Revista Logos, Ciencia & Tecnología
ISSN: 2145-549X
ISSN: 2422-4200
revistalogoscyt@gmail.com
Policía Nacional de Colombia
Colombia

Análisis de la penalización del cibercrimen en países de habla hispana

Rojas Parra, Jaime Hernán
Análisis de la penalización del cibercrimen en países de habla hispana
Revista Logos, Ciencia & Tecnología, vol. 8, núm. 1, 2016
Policía Nacional de Colombia, Colombia
Disponible en: https://www.redalyc.org/articulo.oa?id=517752176020
DOI: https://doi.org/10.22335/rlct.v8i1.339

Este obra está bajo una licencia de Creative Commons Reconocimiento 4.0 Internacional.

Artículos teóricos

Análisis de la penalización del cibercrimen en países de habla hispana

Analysis of the criminalization of cybercrime in Spanish-speaking countries

Análise da criminalização do cibercrime nos países de língua española

Jaime Hernán Rojas Parra jaime.rojas@correo.policia.gov.co
Escuela de Telemática y Electrónica de la Policía Nacional de Colombia, Colombia
http://orcid.org/0000-0002-8191-6250

Revista Logos, Ciencia & Tecnología, vol. 8, núm. 1, 2016

Policía Nacional de Colombia, Colombia

Recepción: 05 Mayo 2015
Aprobación: 18 Julio 2016

DOI: https://doi.org/10.22335/rlct.v8i1.339

Redalyc: https://www.redalyc.org/articulo.oa?id=517752176020

Resumen: El presente artículo propone un análisis de la tipificación y penalización de conductas punibles relacionadas con la delincuencia informática en cada uno de los veinte países de habla hispana a nivel mundial, así como la descripción de la normalización de sus leyes con respecto a los instrumentos y convenios de carácter internacional, relacionados con la regulación de uso de tecnologías de la información. Este análisis se realiza desde las siguientes perspectivas de estudio de la legislación penal existente y vigente, identificación de los delitos informáticos tipificados, selección del delito informático con mayor penalización y participación de cada uno de los países indagados en el convenio de la ciberdelincuencia de Budapest (como referencia mundial en este campo). Asimismo, se presentan las tablas y gráficas comparativas entre los países motivo de estudio, mediante las cuales se identifican los países con mayor y menor cantidad de delitos informáticos tipificados, así como los rangos de penalización máxima y mínima en cada uno.

Palabras clave: castellano, dato, delito, electrónico, informático, internet, ley, país, pena, prisión, red, sistema, telemático, telecomunicaciones.

Abstract: This article proposes an analysis of the criminalization and prosecution of criminal conduct related to cybercrime in each of the 20 spanish-speaking countries worldwide, as well as the description of the normalization of its laws regarding instruments and international agreements related to the regulation of the use of information technology. This analysis is done from the following three perspectives: study of existing criminal law and force, identification of established computer crime, selection of computer crime with greater penalties and participation of each of the countries investigated in the agreement cybercrime Budapest (as a world reference in this field). It also, offered the tables and graphs comparisons between the countries being studied, whereby countries with major and minor amount of established computer crime and the range of maximum and minimum in each of the same penalty are identified countries.

Keywords: Castilian, crime, computer, country, data, electronic, internet, law, network, penalty, system, prison, telecommunications, telematics.

Introducción

Teniendo en cuenta el incontrolable crecimiento de la criminalidad informática con alcances transnacionales, se hace necesario identificar la legislación que penalice o tipifique la delincuencia informática en cada

uno de los países de habla hispana, aunado a que no existe un estudio actualizado de la geolocalización y categorización de la mencionada conducta punible, como tampoco de la capacidad de las naciones para prevenirla o investigarla y de sus políticas públicas o legislativas al respecto, como herramienta útil de cooperación, coordinación y colaboración con el desarrollo de una estrategia internacional para su neutralización desde la infraestructura del Estado, como ente de persecución penal.

Como lo refiere una de las publicaciones científicas de la Policía Nacional de Colombia, "El líder policial, para el nuevo modelo social y de convivencia que se avecina, tendrá que fortalecer sus competencias de pensamiento estratégico, para que su nuevo liderazgo sea un factor fundamental en su responsabilidad de velar por la convivencia en paz de todos los colombianos" (Pulecio, 2016).

La necesidad de adelantar una investigación de este tipo radica en los constantes cambios y modificaciones que sufren las leyes penales en el mundo, debido a que la gran mayoría de países son conscientes de que esta regulación debe adaptarse a las necesidades y urgencias que aparecen a medida que evolucionan las tecnologías de la información, así como los riesgos y vulnerabilidades que implica su utilización.

Así, se requiere un estudio actualizado y vigente de la identificación de los niveles de severidad o permisividad con respecto al castigo que significa la comisión de delitos informáticos (Vergel, Martínez, Zafra, 2016), para de esta manera conocer las regiones con mayor o menor fragilidad a la delincuencia informática, así como sus consecuencias y por supuesto obtener conclusiones que permitan identificar los países en los que potencialmente se hace cómodo o no cometer delitos informáticos.

