Delitos Informáticos en Latinoamérica: Un estudio de derecho comparado. 1ra. Parte.

Temperini, Marcelo Gabriel Ignacio
Becario Tipo I de CONICET, Doctorando en Derecho en la Facultad de Ciencias Jurídicas y Sociales de la Universidad Nacional del Litoral

Abstract
De acuerdo a diferentes estudios actuales, los delitos informáticos son los de mayor crecimiento en los últimos años, con una proyección cada vez mayor. La posibilidad de su comisión a través de Internet permite que sin mayores complicaciones, el delincuente pueda estar en un determinado país, utilizar servicios de otro, para finalmente atacar a una o más víctimas de un tercer país interviniente. Esta característica de trasnacionalidad demanda un desafío para el Derecho y en especial para los sistemas jurídicos penales, que deben concebir la necesidad de ciertos niveles mínimos de coordinación, que permitan un combate eficaz de este tipo de actividad delictiva. En este marco, la presente investigación tiene por objeto analizar la situación de los delitos informáticos en la región, en su aspecto material sustantivo, a través de un desarrollo de derecho comparado sobre los diferentes países de Latinoamérica. Como metodología, se ha trabajado en la búsqueda y recolección de la legislación vigente en cada país, destacando sus características generales. Desde allí, previa determinación del alcance, se ha configurando la realización de un cuadro comparativo que permite identificar qué países poseen sanción penal de los delitos informáticos más comunes. A modo de conclusión se lograron obtener estadísticas actualizadas con un ranking de países de acuerdo al estado de situación en la regulación penal de los delitos informáticos más importantes, así como la lista de delitos informáticos menos sancionados.

Palabras Claves: Delitos informáticos, cibercrimen, legislación, derecho comparado, Latinoamérica.

Introducción

Las actividades informáticas delictivas están en crecimiento a nivel global, incluyendo a América Latina [1].

El incremento de la delincuencia informática encuentra algunas de sus respuestas en una gran variedad de factores, cuyo desarrollo ya ha sido trabajado ampliamente por la doctrina [2]. El incremento de tecnología disponible, tanto para el delincuente como las víctimas, combinado con el escaso conocimiento o información sobre cómo protegerse de los posibles delitos que se pueden sufrir a través de las nuevas tecnologías, otorga a los delincuentes las llaves a las puertas de un inmenso campo fértil de potenciales víctimas de ataques.

Por otro lado, el crecimiento sostenido del mercado negro de la información [3], funciona como motor que impulsa una importante masa de ataques informáticos, principalmente destinados a obtener bases de datos con información personal.

De acuerdo a uno de los estudios de mayor relevancia mundial en delitos informáticos [4], en el cuál se han entrevistado más de 13.000 adultos en 24 países, para el año 2012, se calculó que los costos directos asociados con los delitos informáticos que afectan a los consumidores en el mundo ascendieron a US$ 110.000 billones en doce meses. El mismo estudio revela que por cada segundo 18 adultos son víctimas de un delito informático, lo que da como resultado más de un millón y medio de víctimas de delitos informáticos cada día, a nivel mundial.

Entre los desafíos citados anteriormente, uno de los más importantes es el hecho que este tipo de delitos pueden ser cometidos sin respetar barreras geográficas o jurisdiccionales. En este sentido, cualquier delincuente informático puede operar acciones desde un determinado lugar, conectarse a sistemas o equipos en otra parte y finalmente atacar datos o sistemas ubicados en otro lugar. La cadena puede tener indeterminadas variables dependiendo de la complejidad del ataque y de los

conocimientos del delincuente. Si bien esta situación no sucede en todos los casos, es relativamente sencillo realizar estos ataques en la actualidad para personas con conocimientos en informática. Esto representa para el Derecho un verdadero desafío a vencer.

Manuel Castells [5], en ocasión de un discurso del 2001, y hablando del "caos" positivo que Internet genera en la comunicación, dijo: "Técnicamente, Internet es una arquitectura de libertad. Socialmente, sus usuarios pueden ser reprimidos y vigilados mediante Internet. Pero, para ello, los censores tienen que identificar a los trasgresores, lo cual implica la definición de la trasgresión y la existencia de técnicas de vigilancia eficaces. La definición de la trasgresión depende, naturalmente, de los sistemas legales y políticos de cada jurisdicción. Y aquí empiezan los problemas. Lo que es subversivo en Singapur no necesariamente lo es en España". En seguida citó el ejemplo de cuando en 2000 un sitio Web de EE.UU. organizó la venta de votos de personas ausentes, hecho que representaba un delito electoral en ese país. Pero la Web se mudó a Alemania, donde ese hecho ya no podía ser perseguido por las leyes de ese país.

