Debate Jurídico Ecuador. Revista digital de Ciencias Jurídicas de UNIANDES
Vol. 1 / Nro. 1 / septiembre-diciembre / Año. 2018 / pp. 3-14

ARTÍCULO DE REVISIÓN
CIENCIAS JURÍDICAS

EL DELITO INFORMÁTICO EN AMÉRICA

CYBERCRIME IN AMERICA

Narváez Montenegro, Bolívar David [I]; Recalde Machado, Gabriel Estefanía [II].

I. david_narvaez@outlook.es, Facultad de Jurisprudencia, Carrera de Derecho, Universidad Regional Autónoma de los Andes, Ambato, Ecuador.
II. stefania_20@outlook.com Facultad de Jurisprudencia, Carrera de Derecho, Universidad Regional Autónoma de los Andes, Ambato, Ecuador.

Recibido: 12/05/2018
Aprobado: 15/07/2018

RESUMEN

El ciberdelito, al igual que otras figuras penales, ha sido objeto de análisis por parte de juristas y expertos en seguridad informática de todo el mundo; lo que permitió que muchas legislaciones del continente americano tipifiquen conductas ciber-delictuales, tomando en consideración lo que se ha analizado doctrinalmente y tipificado en otros continentes. Sin embargo, no ha existido un estudio adecuado sobre la realidad del delito informático en el continente americano que haya permitido identificar los imperfectos jurídicos respecto a ciertas ciber-conductas que deben ser consideradas y sancionadas como figuras penales independientes, lo que llevó a la necesidad de efectuar una investigación que identifique los delitos informáticos tipificados en países que más avances presentan sobre el tema, y, en base a ello, se estableció las falencias y/o vacíos presentes en las legislaciones del continente americano. Este trabajo de investigación se fundamentó en publicaciones nacidas en la Academia y del análisis que al respecto efectuaron los autores, aplicando métodos teóricos y empíricos que, conjugados con la técnica de la entrevista y la encuesta, concluyó en una propuesta viable y novedosa. De esta forma se detalló las conductas criminales ejecutadas con herramientas informáticas que constan en la legislación americana; y una vez identificadas se detectó las falencias existentes y se proporcionó una posible solución en base a la tipificación de ciertas ciber-conductas que no constan como figuras penales independientes en los cuerpos jurídico-penales de América, y que en muchas ocasiones son sancionadas acoplándolas a figuras penales tradicionales que contienen una pena no proporcional con el daño causado.

PALABRAS CLAVE: Informática; delito, derecho, ley, convenio.

ABSTRACT

Computer crime, like other criminal offenses, has been analyzed by lawyers and security experts from America and the world; what has allowed many laws of this continent criminalize behaviors cybercriminals taking into consideration what is typified in other continents and based on the study on the subject have made the experts. However, there is no adequate study of the reality of computer crime in the Americas, leading to the need for a job that identifies each cybercrime established in countries that have more progress on the issue, and, on this basis, to identify gaps that occur on the mainland; allowing propose certain computer crimes that have not been subjected to proper analysis by the legislature. This research will be based on works born in the Academy and the analysis performed thereon to the author. Thus, the reader is offered a detail of criminal behavior performed with tools contained in the American legislation; and based on that detect the flaws and provide a possible solution.

KEYWORDS: computer; crime; right; law; convention

INTRODUCCIÓN

El presente trabajo de investigación científica contiene una visión absolutamente nueva respecto a la identificación de las falencias en la legislación americana en cuanto a los delitos informáticos, tomando como base lo tipificado en legislaciones de mayor avanzada que la nuestra y criterios doctrinales.