Análisis específico por país

España

Mediante la Ley Orgánica 10 del 23 de noviembre de 1995, las Cortes Generales y el rey de España aprobaron y sancionaron el Código Penal vigente, el cual incluye la tipificación de la delincuencia informática.

El delito informático con mayor pena de prisión en este país es la "Alteración, copia, reproducción o falsificación de tarjetas de crédito o débito o cheques de viaje; así como la fabricación o tenencia de útiles, materiales, instrumentos, sustancias, máquinas, programas de ordenador o aparatos, específicamente destinados a la comisión de la conducta referida" (las Cortes Generales y el rey de España, 1995).

España es un modelo de referencia en este campo, debido a su condición de Estado miembro del Concejo Europeo, firmó el convenio del cibercrimen el 23 de noviembre del 2001, realizando su última ratificación el 3 de junio de 2010 y entrada en vigor el 1.º de octubre del mismo año.

República Dominicana

El Congreso Nacional de la República Dominicana dispone la Ley 53 del 2007, sobre "crímenes y delitos de alta tecnología", cuyo objeto es la protección integral de los sistemas de tecnologías de la información y comunicación, su contenido, la prevención y sanción de las conductas punibles cometidas contra estos o las cometidas mediante el uso de tecnología en perjuicio de las personas.

Los delitos informáticos con mayor pena de prisión en esta nación son los siguientes:

- "El sabotaje, espionaje o suministro de informaciones, a través de un sistema informático, electrónico, telemático o de telecomunicaciones, atentando contra los intereses fundamentales y seguridad de la Nación" (Congreso Nacional de la República Dominicana, 2007).
- "Ejercer actos de terrorismo, con el uso de sistemas electrónicos, informáticos, telemáticos o de telecomunicaciones" (Congreso Nacional de la República Dominicana, 2007).

La República Dominicana es el primer país latinoamericano en ratificar el Convenio sobre la Ciberdelincuencia, debido a que a principios de 2013 ratificó su adhesión como Estado no miembro del Consejo de Europa, convenio que entró en vigor en junio del mismo año, siendo a partir de ese momento un modelo para Sur y Centroamérica.

Panamá

El Código Penal de Panamá, adoptado por la Ley 14 de 2007, con las modificaciones y adiciones introducidas por las leyes 26 de 2008, 5.ª de 2009, 68 de 2009 y 14 de 2010, tipifica principalmente los delitos informáticos en su título viii, "Delitos contra la seguridad jurídica de los medios electrónicos".

Los delitos informáticos con mayor pena de prisión en este país son los siguientes:

- "Fabricar, elaborar, producir, ofrecer, comercializar, exhibir, publicar, publicitar, difundir o distribuir a través de Internet o de cualquier medio masivo de comunicación o información, material pornográfico; presentando o representando virtualmente a una o varias personas menores de edad en actividades de carácter sexual, reales o simuladas" (Gobierno de Panamá, 2010).
- "Utilizar Internet, para el entrenamiento en la construcción de artefactos explosivos o el reclutamiento de personas, para la ejecución de actos con fines terroristas" (Gobierno de Panamá, 2010).

El 5 de marzo de 2014 se ratifica la adhesión de Panamá al Convenio sobre la Ciberdelincuencia como Estado no Miembro del Consejo de

Europa, entró en vigor el 1.º de julio del mismo año. Se convierte en el segundo país latinoamericano, después de República Dominicana, en ratificar el convenio citado.

Colombia

Mediante la Ley 1273, del 5 de enero de 2009, se modifica el Código Penal Colombiano con el objeto de crear un nuevo bien jurídico tutelado denominado "De la protección de la información y de los datos", además de preservar integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones.

El Congreso de Colombia decreta la adición al Código Penal del título vii bis, "De la protección de la información y de los datos", el cual se compone únicamente de dos capítulos, a saber:

El delito informático con mayor pena de prisión en Colombia es el hurto por medios informáticos y semejantes, el cual consiste en superar medidas de seguridad informáticas para apoderarse de una cosa mueble ajena, con el fin de obtener provecho para sí o para otro, mediante la manipulación de un sistema informático, una red de sistema electrónico, telemático u otro medio semejante o mediante la suplantación de un usuario ante sistemas de autenticación y de autorización establecidos (Congreso de la República de Colombia, 2009).

El 11 de septiembre de 2013, Colombia fue invitada a adherirse al Convenio sobre la Ciberdelincuencia, por parte del Consejo de Ministros del Consejo de Europa, con la posibilidad de ser parte de su protocolo adicional, relativo a la penalización de actos de índole racista y xenófoba, cometidos por medio de sistemas informáticos. A partir de dicha fecha se cuenta con un máximo de cinco años para adherir a este importante instrumento internacional.

Argentina

Mediante la Ley 26388, del 4 de junio de 2008, se modifica la Ley 11179, Código Penal de la Nación Argentina, con el objeto de incorporar y sustituir del código referido varios artículos regulatorios de los delitos informáticos.