En consecuencia, una importante cantidad de grupos de delincuentes informáticos, organizan sus ataques desde lugares con poca o nula legislación en la materia, o bien, en aquellos países que aún teniendo legislación al respecto, no poseen un adecuado sistema para la detección y persecución eficaz de este tipo de delitos. Un ejemplo de ello fue el caso de un ataque de tipo viral que costó a empresas norteamericanas miles de millones de dólares, el cuál fue atribuido por el FBI a un estudiante en Filipinas al que no se lo pudo acusar de crimen alguno. Rápidamente el gobierno filipino dispuso legislación para combatir el crimen cibernético con el objetivo de evitar futuros inconvenientes [6].

En un contexto de incremento de la ciberdelincuencia organizada a nivel mundial, los llamados "paraísos legales informáticos", son los considerados al momento de ejecución de estas actividades.

En palabras del Dr. Marcelo Riquert [7], habida cuenta de las posibilidades que brindan las nuevas tecnologías de la comunicación y la aparición en escena de un nuevo espacio, el virtual o ciberespacio, en materia de delincuencia, facilitando la afectación de bienes jurídicos a una distancia y con una velocidad impensadas, resulta un lugar común la afirmación de estar en presencia de una problemática frente a la que el proceso de homogeneización legislativa y de cooperación en los ámbitos sustantivos y adjetivos, es una necesidad ineludible si se quiere evitar la existencia de "paraísos" de impunidad.

En este marco, la presente investigación tiene por objeto analizar la situación de los delitos informáticos en la región, en su aspecto material sustantivo, a través de un desarrollo de derecho comparado sobre los diferentes países de Latinoamérica.

Elementos del Trabajo y metodología

En cuanto a la metodología, se ha trabajado inicialmente en la recolección de la legislación aplicable en cada uno de los países pertenecientes a Latinoamérica, más precisamente de los siguientes países que se detallan a continuación por orden alfabético: Argentina, Bolivia, Brasil, Chile, Colombia, Costa Rica, Cuba, Ecuador, El Salvador, Guatemala, Haití, Honduras, México, Nicaragua, Panamá, Paraguay, Perú, Puerto Rico, República Dominicana, Uruguay y Venezuela.

Si bien se ha intentado analizar la mayor cantidad de los países de la región señalada, algunos de ellos han debido ser excluidos del estudio.

Entre los diferentes límites fijados en los alcances de la investigación, se debe destacar que la misma recoge solamente la normativa vigente en países latinoamericanos en los aspectos de derecho

sustantivo, no considerando dentro de los objetivos aquellos referidos al ámbito del derecho procesal penal.

A modo genérico, se ha utilizado como recurso de normativas la biblioteca digital del Departamento de Cooperación Jurídica, dependiente de la Secretaría de Asuntos Jurídicos, de la Organización de los Estados Americanos [8], en la cuál existe una sección dedicada exclusivamente al estudio de los Delitos Cibernéticos.

En cada uno de los países se ha consultado y analizado la normativa específica (en caso de existir) y en sus códigos penales vigentes, ya que variadas ocasiones, aún no existiendo una legislación especial o reforma dedicada a la materia, se encontraron que los delitos analizados pueden ser sancionados por los tipos penales "clásicos".

Como consecuencia de este trabajo, se construyó un cuadro de situación con una breve descripción del marco jurídico encontrado en cada país, los que han sido condensados en la Tabla Nº 1 expuesta dentro del apartado de los resultados.

Posteriormente, se ha realizado un análisis de cada una de esas normativas, configurando la realización de un cuadro comparativo que permite identificar a los países que poseen sanción penal para determinadas acciones delictuales informáticas. Son determinadas, puesto que si bien el trabajo completo incluye el relevamiento de todas las figuras penales sobre delitos informáticos vigentes en cada país, con el objetivo de poder distribuir cuantitativamente los resultados de este análisis, se ha procedido a segmentar esta clasificación, publicándose en el presente estudio, aquellos delitos propuestos como obligatorios en el Capítulo II (Medidas que deben ser adoptadas a nivel nacional), Sección 1 (Derecho penal material) de la Convención sobre Cibercriminalidad de Budapest [9]. Se destaca que más allá de la obligatoriedad inicial, la Convención permite aplicar algunas reservas sobre algunos artículos.