La identificación de ciber-conductas que a criterio de los autores deben ser consideradas en la legislación americana, resulta necesaria por el aparecimiento de nuevas herramientas tecnológicas que lleva a los Estados a tipificar conductas delictuales no contempladas en su ordenamiento jurídico penal. Se realizó esfuerzos por abarcar todas las formas posibles de conductas que vulneren derechos, y para las cuales la normativa penal no ofrece un marco óptimo y completo que las tipifique y sancione. Esto ha llevado a que expertos en seguridad informática y profesionales del Derecho, efectúen análisis que han arrojan nuevas clasificaciones de delitos informáticos, así como las formas de prevenir y combatir los mismos. Mediante un estudio exhaustivo se ha logrado identificar los comportamientos ciber-delictuales que se cometen en el mundo y que son tipificadas y sancionadas en legislaciones, que han abordado el tema con seriedad a través de trabajos de investigación científica en el que han confluido conocimientos informáticos y jurídicos. Lo referido permitió que el trabajo de investigación identifique las falencias existentes en el ordenamiento jurídico ecuatoriano.
Sin embargo, de que el Código Orgánico Integral Penal tipifica el delito informático, no incluye todas las conductas criminales ejecutadas con herramientas informáticas (COIP, 2014). Efectivamente, la norma jurídica actual no considera ciertas conductas informático-criminales;

dejando a los jueces la complicada tarea de acoplarlas a figuras penales tradicionales. De esta manera se pretende estructurar un marco de falencias de conductas cibercriminales producto del trabajo de investigación desarrollado en el seno de la Academia, que prevengan la afectación de derechos e intereses de terceros en el continente americano, y en base a ello el legislador pueda establecer las sanciones adecuadas a las mismas.

No obstante, para entender el contexto jurídico del delito informático, es preciso conocer la definición del delito como tal. Para ello, anotamos una de las definiciones más clásicas propuestas por Cuello-Calón (1964): "delito en una acción humana antijurídica, típica, culpable y punible". (p. 342). La definición antedicha quiere decir que las infracciones informáticas consisten en actos ejecutados por seres humanos, que se contraponen a la norma jurídica, y que, habiendo sido escritos en la misma, se ejecutan con culpabilidad, lo que lleva una sanción impuesta por los Estados a su autor (es), cómplice (s) y/o encubridor (es)

De acuerdo a lo expuesto, al delito informático se lo puede definir de la siguiente forma: "Acto humano culpable ejecutado con empleo de herramientas informáticas, que lesiona bienes jurídicamente protegidos, y que se encuentra tipificado y sancionado en la norma jurídica". (Narváez-Montenegro, Fiallos, Bucaram, Viscaino, & Carrera-Calderón, 2015, pág. 52). Es menester anotar que, si bien existen varias conductas ciber-delictuales, no todas merecen ser consideradas como delitos, ya que su gravedad es menor en relación a otros hechos; por lo que bien podemos enmarcar ciertas ciber-conductas en el ordenamiento jurídico penal como meras contravenciones. Por esta razón, a criterio del autor, no debería emplearse la denominación de delitos informáticos, si no de infracciones informáticas.

En el contexto internacional, han existido hechos de enorme significación que tienden a combatir el cometimiento de ciberdelitos. Entre ellos hallamos la Convención efectuada en 1971 sobre la Protección y Producción de Fonogramas, que surge como consecuencia de su reproducción ilegal, y por el consiguiente perjuicio que ocasiona a los autores, artistas, intérpretes, ejecutantes y productores de los mismos. En la misma década, en 1974, se dio el Convenio que trató sobre la Distribución de Señales Portadoras de Programas Transmitidas por Satélite. De igual forma, hallamos la Convención de Estocolmo en 1967, sobre Propiedad Intelectual. Después de una década en la República de Cuba, la Organización de Naciones Unidas, y en vista del crecimiento desmedido en el índice de cometimientos de delitos informáticos, decidió debatir a profundidad el tema; como resultado, se logró identificar tres ciberdelitos básicos:

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

El 23 de noviembre del 2001 en Hungría, aconteció el hecho más significativo en cuanto al combate de delitos informáticos, este fue la “Convención de Cibercriminalidad” organizado por el Consejo de Europa. Éste fue un instrumento mucho más amplio que los anteriores, por cuanto abarca más conductas que hasta esa fecha eran enmarcadas en otras figuras penales. Fue ratificada en un principio por treinta países del mundo. A continuación, procedemos a detallar las ciber-conductas identificadas en el Convenio de Ciber-criminalidad realizado en Hungría en el año 2001: acceso ilícito, interceptación ilícita, ataque contra la integridad de los datos, ataque contra la integridad del sistema, abuso de dispositivos, falsificación informática, fraude informático, infracciones relativas a la pornografía infantil, infracciones vinculadas a los atentados a la propiedad intelectual y a los derechos afines.

Iberoamérica por su parte, inició a comienzos de los noventa el debate acerca del delito informático; para lo cual, recogió lo que se había tipificado en legislaciones europeas y en la estadounidense. Entre los estados que empezaron esta tarea estuvo Chile y España, con un marco normativo que resultó novedoso e influyente en nuestro continente; lo que ha permitido que muchas legislaciones latinoamericanas estructuren una variedad de conductas ciber-delictuales, igual y hasta superior al que tienen países con mayor desarrollo normativo y tecnológico que el de Sudamérica, como el paso a señalar:

Estados Unidos

Ciertamente, la contribución de la legislación estadounidense sobre el tema fue significativa, si bien es cierto los Estados Unidos no fue el primer Estado en tipificar en su normativa penal los delitos informáticos, si fue el pionero en abordar de manera más amplia y detallada ciertas conductas informáticas consideradas delictuales. Este país adoptó en 1986 el Acta de Fraude y Abuso Computacional, que preveía conductas que podían resultar lesivas a la información digital almacenada. Con el pasar del tiempo, y dado el aparecimiento de nuevas formas tecnológicas que hacen vulnerable la información digital, se vio la necesidad de reemplazarla por el Acta Federal de Abuso Computacional.

Como se citó anteriormente, a nivel latinoamericano, existen legislaciones que han dado avances considerables sobre el tema, a continuación, se procede a efectuar un listado de países y las conductas cibercriminales que han tipificado en su ordenamiento jurídico penal.

Argentina

Interrupción de comunicaciones, daño informático agravado, distribución y tenencia con fines de distribución de pornografía infantil, violación de correo electrónico, acceso ilegítimo a sistemas informáticos, daño informático y distribución de virus (Ley 26.388, 2009).

Brasil

El acceso no autorizado a ordenadores, conectados o no a internet, mediante la violación de sus mecanismos de seguridad; el robo de contraseñas y contenidos de correos electrónicos; la invasión de dispositivos electrónicos ajenos con el "fin de obtener, cambiar o destruir datos o informaciones"; la producción y distribución de dispositivos que permitan invadir teléfonos inteligentes o tabletas electrónicas; la obtención ilegal de datos bancarios por vías electrónicas y la prohibición impuesta a los medios de comunicación de difundir cualquier tipo de contenido que pueda resultar racista (Ley 12.737, 2012).

México

Es necesario establecer que México es de los países que posee el espectro más amplio de conductas ciber-delictuales, de hecho, que se ha llegado a determinar la existencia de más de doscientos ciberdelitos. Entre ellos establecemos lo más importantes: “revelación de secretos, cracking, hacking, cyberbullying, spam, ciberpunk, acceso no autorizado a sistemas informáticos, entre otros” (Código Penal Federal México, 1999, pág. 120).