El Senado y Cámara de Diputados argentinos, reunidos en congreso, sancionaron la sustitución del epígrafe del capítulo iii del título v del libro ii de su Código Penal, definiéndolo como "Violación de secretos y de la privacidad", el cual castiga y tipifica las conductas punibles como aparece a continuación:

El delito informático con mayor pena de prisión es "Defraudar con nombre supuesto, calidad simulada, falsos títulos, influencia mentida, abuso de confianza o aparentando bienes, crédito, comisión, empresa o negociación o valiéndose de trucos o engaños, mediante cualquier técnica de manipulación informática que altere el normal funcionamiento de

sistemas informáticos" (Senado y Cámara de Diputados de la Nación de Argentina, 2008).

En marzo de 2010, Argentina fue invitada a adherirse al Convenio sobre la Ciberdelincuencia por parte del Consejo de Ministros del Consejo de Europa.

Chile

Mediante la Ley 19223, del 7 de junio de 1993, el Congreso Nacional de Chile tipifica las figuras penales relativas a la informática con la promulgación de tan solo cuatro artículos que sancionan los delitos informáticos.

Asimismo, mediante la Ley 18168 del 10 de octubre de 1982, la Junta de Gobierno de la República de Chile aprueba la ley general de telecomunicaciones, en la cual se tipifican algunas conductas relacionadas con el uso indebido de las telecomunicaciones.

Existe también un complemento a la ley de delitos informáticos de Chile, realizado mediante la Ley 20009, del 18 de marzo de 2005, que sanciona el uso indebido de tarjetas de crédito o débito y limita la responsabilidad de los propietarios de tarjetas de crédito por operaciones realizadas con tarjetas extraviadas, robadas o hurtadas.

El delito informático con mayor pena de prisión en Chile es la "Difusión pública o privada de cualquier comunicación obtenida con infracción a lo establecido en Ley General de Telecomunicaciones, algunas de las cuales se describen anteriormente" (Congreso Nacional de Chile, 2005).

Durante el año 2010, el Consejo de Europea emitió la invitación a Chile para formar parte del Convenio sobre la Ciberdelincuencia; actualmente este país se encuentra realizando las gestiones para su adhesión.

Costa Rica

Mediante la Ley 9048, del 6 de noviembre de 2012, la Asamblea Legislativa de la República de Costa Rica reforma varios artículos del Código Penal y el título vii en la sección viii, denominada "Delitos informáticos y conexos".

El tipo penal informático con mayor pena de prisión en Costa Rica es el que se cometa para afectar la lucha contra el narcotráfico o el crimen organizado, por medio de sistemas o redes informáticas o telemáticas, contenedores electrónicos, ópticos o magnéticos. La pena podría llegar a ser hasta de 240 meses de prisión (Asamblea Legislativa de la República de Costa Rica, 2012). El 31 de enero de 2007, el Comité de Ministros del Consejo de Europa invitó a Costa Rica a adherirse al Convenio sobre la Ciberdelincuencia.

México

Mediante una reforma publicada el 6 de junio de 2007 se modifica el Código Penal Federal de México, con el objeto de penalizar las conductas relacionadas con la corrupción de menores e incapaces, pornografía infantil y prostitución sexual de menores, delitos en materia de derechos de autor, revelación de secretos y acceso ilícito a sistemas y equipos de informática.

El delito informático con mayor pena de prisión en México es "Transmitir, elaborar, reproducir, vender, arrendar, exponer o publicitar material que contenga grabaciones de actos de exhibicionismo corporal, lascivos o sexuales en que participen uno o más menores de 18 años" (Gobierno de México, 2007).

El 31 de enero del 2007 México fue invitado a adherirse al Convenio de Budapest, adhesión pendiente debido a que cuenta con el Estatuto de Observador ante el Consejo de Europa desde 1999, lo que le ha permitido tanto la realización de reformas constitucionales en telecomunicaciones, estrategias digitales nacionales, como ganar experiencia en el Comité Especializado en Seguridad de la Información del Consejo de Seguridad Nacional.

Perú

El 22 de octubre de 2007, el Congreso de la República de dicha nación emite la Ley 30096 o ley de delitos informáticos, la cual tiene por objeto prevenir y sancionar toda conducta ilícita cometida a través de la utilización de tecnologías de la información o comunicación que puedan llegar a afectar sistemas, datos informáticos y otros bienes jurídicos penalmente importantes.

Esta ley, cuya finalidad es luchar contra la ciberdelincuencia, consta de siete capítulos, a saber: "finalidad y objeto de la Ley", "delitos contra datos y sistemas informáticos", "delitos informáticos contra indemnidad y libertad sexuales", "delitos informáticos contra la intimidad y el secreto de las comunicaciones", "delitos informáticos contra el patrimonio", "delitos informáticos contra la fe pública" y finalmente "disposiciones comunes".