Dicha decisión ha sido tomada bajo el razonamiento que la citada Convención es una de las más trabajadas a nivel internacional en la materia. La misma fue firmada en Budapest en 2001, entró en vigencia el 1o de julio de 2004 y en su redacción participaron los 41 países miembros del Consejo de Europa, junto a otros Estados no miembros como Estados Unidos, Canadá, Japón y Sudáfrica. El objetivo de esta convención es recurrir a la colaboración internacional entre países, de manera de se establezca que una conducta lesiva sea delito en cada jurisdicción. Así, no obstante se mantengan y se respeten las legislaciones locales, los Estados deben definir delitos informáticos basados en un modelo común.

Concluida la digresión, la decisión sobre la segmentación de los resultados encuentra fundamento en que la cantidad de delitos informáticos tipificados difiere en cantidad de acuerdo al nivel de desarrollo legislativo de cada país. Ergo, en algunos Estados, es posible encontrar legislación moderna (últimos 5 años), en las cuáles ya se consideran sanciones penales para conductas que no eran conocidas, o al menos no habían alcanzado el nivel de intensidad en la región para ser considerados como ataques informáticos especiales. Por citar un ejemplo, en algunos de los países es posible encontrar más de 15 figuras penales relativas a los delitos informáticos. En consecuencia, y teniendo en consideración las limitaciones de espacio de la presente investigación, se ha decidido optar por la divulgación de sólo una parte de los resultados obtenidos, siendo estos restringidos a un cuadro de derecho comparado sobre los delitos informáticos considerados entre los artículos 2 y 9 de la Convención de Cibercriminalidad de Budapest. A continuación, se listan los tipos penales considerados como delitos informáticos para la presente investigación: Acceso ilícito (art. 2); Interceptación ilícita (art. 3); Atentados contra la integridad de los datos (art. 4); Atentados contra la integridad del sistema (art. 5); Abuso de

equipos (art. 6); Falsedad Informática (art. 7); Estafa Informática (art. 8); Infracciones relativas a la pornografía infantil (art. 9).

Es necesario destacar que no ha sido incluida la consideración del artículo 10 de la Convención de Cibercriminalidad de Budapest. Este artículo regula aquellas infracciones vinculadas a los atentados a la propiedad intelectual y a los derechos afines, y su exclusión ha sido decidida toda vez que ello implicaba un desarrollo aún más complejo en relación a la investigación de las legislaciones de cada país, ya que implicaba el agregado de normativa relativa a propiedad intelectual.

Dicha explicación sirve parcialmente como base para fundamentar la inclusión del artículo 9, relativo a la sanción de la pornografía infantil. Si bien el delito clásico también es materia de normativa especial, aquí se puede observar que muchas normativas relativas a los delitos informáticos lo han considerado como propio por considerarlo como una manifestación especial de la problemática impulsada por las nuevas tecnologías. De acuerdo al Protocolo Facultativo de la Convención sobre los derechos del niño, relativo a la venta de niños, la prostitución infantil y la utilización de niños en la pornografía [10], en su Art. 2º, inc. C, se establece que "por pornografía infantil se entiende toda representación, por cualquier medio, de un niño dedicado a actividades sexuales explícitas, reales o simuladas, o toda representación de las partes genitales de un niño con fines primordialmente sexuales".

Para estos casos, se ha trabajado como material de referencia un cuadro comparativo latinoamericano, realizado por el Ministerio de Justicia y Derechos Humanos de Argentina, con colaboración de UNICEF [10].

Resultados

Como producto de la presente investigación, se han elaborado cuatro tablas con los resultados obtenidos.

En la Tabla Nº 1, se puede observar la primera etapa de los resultados, indicándose por país, la legislación vigente y pertinente en materia de delitos informáticos, junto a un breve resumen de las observaciones realizadas sobre el marco jurídico aplicable.

La Tabla Nº 2 dispuesta a continuación, es producto del análisis de las normativas citadas, de acuerdo a la metodología y los criterios ya desarrollados en el apartado correspondiente. Dicho cuadro expresa la situación para cada uno de los países, y para cada uno de los delitos informáticos considerados en la investigación, indicándose si se ha encontrado o no una sanción penal que los reprima, y en su caso, cuál sería el artículo aplicable para esa conducta.

