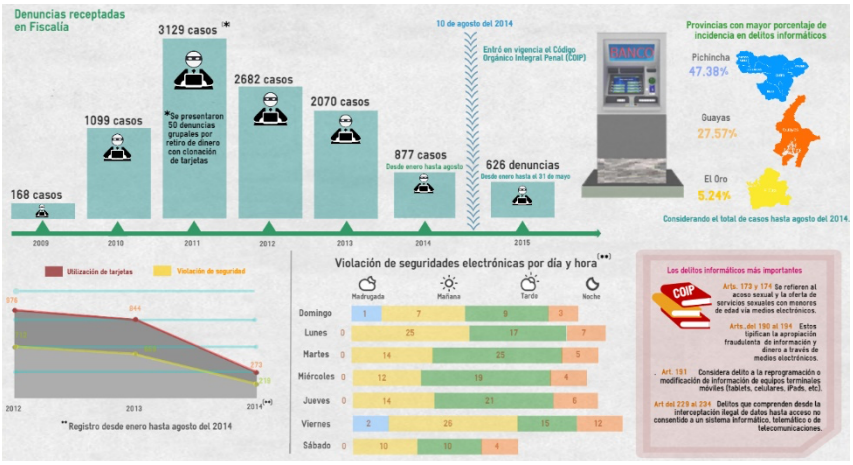

Figura 1. Los Delitos Informáticos. Fuente. (FGE, 2015)

Para el Análisis Legal basado a la regulación por países según el estudio de (Carlos Alcívar Trejo, Gustavo Domenech Alvarez & Karla Ortìz Chimbo, 2015) tenemos:

Argentina

Conforme a la ley vigente (Ministerio de Justicia y Derechos Humanos Presidencia de la Nación, 2008), 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).

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

Para (MPF, 2014), 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, programas o 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.

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

Según (Alcaldía Mayor de Bogotá, 2009), 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.

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.

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 investigación, 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 continúe 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

Según (Asamblea Nacional, 2014), 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.

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

Según (Ministerio de Justicia, 1993) 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.

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.
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.

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.

La acotación de (Francisco Bolaños Burgos & Cristopher Gómez Giacoman, 2015) es muy válida y se concuerda que 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.

CONCLUSIONES

La aproximación a un temática de gran preocupación y sobre todo de mucho interés, se puede marcar que dado el carácter transnacional de las infracciones realizados mediante el uso de las computadoras, es provechoso instituir acuerdos o tratados de extradición para entre los países para mutua para contrarrestar fervorosamente los sucesos de la criminalidad informática.

Los delitos informáticos han evolucionado con el adelanto de la tecnología y esto hace mucho más complejo poder llegar con los responsables, ya sea en cualquier país, obteniendo un impacto en los ciudadanos, económicamente trasladando consigo responsabilidades con las instituciones a manera de deudas. La importancia de contar con contraseñas seguras, un buen antivirus para acceder a diversos sitios webs, a más de utilizar herramientas de almacenamiento con son las nubes y así proteger las amenazas de ciber delincuentes.

El no compartir claves personales, de seguridad o cualquier clave que involucre información valiosa con otro tercero u personas para evitar suplantación de datos por otras personas de esta misma manera aprender a reconocer las páginas seguras.

Navegar en páginas con https para no responder mails descomidos y ni responder a números, además de no proporcionar datos personas o familiares y por ultimo denunciar aquellas páginas que cometan estos delitos informáticos.

REFERENCIAS

Acevedo Esparza. (2010). Tecnología e Informática. Ecuador: Colegio Técnico Industrial José Elias Puyana.

Alain Ambrosi, Valérie Peugeot & Daniel Pimienta. (2005). Enfoques Multiculturales sobre las Sociedades de la Información. Francia: C&F.

Alcaldía Mayor de Bogotá. (05 de 01 de 2009). Régimen Legal De Bogotá D.C. Obtenido de Ley 1273 de 2009 Nivel Nacional: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34492

Asamblea Nacional. (02 de 09 de 2014). LA ASAMBLEA NACIONAL DE LA REPÚBLICA BOLIVARIANA DE VENEZUELA. Obtenido de Ley Especial Contra los Delitos Informáticos: http://web.archive.org/web/20140902120028/http://www.tsj.gov.ve/legislacion/ledi.htm

Barros-Bastidas, C., & Turpo, O. (2020). La formación en investigación y su incidencia en la producción científica del profesorado de educa- ción de una universidad pública de Ecuador. *Publicaciones, 50*(2), 167–185. doi:10.30827/publicaciones.v50i2.13952

Barros Bastidas, C., & Turpo Gebera, O. (2018). Factors influencing the scientific production of university professors: a systematic review . *Pensamiento Americano*, *11*(22). https://doi.org/10.21803/pensam.v11i21-1.276

Carlos Alcívar Trejo, Gustavo Domenech Alvarez & Karla Ortìz Chimbo. (2015). LA SEGURIDAD JURÍDICA FRENTE A LOS DELITOS INFORMÁTICOS. Revista de Investigación Jurídica, 48 - 55.