El 10 de marzo de 2014, el Congreso de la República del Perú emite la Ley 30171, la cual modifica la Ley 30096, ley de delitos informáticos, con el objeto de incorporar la calidad de "deliberada" e "ilegítima" a las conductas delictivas, sancionadas en la tipificación de los delitos informáticos regulados.

Los delitos informáticos con mayor pena de prisión en la República del Perú son los siguientes:

- "Interceptación indebida de datos informáticos en transmisiones no públicas, dirigidas, originadas o efectuadas en sistemas informáticos o electromagnéticos, mediante el uso de tecnologías de la información o comunicación, que comprometa la defensa,

la seguridad o la soberanía nacional" (Congreso de la República del Perú).

- "Fraude a través de las tecnologías de la información o comunicación, para diseñar, introducir, alterar, borrar, suprimir, clonar datos informáticos o cualquier interferencia o manipulación del funcionamiento de sistemas informáticos, para afectar el patrimonio del Estado destinado a fines asistenciales" (Congreso de la República del Perú).

Paraguay

El 26 de noviembre de 1997, el Congreso de la Nación Paraguaya publica su Código Penal mediante la sanción de la Ley 1160, la cual tipifica algunos delitos informáticos, la comisión de otras conductas punibles a través de las nuevas tecnologías y otros tipos penales relacionados con la delincuencia informática.

El delito cometido mediante el uso de medios técnicos con mayor pena de prisión en la República del Paraguay es "Actuar comercialmente o como miembro de una organización criminal dedicada a la falsificación, alteración, adquisición, ofrecimiento, entrega o utilización de tarjetas de débito o de crédito y otros medios electrónicos de pago" (Congreso de la Nación Paraguaya, 1997).

Venezuela

El 4 de septiembre de 2001, la Asamblea Nacional de la República Bolivariana de Venezuela aprueba la Ley Especial Contra Delitos Informáticos, la cual busca proteger integralmente los sistemas que utilizan tecnologías de información y comunicación, prevenir y sancionar los delitos cometidos contra los sistemas referidos o sus componentes y los cometidos a través del uso de este tipo de tecnologías. La Ley Especial Contra Delitos Informáticos se encuentra conformada únicamente por tres títulos. El primero de ellos se relaciona con las disposiciones generales, el segundo trata de los delitos directamente y el tercero determina las disposiciones comunes.

Los delitos informáticos con mayor pena de prisión en la República Bolivariana de Venezuela son los siguientes:

Sabotaje o daño a sistemas. Creación, introducción o transmisión, por cualquier medio, de un virus o programa análogo, con la intención de destruir, dañar, modificar o realizar cualquier acto que altere el funcionamiento o inutilice un sistema que utilice tecnologías de información o cualquiera de los componentes que lo conforman (Asamblea Nacional de la República Bolivariana de Venezuela , 2001).

Manejo fraudulento de tarjetas inteligentes o instrumentos análogos. Crear, capturar, grabar, copiar, alterar, duplicar o eliminar datos o información contenidos en una tarjeta inteligente o en cualquier instrumento destinado a los mismos fines; o usar indebidamente las

tecnologías de información para incorporar usuarios, cuentas, registros o consumos inexistentes o modificar la cuantía de estos (Asamblea Nacional de la República Bolivariana de Venezuela, 2001).

Bolivia

El título x, "Delitos contra la libertad", y el título xii, "Delitos contra la propiedad", del libro segundo del Código Penal de Bolivia contienen, cada uno, un capítulo relacionado con la tipificación de delitos relativos a la delincuencia informática.

Cabe resaltar que mediante la Ley 1768, del 10 de marzo de 1997, el Congreso Nacional decreta las modificaciones al Código Penal, en las que se incluye el capítulo xi del título xii del libro segundo, "Delitos informáticos".

El delito informático con mayor pena de prisión en Bolivia es la manipulación informática para obtener un beneficio indebido para sí o para un tercero mediante el procesamiento o transferencia de datos informáticos que conduzca a un resultado incorrecto o evite un proceso tal cuyo resultado habría sido correcto, ocasionando de esta manera una transferencia patrimonial en perjuicio de tercero (Congreso Nacional de Bolivia, 1997).

Es importante referir que actualmente Bolivia se encuentra desarrollando el proyecto de ley de telecomunicaciones, el cual plantea la modificación de los artículos del Código Penal relacionados con la delincuencia informática, en busca de robustecer y aumentar las penas contra la manipulación informática; la alteración, acceso y uso indebido de datos informáticos y proteger la propiedad intelectual de las obras con soporte electrónico; la falsedad material, ideológica y falsificación de documentos privados; la violación de la correspondencia electrónica privada y la falsificación y suplantación de identidad; el sabotaje informático y la interrupción del normal funcionamiento de sistemas de información o telecomunicaciones.

Nicaragua

El 13 de noviembre de 2007, la Asamblea Nacional de Nicaragua aprobó la Ley No. 641, "Código Penal"; el cual no contiene un Título o Capitulo especifico que sancione los delitos informáticos, pero si evidencia la regulación y castigo de conductas punibles relacionadas, tal como se evidencia a continuación.