Venezuela

Se puede revelar que, en cuanto a delitos informáticos, la legislación venezolana es de las más completas del continente americano. Los cibercrímenes tipificados son:

> Acceso indebido; sabotaje o daño a sistemas; acceso indebido o sabotaje a sistemas protegidos; posesión de equipos o prestación de servicios de sabotaje; espionaje informático; falsificación de documentos; hurto informático; fraude informático; obtención indebida de bienes o servicios; manejo fraudulento de tarjetas inteligentes o instrumentos análogos; apropiación de tarjetas inteligentes o instrumentos análogos; provisión indebida de bienes o servicios, posesión de equipo para falsificaciones; violación de la privacidad de la data o información de carácter personal; violación de la privacidad de las comunicaciones; revelación indebida de data o información de carácter personal; difusión o exhibición de material pornográfico; exhibición pornográfica de niños o adolescentes; apropiación de propiedad intelectual y oferta engañosa (Ley Especial contra los Delitos Informáticos , 2011, pág. 320).

Chile

Destrucción e inutilización de sistemas de tratamiento de información, intercepción e interferencia de información contenida en un sistema informático, alteración, daño, destrucción de datos contenidos en un sistema de tratamiento de información (Ley No. 19.223, 1993).

Costa Rica

Uso doloso e irresponsable de la tecnología de la información, además, la ley en mención aumentó la sanción del delito de corrupción de menores si el delincuente utiliza redes sociales, estableciéndose de cuatro a diez años de prisión. También se tipifica tipos penales para sancionar rigurosamente el espionaje electrónico, la suplantación de identidad, la propagación de malware, el envío de spam y la falsificación de sitios web (Ley 9048.2012, 2012).

Guatemala

fraude Informático, daño informático, acceso ilícito, reproducción de dispositivos de acceso, comercialización de dispositivos fraudulentos, espionaje informático, falsificación informática, violación a la disponibilidad, espionaje informático, intercepción ilícita (Decreto 17-73, 2010).

Panamá.

El acceso ilícito; el apoderamiento, utilización o modificación de información; interferencia, interceptación, obstaculización de sistemas informáticos. (Código Penal de la República de Panamá, 2010).

República Dominicana

Crímenes y Delitos contra la confidencialidad, integridad y disponibilidad de datos y sistemas de información; delitos de Contenido : atentado contra la vida de la persona, el robo mediante la utilización de alta tecnología, la obtención ilícita de fondos, estafa, chantaje, robo de identidad, falsedad de documentos y firmas, uso de equipos para invasión de privacidad, comercio ilícito de bienes y servicios, difamación, injuria pública, atentado sexual, y la adquisición de pornografía infantil; delitos de Propiedad Intelectual y afines; delitos contra las telecomunicaciones; crímenes y delitos contra la nación y actos de terrorismo (Ley N° 53-07, 2007).

Bolivia

Se sanciona la violación de la correspondencia electrónica privada y la falsificación y suplantación de identidad en la web; manipulación informática, la alternación, acceso y uso indebido de datos informáticos; falsedad y falsificación de documentos privados en un sistema digital. Es necesario indicar que antes de la expedición de esta ley la falsedad y falsificación se aplicaba únicamente a documentos físicos o impresos; delitos contra la propiedad intelectual de las obras con soporte electrónico en la web (Ley No 164, 2011) .

Se sanciona a quien cometa sabotaje informático e impida el normal funcionamiento del sistema de información o telecomunicaciones.

Colombia

Acceso abusivo a un sistema informático, obstaculización ilegítima de sistema informático o red de telecomunicación, interceptación de datos informáticos., daño informático, uso de software malicioso, violación de datos personales, suplantación de sitios web para capturar datos personales -es primordial mencionar que este artículo tipifica lo que comúnmente se denomina “phishing”-, hurto por medios informáticos y semejantes, transferencia no consentida de activo (Ley No 1273, 2009).

Perú

En los delitos contra datos y sistemas informáticos se contempla: el acceso ilícito, atentado contra la integridad de datos informáticos, y el atentado contra la integridad de sistemas informático. En los delitos informáticos contra la indemnidad y libertades sexuales se contempla: proposiciones a niños, niñas y adolescentes con fines sexuales por medios tecnológicos. En los delitos contra la intimidad y el secreto de las comunicaciones se contempla: tráfico ilegal de datos, interceptación de datos informáticos. En los delitos informáticos contra el patrimonio se contempla: fraudes informáticos. En los delitos informáticos contra la fe pública: suplantación de identidad (Ley No 30096, 2014).