Si bien la investigación en toda su extensión incluye los textos completos de cada uno de los artículos señalados en el cuadro, por cuestiones prácticas de la extensión máxima permitida oficialmente por la organización de este Congreso, no ha sido posible su incorporación, dejándose solamente indicando el artículo.

Posteriormente, y basados en los resultados de las primeras dos tablas, se han generado otras dos tablas a partir de cálculos estadísticos.

Así, en la Tabla Nro. 3, se calcularon las estadísticas que indican el porcentaje de los países que aún no tienen sanción penal según cada delito informático analizado.

Finalmente, en la Tabla Nro. 4, se han elaborado las estadísticas que expresan, de acuerdo a cada país, el nivel de protección jurídica penal en relación a los delitos informáticos considerados en el presente trabajo.

País	Legislación	Características Generales
Argentina	Código Penal, Ley 26.388 (2008), Ley 25.326 (2000)	A partir de Junio de 2008, la Ley 26.388 conocida como la “ley de delitos informáticos” ha incorporado y realizado una serie de modificaciones al Código Penal argentino. Es decir, la misma no regula este tipo de delitos en un cuerpo normativo separado del Código Penal (CP) con figuras propias o independientes, sino que dicha ley modifica, sustituye e incorpora figuras típicas a diversos artículos del CP actualmente en vigencia. Se modificó el Epígrafe del Capítulo III cuyo nuevo título es "Violación de Secretos y de la Privacidad", Los artículos que modifica o agrega son: 128, 153, 153 bis, 155, 157, 157 bis, 173, 183, 184, 197, 255. El art. 157 bis ya había sido incorporado por la Ley 25.326 de Protección de Datos Personales (2000) pero fue modificado por la Ley 26.388.
Bolivia	Código Penal, Ley 1.768 (1997), Ley 3325 (2006)	La Ley 1.768 realiza una reforma general al Código Penal. Allí incorpora como Capítulo XI, del Título XII, del Libro Segundo del Código Penal, el de "DELITOS INFORMÁTICOS". Dentro de este capítulo, se incorporan 2 artículos: 363 bis y ter, en cuyos textos se tipifica algunos delitos informáticos.
Brasil	Ley 12.737 (2012), Ley 11.829 (2008)	La Ley 12.737 es una ley reciente (año 2012), en la cuál se dispone la tipificación criminal de los delitos informáticos y otras providencias. En su regulación incorpora modificaciones para los artículos 154-A, 154-B, 266 y 298. Por su parte, la Ley 11.829 regula el Estatuto de la Niñez y la Adolescencia, para mejorar la lucha contra la producción, venta y distribución de pornografía infantil, así como tipificar como delito la adquisición y posesión de dicho material y otros comportamientos relacionados con la pedofilia en Internet.
Chile	Ley 19.223 (1993), Ley 20.009 (2005), Ley 18.168 (2002)	La Ley 19.223 es una ley “Relativa a Delitos Informáticos” de acuerdo a su propio título, donde regula cuatro artículos, desde los cuáles se tipifican varios delitos informáticos. La Ley 20.009 regula la responsabilidad para el caso de robo, hurto o extravío de tarjetas de crédito, en cuyo texto se sancionan algunas conductas relacionadas con estos aspectos. La Ley 18.168 (modificada por diferentes normativas) regula de manera general las telecomunicaciones, incorporando algunos tipos penales sobre la interferencia o captación ilegítima de señales de comunicación.
Colombia	Ley 1.273 (2009), Ley 1366 (2009)	La ley 1.273, de reciente sanción legislativa (año 2009), modifica el Código Penal, creando un nuevo bien jurídico tutelado denominado "de la protección de la información y de los datos”. Se afirma que dicha normativa busca preservar integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones. A través de esta incorporación, suma el CAPITULO I, titulado "De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos", a partir del cuál regula una serie de artículos penales que van desde el artículo 269A hasta el artículo 269J. Adicionalmente se incorpora el artículo 58, considerando como agravante general “si la realización de alguna de las conductas punibles, se realicen utilizando medios informáticos, electrónicos o telemáticos”.
Costa Rica	Ley 9.048 (2012)	La Ley 9048 es una modificación importante del Código Penal de este país. Inicialmente reforma los artículos 167, 196, 196 bis, 214, 217 bis, 229 bis y 288 de la Ley Nº 4573. Por otro lado adiciona el inciso 6) al artículo 229 y un artículo 229 ter. Finalmente modifica la sección VIII del título VII del Código Penal, titulándolo "Delitos informáticos y conexos", donde regula desde el art. 230 hasta el art. 236. En esta modificación bastante integral, agrega una importante cantidad de delitos informáticos al Código Penal, desde los más tradicionales hasta algunos más modernos como la Suplantación de Identidad (art. 230) o el espionaje cibernético (art. 231).