El delito informático con mayor pena de prisión en Nicaragua es "Introducirse indebidamente y con fines de espionaje en los programas informáticos relativos a la seguridad nacional o defensa nacional" (Asamblea Nacional de Nicaragua, 2007).

Guatemala

El 27 de julio de 1973, el Congreso de la República de Guatemala promulga el Decreto 17-73, con el que se dicta el Código Penal, el cual se encuentra actualmente reformado de acuerdo con las importantes necesidades y urgencias de la realidad guatemalteca, así como con los avances de la ciencia penal y la evolución de las tecnologías de la información, la comunicación y sus sistemas.

El delito informático con mayor pena de prisión en Guatemala es utilizar registros informáticos o programas de computación para ocultar, alterar o distorsionar información requerida para una actividad comercial, para el cumplimiento de una obligación respecto al Estado o para ocultar, falsear o alterar los estados contables o la situación patrimonial de una persona física o jurídica (Congreso de la República de Guatemala, 1973).

Hasta ahora, la República de Guatemala no ha sido invitada a adherirse al Convenio sobre la Ciberdelincuencia, aunque desde el 2010 este país cuenta con un dictamen favorable de la Iniciativa 4055, que busca crear la ley de delitos informáticos, cuyo objeto es la prevención y sanción de los delitos informáticos, además de brindar protección e inviolabilidad a la confidencialidad, integridad y disponibilidad de datos y tecnologías de la información de las personas.

Honduras

El 26 de septiembre de 1983, el Congreso Nacional de Honduras promulga el Decreto 144-83, con el que se crea el Código Penal.

El delito informático con mayor pena de prisión en Honduras es "Financiar, producir, reproducir, distribuir, importar, exportar, ofrecer, comercializar o difundir, por medio directo, mecánico, informático o electrónico, material en el que se evidencien personas menores de 18 años de edad en acciones o actividades pornográficas o eróticas" (Congreso Nacional de Honduras, 1983).

Ecuador

El 28 de enero de 2014, la Asamblea Nacional de la República del Ecuador expide el Código Orgánico Integral Penal, el cual cuenta con una sección especial relacionada con los delitos contra la seguridad de los activos de los sistemas de información y comunicación, además de incluir a lo largo de sus artículos las sanciones a las conductas penales clásicas cometidas a través de medios informáticos o electrónicos.

El delito informático con mayor pena de prisión en Ecuador es la pornografía con utilización de niñas, niños o adolescentes, mediante la fotografía, filmación, grabación, producción, transmisión o edición de materiales visuales, audiovisuales, informáticos, electrónicos o de cualquier otro soporte físico o formato que contenga su representación

visual de desnudos o semidesnudos reales o simulados (Asamblea Nacional de la República del Ecuador, 2014).

Hasta ahora, Ecuador no ha sido invitado a adherirse al Convenio sobre la Ciberdelincuencia, aunque está analizando adelantar las gestiones para hacerlo, teniendo en cuenta la expedición de su nuevo Código Orgánico Integral Penal, que tipifica la delincuencia informática de manera detallada, como se evidencia, además de contar con la Ley 67 del 2002, "Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos", cuyo objeto es regular los mensajes de datos, la firma electrónica, los servicios de certificación, la contratación electrónica y telemática, la prestación de servicios electrónicos a través de redes de información, incluidos el comercio electrónico y la protección a los usuarios de estos sistemas.

El Salvador

El 10 de junio de 1997, la Asamblea Legislativa de El Salvador publica el Código Penal, modificado por última vez el 16 de octubre de 2014, con el fin de enunciar los delitos o faltas que cometen las personas y las penas que tendrán que cumplir, dentro de las que se tipifican y sancionan algunas conductas penales clásicas cometidas a través de medios informáticos o electrónicos.

El delito informático con mayor pena de prisión en El Salvador es la utilización de personas menores de 18 años e incapaces o deficientes mentales en pornografía mediante la producción, reproducción, distribución, publicación, importación, exportación, ofrecimiento, financiación, venta, comercialización o difusión de sus imágenes o voz en forma directa, informática, audiovisual o virtual, para exhibir actividades sexuales, eróticas o inequívocas de naturaleza sexual, explícitas o no, reales o simuladas (Asamblea Legislativa de El Salvador, 2014).

Uruguay

El Código Penal de la República Oriental de Uruguay es la única legislación que se relaciona con la tipificación de la delincuencia informática, aunque no se enuncian ni sancionan conductas penales cometidas a través de medios electrónicos, sistemas informáticos o programas de computación.

El delito informático con mayor pena de prisión en Uruguay es la "Violación de correspondencia escrita, mediante apertura, interceptación, destrucción u ocultamiento de encomiendas y demás objetos postales para apropiarse de su contenido o interrumpir el curso normal de los mismos" (República Oriental de Uruguay, 1933).