Paraguay

Pornografía infantil, violación del secreto de la comunicación, intercepción ilícita, interferencia en el sistema, fraude informático e Intercepción ilícita (Ley No 1160/97, 2010).

Uruguay

Uno de los países cuya legislación penal se encuentra más rezagada en materia de delitos informáticos es la uruguaya. En la actualidad la temática del presente artículo está amparada por la ley No 18.331 de Protección de Datos Personales y Acción de Habeas Data y por los artículos 72 y 332 de la Constitución. Sin embargo, el Parlamento uruguayo, en vista del alto índice de delitos que se dan empleando medios informáticos, discute una reforma del Código del Proceso Penal donde se incluye un capítulo relativo a los delitos informáticos, entre los que se consideran: acceso ilícito a sistemas informáticos; intercepción ilícita de información; ataques a la integridad de los datos y del sistema; uso indebido de dispositivos, software o claves de acceso; falsificación y fraude informático (Ley No 18.331, 2008) .

Una vez efectuada una breve revista a la realidad de la legislación americana y española en cuanto a los delitos informáticos, es necesario sacar a limpio las ciber-conductas que deben ser consideradas y sancionadas de manera independiente -y no acoplarlas a figuras penales tradicionales como se ha efectuado hasta ahora-; así como también ciertas recomendaciones que los Estados deben adoptar para evitar su cometimiento.

- Se define el tema y se orienta al lector acerca del tema sobre la revisión.
- Se exponen los objetivos de la investigación.
- No deberá mostrar resultados ni conclusiones del trabajo.
- Escrito en tiempo presente, revisando las publicaciones que orientan al autor, con las citas correspondientes.

DESARROLLO

Recomendaciones a ser consideradas por la legislación americana en cuanto a infracciones informáticas:

Es preciso iniciar el presente tema indicando que, aunque casi la totalidad de legislaciones americanas contienen un marco normativo que tipifica las ciber-conductas criminales, también es verdad que hay infracciones informáticas que merecen ser consideradas de manera más amplia e independiente a otros delitos (no sancionarles acoplándolas a figuras penales tradicionales por que la afectación es mayor si se cometen mediante una red social o correos electrónicos). Ante lo dicho, el objeto del presente artículo, consiste en poner a consideración del legislador americano y de la Academia, recomendaciones y conductas que pueden ser debatidas para una posible tipificación de manera independiente a otras figuras penales tradicionales, y que han sido recogidas del segundo capítulo de (Narváez-Montenegro, Fiallos, Bucaram, Viscaino, & Carrera-Calderón, 2015) y que detallamos a continuación:

De los delitos contra la intimidad y el honor. -

Sin duda, existen ciertos tipos de delitos informáticos afectan la intimidad y el honor de millones de personas en el mundo, las cuales han visto como un tercero (que en varias ocasiones resulta desconocido) valiéndose de la web hace públicas imágenes o grabaciones que solo le incumben a la persona afectada, y que deben tener en ciertas circunstancias una sanción especial , ya que no es lo mismo violar la intimidad y el honor de alguien ante 5 o 10 personas , que hacerlo en valiéndose de una red social donde la vulneración puede acontecer frente ante miles o millones de personas en cuestión de minutos , imágenes o grabaciones que aunque sean borradas por las mismas redes sociales, youtube, etc. , muchas veces quedarán gravadas de manera permanente en celulares o computadoras de las personas que las apreciaron. Ante esto detallamos ciertas circunstancias que se pueden presentar en este delito (Narváez-Montenegro, Fiallos, Bucaram, Viscaino, & Carrera-Calderón, 2015, pág. 75)

Delito contra la intimidad y el honor de las personas. -

- Cuando una persona publique o descargue en redes telemáticas imágenes, videos o grabaciones de actos privados (no sexuales) de un tercero que afecten su imagen o le causen algún perjuicio. Ejemplo: grabar y publicar a una persona con su amante en un café.