Claudio Magliona Markovicth & Macarena López Medel. (1999). Delincuencia y Fraude Informático. Santiago de Chile: Jurídica de Chile.

Daniel Behar Rivero. (2008). Metodología de la Investigación. Argentina: Shalom.

Fernando Miró Llinares. (2012). El cibercrimen. Madrid: Marcus Felson.

FGE. (13 de 06 de 2015). Fiscalía General del Estado Ecuador. Obtenido de Los delitos informáticos van desde el fraude hasta el espionaje: https://www.fiscalia.gob.ec/los-delitos-informaticos-van-desde-el-fraude-hasta-el-espionaje/

Francisco Bolaños Burgos & Cristopher Gómez Giacoman. (2015). Estudio cualitativo de la relación de las leyes y la pericia informática en el Ecuador. Recibe, 26-27.

José Cuervo Alvarez. (01 de 01 de 2014). Informática Jurídica. Obtenido de Delitos informáticos: Protección Penal de la Intimidad: http://www.informatica-juridica.com/trabajos/delitos-informaticos-proteccion-penal-de-la-intimidad/

Julio Téllez Valdés. (2008). Derecho informático. México: McGraw-Hill.

Luis Camacho Losa. (1987). El Delito Informático. Madrid: L. Camacho.

Ministerio de Justicia. (07 de 06 de 1993). Biblioteca del Congreso Nacional de Chile / BCN. Obtenido de Delitos Informáticos; Sistemas de Información; Ley no. 19.223: https://www.leychile.cl/Navegar?idNorma=30590

Ministerio de Justicia y Derechos Humanos Presidencia de la Nación. (04 de 06 de 2008). InfoLEG. Obtenido de CODIGO PENAL: http://servicios.infoleg.gob.ar/infolegInternet/anexos/140000-144999/141790/norma.htm

MPF. (02 de 2014). Ministerio Publico Fiscal de la Ciudad Autonoma de Buenos Aires. Obtenido de Delitos informaticos: http://delitosinformaticos.fiscalias.gob.ar/wp-content/uploads/2014/02/CyberCrime-Informe-

Ricardo Levene & Ricardo Levene. (24 de 11 de 2005). DerechoEcuador. Obtenido de Delitos Informáticos: https://www.derechoecuador.com/delitos-informaticos

Roberto Hernández Sampieri, Carlos Fernández Collado & María del Pilar Baptista Lucio. (2010). METODOLOGÍA de la investigación. México: McGraw-Hill.

Rodríguez Morales, A., Barros Bastida, C., & Milanés Gómez, R. (2019). Profesionalización docente y formación desde un nuevo currículo en la Universidad de Guayaquil. *Revista Universidad y Sociedad*, *11*(1), 243-248.

Tapia-León, M., Rivera Villalta, M. D. C., Luján-Mora, S., & Barros Bastidas, C. I. (2017). Análisis de la calidad de los resúmenes de tesis de grado de las universidades del Ecuador respecto a normas internacionales.

von Feigenblatt, Otto Federico, A Socio-Cultural Analysis of Romantic Love in Japanese Harem Animation: A Buddhist Monk, a Japanese Knight, and a Samurai (September 16, 2010). Journal of Asia Pacific Studies, Vol. 1, No. 3, pp. 636-646, 2010, Available at SSRN: https://ssrn.com/abstract=1760643

von Feigenblatt, Otto Federico, Costa Rica's Foreign Policy: Can 'Right' Become 'Might'? (November 27, 2008). Journal of Alternative Perspectives in the Social Sciences, Vol. 1, No. 1, pp. 11-15, 2008, Available at SSRN: https://ssrn.com/abstract=1308245

von Feigenblatt, Otto Federico, Human Security and the Responsibility to Protect: A Holistic Approach to Dealing with Violent Conflict in Southeast Asia (May 13, 2009). Journal of Social Sciences, Vol. 11, No. 1, pp. 27-40, 2009, Available at SSRN: https://ssrn.com/abstract=1570171