Es importante mencionar que el 16 de mayo de 2014, la Comisión de Constitución, Códigos, Legislación General y Administración de la República Oriental de Uruguay presenta al presidente de la Asamblea General el proyecto de ley de delitos informáticos, el cual consta de siete

artículos, mediante los que se busca tipificar conductas punibles como las siguientes:

- Acceso no autorizado a todo o parte de un sistema informático.
- Daño a sistemas informáticos. Prisión de 6 a 36 meses.
- Estafa informática. Prisión de 6 a 48 meses.
- Suplantación de identidad mediante la utilización de tecnologías, para la cual hay penas de 18 a 96 meses de prisión.
- Tratamiento engañoso, abusivo o extorsivo de datos personales, 3 a 72 meses de prisión.
- Circunstancias de agravación punitiva.

Puerto Rico

El 30 de julio de 2012, mediante la Ley 146, se adopta el Código Penal, actualmente vigente, y se deroga el anterior (del 2004), con el fin de incluir sanciones a algunas conductas penales clásicas cometidas a través de Internet, medios electrónicos o informáticos.

Puerto Rico cuenta también con la Ley 165 del 2008, "Ley de Regulación de Programación de Espionaje Cibernético", cuyo fin es proteger al consumidor en el uso y abuso de la programación cibernética y de cualquier subterfugio electrónico que permita a un tercero acceder sin autorización a la información contenida en un programador que no le pertenece.

El delito informático con mayor pena de prisión en Puerto Rico es el sabotaje de servicios esenciales mediante la destrucción, daño, alteración o interrupción del funcionamiento de las instalaciones o equipos de los servicios de agua, gas, electricidad, teléfono, telecomunicaciones, sistemas o redes de computadoras o cualquier otra propiedad destinada a proveer servicios públicos o privados esenciales y se impida que una persona solicite o reciba ayuda para su vida, salud o integridad física (Gobierno de Puerto Rico, 2012).

Cuba

El 28 de diciembre de 1987, la Asamblea Nacional del Poder Popular de la República de Cuba acuerda mediante la Ley 62 el Código Penal, el cual no tipifica de manera concreta o específica la delincuencia informática.

El delito informático con mayor pena de prisión en Cuba es "Impedir u obstaculizar su normal uso o funcionamiento, así como destruir, alterar, dañar o perjudicar en cualquier forma, fuentes energéticas, obras hidráulicas, servicios de transporte terrestre, de comunicaciones y de difusión" (Asamblea Nacional del Poder Popular de la República de Cuba, 1987).

Tipificación de la delincuencia informática en cada país

Cantidad de delitos informáticos tipificados por país

A continuación se analiza la cantidad de delitos informáticos tipificados por cada país materia de estudio; República Dominicana tiene más que los demás (31) y Uruguay es el que tiene menos, tan solo 4.

Tabla 1.
Delitos informáticos tipificados por país

Puesto	País	Cantidad
1.º	República Dominicana	31
2.º	Paraguay	22
3.º	Costa Rica	21
4.º	México	20
5.º	Venezuela	20
6.º	Ecuador	19
7.º	Chile	14

Tabla 1. Continuación
Delitos informáticos tipificados por país

8.º	España	13
9.º	Argentina	13
10	Nicaragua	13
11	Perú	12
12	El Salvador	12
13	Puerto Rico	11
14	Cuba	11
15	Panamá	10
16	Colombia	9
17	Guatemala	9
18	Honduras	8
19	Bolivia	6
20	Uruguay	4
Promedio ponderado general		13,9

Fuente: Código penal o legislación equivalente en cada país estudiado.

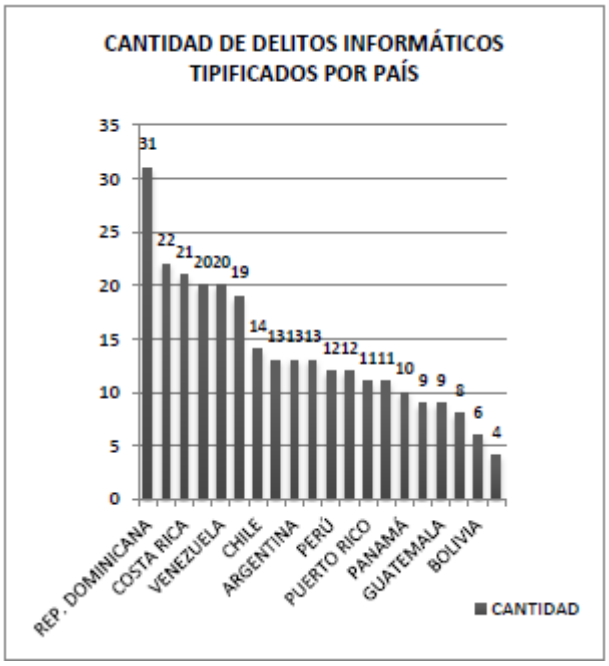

Figura 1.
Cantidad de delitos informáticos tipificados por país
Fuente: Código penal o legislación equivalente en cada país estudiado.