- Cuando una persona publique, mire o descargue en redes telemáticas imágenes, videos o grabaciones que evidencien partes íntimas del cuerpo, o la vida sexual de otra persona.
- Cuando una persona suba en redes interconectadas imágenes, videos o grabaciones de un tercero que tienda a ridiculizar su imagen y/o causarle burla social.
- Usurpación de identidad en redes sociales y direcciones electrónicas

- De la apertura indebida de cuentas. - Cuando una persona abra una cuenta en una red social o una dirección electrónica empleando la identidad de una tercera persona que exista o haya existido, efectuando usos que den a entender que se trata de la persona usurpada.
- Apoderamiento indebido de cuentas. - Cuando una persona se apodere fraudulentamente de una cuenta de red social o dirección electrónica de una persona que exista o haya existido, efectuando usos que den a entender que se trata de la persona despojada del control de su cuenta.
- Uso indebido de imágenes fotográficas. - Cuando en su cuenta de red social o dirección electrónica, haga uso de fotografías de otros u otras personas que existan o hayan existido, como parte de su identificación ante los demás.

Del hostigamiento Psicológico. -

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

De la instigación. -

- A menores de edad: Cuando una persona influye en otra persona para que realice algún acto reñido con la ley, la moral o las buenas costumbres, o atente contra su vida.
- A mayores de edad: Cuando una persona influye en otra persona para que realice algún acto reñido con la ley o atente contra su vida.

Una vez que se ha establecido las conductas cibercriminales que merecen un debate más amplio en la legislación americana para su posible positivización en la normativa jurídica penal como figuras penales independientes, en menester que los Estados empiecen el debate con las compañías propietarias de las cuenteas de redes sociales y correos electrónicos, a fin de que su apertura no resulte tan sencillo, sino que se considere en mecanismos que permitan identificar a su titular, sea exigiendo que para su apertura la persona deba proporcionar información como su número de cedula, fecha de expedición de la misma, seguro social, fecha de expedición de permiso de conducir, etc. ,información digital con la que cuenta el Estado y que puede ser cruzada con la base de datos de dichas compañías. Todo esto considerando

la importancia y el poder que han tomado las redes sociales (particularmente) en la actualidad, y que su titularidad debe ser identificable de manera inmediata por las autoridades.
De igual forma, es necesario que las compañías referidas, a pedido del titular de la cuenta, puedan cerrar de manera inmediata cuentas hackeadas , ideando mecanismos con espacios web y con claves alternas o datos de información que solo el titular sepa, ya que en la actualidad no resulta fácil que una persona pueda cerrar inmediatamente una cuenta en una red social en caso que haya perdido el control total de la misma, y hasta tanto, los ciberdelincuentes pueden hacer publicaciones u actos delictivos que pueden vulnerar el derecho de las personas afectadas.

De igual forma es menester que los Estados obliguen a los cyber o centros de cómputo a tener cámaras de seguridad y guardar los videos de los últimos meses (6 meses como mínimo), a fin de conocer la identidad de la persona que utilizó una máquina en particular, desde la cual de cometió uno de los delitos informáticos señalados.