Se puede afirmar que en Uruguay, Bolivia y Honduras existen muy pocas conductas penales relacionadas con la delincuencia informática tipificadas en sus legislaciones, y por tanto se convierten en países con mayor riesgo y propensión a actuaciones delictivas ilegítimas y deliberadas respecto de delitos informáticos.

Penas máximas a delitos informáticos tipificados por país

El estudio de las penas máximas para los delitos informáticos tipificados por país evidencia que aquel con mayor severidad en el castigo con pena de prisión es República Dominicana (360 meses) y el de menor castigo con esta pena es Uruguay (48 meses), como se ilustra en la siguiente tabla, ordenada de mayor a menor.

Tabla 2.
Penas máximas para delitos informáticos tipificados por país

Puesto	País	Meses
1.º	República Dominicana	360
2.º	Costa Rica	240
3.º	Colombia	192
4.º	Ecuador	192
5.º	Honduras	180
6.º	Puerto Rico	180
7.º	México	168
8.º	El Salvador	144
9.º	Panamá	120
10	Perú	120
11	Paraguay	120
12	Venezuela	120
13	Cuba	120
14	España	96

Tabla 2. Continuación
Penas máximas para delitos informáticos tipificados por país

15	Nicaragua	96
16	Argentina	72
17	Chile	60
18	Bolivia	60
19	Guatemala	60
20	Uruguay	48
Promedio ponderado general		137,4

Fuente: Código penal o legislación equivalente en cada país estudiado.

Igualmente, en la siguiente gráfica 2 se comparan los códigos penales o su legislación equivalente respecto del máximo de meses de prisión como sanción a la comisión del delito informático de mayor gravedad. Se tiene un promedio ponderado general de 137,4 meses para los 20 países hispanohablantes.

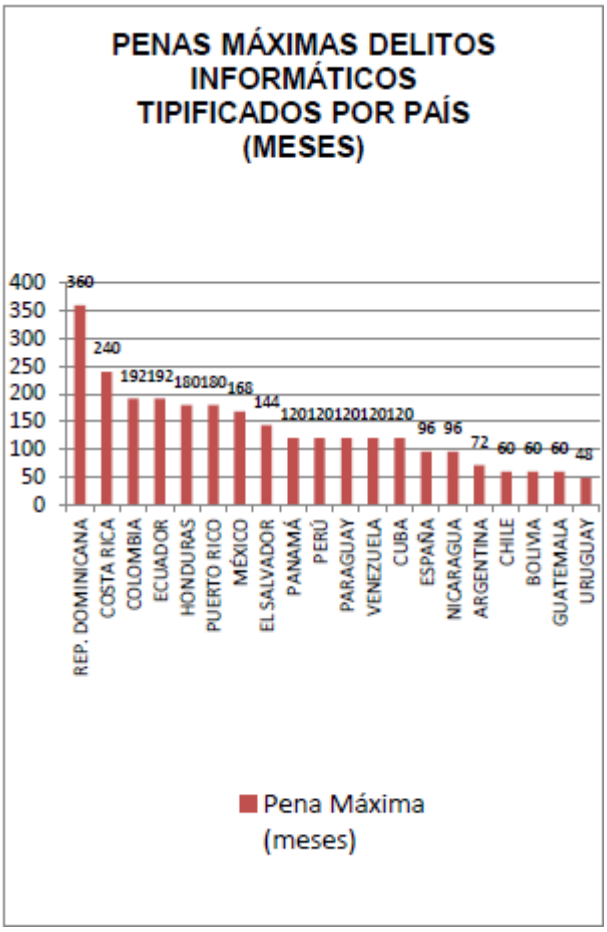

Figura 2
Penas máximas para delitos informáticos tipificados por país.
Fuente: Código penal o legislación equivalente en cada país estudiado.

Penas mínimas a delitos informáticos tipificados por país

Igualmente, se realiza un estudio de las penas mínimas para los delitos informáticos tipificados por país; aquellos con mayor castigo en la pena mínima de prisión son Colombia y Honduras (36 meses), mientras que en Paraguay, Bolivia, El Salvador, Uruguay y Puerto Rico ocurre lo contrario (no aplican esta pena), como se ilustra en la siguiente tabla, ordenada de mayor a menor.

Puesto	País	Meses
1.º	Honduras	36
2.º	Colombia	36
3.º	Ecuador	12
4.º	Venezuela	12
5.º	Perú	12
6.º	Panamá	12
7.º	Guatemala	6
8.º	Nicaragua	6
9.º	Costa Rica	6
10	España	6
11	Cuba	3
12	México	3
13	República Dominicana	3
14	Chile	2

Tabla 3.
Penas mínimas para delitos informáticos tipificados por país
Fuente. Código penal o legislación equivalente en cada país estudiado.

Tabla 3. Continuación
Penas mínimas para delitos informáticos tipificados por país

15	Argentina	0.5
16	Puerto Rico	0
17	Uruguay	0
18	El Salvador	0
19	Bolivia	0
20	Paraguay	0
Promedio ponderado general		7,775

Mediante la siguiente gráfica se comparan los códigos penales o sus legislaciones equivalentes en los países estudiados respecto del mínimo de meses de prisión para la comisión del delito informático de menor gravedad. Se tiene un promedio general de 7,775 meses.

Figura 3.
Penas mínimas a delitos informáticos tipificados por país
Fuente: Código penal o legislación equivalente en cada país estudiado.

Paraguay, Bolivia, El Salvador, Uruguay y Puerto Rico no castigan con prisión las conductas penales relacionadas con la delincuencia informática.

Conclusiones

Es justo reconocer que de los países estudiados, República Dominicana se caracteriza por ser una de las naciones de habla hispana con mayor severidad penal en lo relacionado con la delincuencia informática, ya que cuenta con el mayor número de delitos informáticos tipificados y las más altas penas de prisión.

Uruguay y Bolivia son los países donde los delitos informáticos no implican la privación de la libertad, situación por la cual llama la atención, ya que estimula el desarrollo de la delincuencia informática.

Paraguay, El Salvador y Puerto Rico son los que castigan con menos meses de prisión las conductas penales relacionadas con la delincuencia informática, cuentan con una cantidad aceptable de delitos informáticos tipificados y un buen número de penas máximas en meses de prisión.

En general, los países restantes están relativamente equilibrados con respecto a las sanciones a la delincuencia cibernética; por tanto, es importante referir que en la mayoría de países de habla hispana no debería ser llamativo incurrir en conductas como acceso o interceptación ilícita a redes y sistemas informáticos, ataques a la integridad de los datos y de los sistemas y falsificación o fraude informático.

Referencias bibliográficas

Congreso de la Nación Paraguaya. (1997). Ley 1160 de noviembre de 1997, Código Penal de Paraguay. Asunción.

Congreso de la República de Colombia. (2009). Ley 1273 de enero de 2009 "de la protección de la información y de los datos". Bogotá.

Congreso de la República de Guatemala. (1973). Decreto 17-73 de julio de 1973, Código Penal de Guatemala. Ciudad de Guatemala.

Congreso de la República del Perú. (s. f.). Ley 30096 de 22 de octubre de 2007, "Ley de Delitos Informáticos".

Congreso Nacional de Bolivia. (1997). Ley 1768 de marzo de 1997, Código Penal. Sucre.

Congreso Nacional de Chile. (1993). Ley 19223 de junio de 1993. Santiago de Chile.

Congreso Nacional de Chile. (2005). Ley 20009 de marzo de 2005 "Complemento a la Ley de Delitos Informáticos de Chile". Santiago de Chile.

Congreso Nacional de Honduras. (1983). Decreto 144-83 de septiembre de 1983, Código Penal. Tegucigalpa.

Congreso Nacional de la República Dominicana. (2007). Ley número 53 del 2007, sobre "Crímenes y Delitos de Alta Tecnología". Santo Domingo.

Gobierno de México. (2007). Reforma de junio de 2007, "Modificación al Código Penal Federal de México". Ciudad de México.

Gobierno de Panamá. (2010). Ley 14 de 2010, Código Penal de Panamá. Ciudad de Panamá.

Gobierno de Puerto Rico. (2012). Ley 146 de julio de 2012, Código Penal. San Juan.

Senado y Cámara de Diputados de la Nación de Argentina. (2008). Ley 26388 del 4 de junio de 2008, Código Penal de la Nación Argentina. Buenos Aires.

Asamblea Nacional de la República del Ecuador. (2014). Código Orgánico Integral Penal de enero de 2014. Quito.

Asamblea Legislativa de El Salvador. (2014). Modificación al Código Penal de El Salvador. San Salvador.

Asamblea Legislativa de la República de Costa Rica. (2012). Ley 9048 de Noviembre de 2012, Reforma el Código Penal de Costa Rica. San José.

Asamblea Nacional de la República Bolivariana de Venezuela. (2001). Ley Especial Contra Delitos Informáticos de septiembre de 2001. Caracas.

Asamblea Nacional de Nicaragua. (2007). Ley 641 de noviembre de 2007, Código Penal de Nicaragua. Managua.

Asamblea Nacional del Poder Popular de la República de Cuba. (1987). Ley 62 de diciembre de 1987, Código Penal. La Habana.

Las Cortes Generales y el Rey de España. (1995). Ley Orgánica 10 del 23 de noviembre de 1995, Código Penal Español. Madrid.

Pulecio, C. D. (2016). Pensamiento estratégico, el gran desafío para las Fuerzas Armadas de Colombia. En C. D. Pulecio, Revista Logos Ciencia & Tecnología (págs. 9-16). Bogotá: Imprenta Nacional.

República Oriental de Uruguay. (1933). Código Penal Uruguayo. Montevideo.

Vergel, M., Martínez, J. & Zafra, S. (2016). Factores asociados al bullying en instituciones de educación superior. Revista Criminalidad, 58 (2): 197-208.