CONCLUSIONES

De acuerdo a lo citado, es necesario que la legislación penal americana tome en consideración los delitos propuestos, ya que, si bien los mismos son acoplados a figuras penales tradicionales, no se toman en cuenta las circunstancias que se describen anteriormente. Por ejemplo, la afectación a la intimidad y el honor de una persona a través de una red social puede causarle un perjuicio mayor, ya que en segundos puede difundir grabaciones o imágenes perjudiciales a miles o millones de personas en todo el mundo. De igual forma, la usurpación de identidad a través de redes sociales o direcciones electrónicas puede darse de diferentes formas y por ende su sanción deberá ser diferente; ciertamente, no es lo mismo que un desconocido abra una cuenta empleando el nombre y foto de otra persona, que apoderarse de la cuenta de Facebook que actualmente posee, efectuar publicaciones perjudiciales, frente a su familia y amigos que mantienen contacto con el perjudicado, los cuales pueden leer en instantes afirmaciones o mensajes que pueden lesionar su imagen o la de terceros; de igual forma, la afectación será diferente si una persona utiliza únicamente como foto de perfil el rostro de otra, pero ante los demás se da a conocer con su identidad original, lo que no significa ni faculta por supuesto, que una persona utilice y muestre el rostro de un tercero como medio de identificación frente a terceros.

Así como los anteriores, el hostigamiento psicológico es un fenómeno social que afecta a miles de personas en todo el mundo, y su cometimiento se facilita al emplear la web, mediante cuentas en redes sociales ficticias, o direcciones electrónicas falsas; por lo que es necesario que el legislador americano analice la posibilidad de tipificar estas conductas como figuras penales con una sanción tomando en cuenta las circunstancias como fue cometida.

Por otro lado, resulta necesario que los Estados obliguen a los lugares de alquiler de computadores, a instalar cámaras de seguridad. Además de la necesidad de que las compañías propietarias de dichas redes y correos electrónicos creen mecanismos que permitan identificar a su titular, así como también, que creen mecanismos que permitan a una persona cerrar una cuenta o dirección electrónica de manera inmediata, sin necesidad de entrar a la misma, sino desde otro espacio web y con mecanismos que solo la persona afectada pueda conocer.

Así también, es menester considerar que la globalización hace necesario armonizar las legislaciones del mundo a fin de consolidar un único ordenamiento jurídico en cuanto a infracciones informáticas, ya que, en efecto, la figura del delito informático es de carácter universal, ya que las mismas conductas criminales que pueden ejecutarse en EEUU se pueden cometer en Japón o en el Ecuador, por lo que la configuración de un solo marco jurídico que establezca los delitos informáticos si es posible.

REFERENCIAS

Código Penal de la República de Panamá. (2010). *Código Penal de la República de Panamá.* Panamá: Nacional.

Código Penal Federal México. (1999). *Código Penal Federal República de México.* Mexico: Nacional.

COIP. (2014). *Código Orgánico Integral Penal.* Quito: Nacional.

Cuello-Calón, E. (1964). *Derecho penal. Parte General.* Barcelona: Bosch.

Decreto 17-73. (2010). *Ley de delitos informáticos.* Managua: Nacional.

Ley 9048.2012. (2012). *Reforma de la Sección VIII, Delitos Informáticos y Conexos, del Título VII del Código Penal.* San José: Nacional.

Ley Especial contra los Delitos Informáticos . (2011). *Ley Especial contra los Delitos Informáticos .* Caracas: Nacional.

Ley N° 53-07. (2007). *Ley N° 53-07 contra Crimenes y Delitos de Alta Tecnología.* Santo Domingo: Nacional.

Ley No 1160/97. (2010). *Código Penal Paraguayo .* Asunción : Nacional.

Ley No 1273. (2009). *Ley No 1273. .* Bogota: Nacional.

Ley No 164. (2011). *Ley General de Telecomunicaciones .* La Paz: Nacional.

Ley No 18.331. (2008). *Protección de Datos personales y Acción de Habeas Data.* Montevideo: Nacional.

Ley No 30096. (2014). *Ley de delitos informáticos.* Lima: Nacional.

Ley No. 19.223. (1993). *Delitos Informáticos; Sistemas de Información; Ley no. 19.223.* Valparaiso: Nacional Chile.

Narváez-Montenegro, D., Fiallos, S., Bucaram, A., Viscaino, F., & Carrera-Calderón, F. A. (2015). *Derecho informático. Conceptos, principios y prácticas.* Quito: Jurídica del Ecuador.