País	Legislación	Características Generales
Cuba	Resolución 204/96, Resolución 6/96, Decreto Ley 199/99, Ley de Soberanía Nacional	En este país se ha podido acceder a la Resolución 204/96, la cuál dispone el Reglamento sobre la Protección y Seguridad Técnica de los Sistemas Informáticos, junto a la Resolución 6/96 que pone en vigor el Reglamento sobre la Seguridad informática, con medidas establecidas para la protección y seguridad del Secreto Estatal. Por otro lado, el Decreto Ley 199/99 define como objetivo fundamental establecer y regular el Sistema para la Seguridad y Protección de la Información Oficial. Si bien no existe legislación específica para delitos informáticos, se han encontrado distintas posturas en la doctrina. Por un lado, se opina sobre la necesidad de regulación especial en la materia, y por otro se considera que por la forma en que están redactados algunos delitos y por la filosofía del Código cubano de sancionar por los valores atacados y por los medios empleados, los tipos penales ya existentes son aplicables.
Ecuador	Ley Nº 67/2002 (2002)	La Ley No. 67/2002 regula el Comercio Electrónico, Firmas y Mensajes de datos. En dicha norma, dentro del Capítulo I del Título V, titulado "DE LAS INFRACCIONES INFORMÁTICAS", el art. 57 afirma que "Se considerarán infracciones informáticas, las de carácter administrativo y las que se tipifican, mediante reformas al Código Penal, en la presente ley." En artículo siguiente, agrega y modifica varios artículos al Código Penal, incorporando diferentes figuras de delitos informáticos.
El Salvador	Decreto 1030 / 1997 (1997)	No se ha encontrado legislación específica en la materia. No obstante, posee la adaptación de ciertos delitos clásicos a las nuevas modalidades informáticas. Entre ellos, se pueden mencionar los artículos siguiente: 172, 185, 186, 190, 208 No.2, 216, 222 No. 2, 228, 230, 231 y 302 del Código Penal de El Salvador.
Guatemala	Código Penal	Dentro del Código Penal, posee el Capítulo VII, titulado "De los delitos contra el derecho de autor, la propiedad industrial y delitos informáticos". Allí incorpora distintos artículos penales para las figuras de los delitos informáticos, en especial desde el artículo 274 inc. A hasta el inciso G.
Haití	-	No se ha encontrado legislación sobre la materia.
Honduras	Código Penal; Decreto 144/83	Si bien no se ha encontrado legislación especial en la materia, si posee la adaptación de ciertos delitos clásicos a las nuevas modalidades informáticas. Entre ellos podremos encontrar los artículos 214, 215, 223 y 254. Por otro lado, el Decreto 144/83 incorpora algunos delitos para tipificar la pornografía infantil a través del art. 149 y sus incisos al Código Penal.
México	Reforma 75 del Código Penal Federal (1999)	Mediante reformas se crearon en el Código Penal Federal, los artículos 211 bis 1 al 211 bis 7, que buscaron tipificar los delitos informáticos clásicos teniendo en consideración la fecha de su incorporación. Se destaca la diferente que atentan contra los sistemas de cómputo que pueden o no, ser parte del sector financiero mexicano. Es importante destacar, que algunos Estados Mexicanos tienen además sus propias normas penales, incorporando otros delitos informáticos no analizados en este trabajo.
Nicaragua	-	No se ha encontrado legislación sobre la materia.

País	Legislación	Características Generales
Panamá	Código Penal y sus reformas; Ley 51 (2008)	No se ha encontrado legislación especial en la materia. No obstante, posee la adaptación de ciertos delitos clásicos a las nuevas modalidades informáticas. Entre ellos pueden citarse los artículos 162 a 165, 180, 184, 185, 220, 237, 260, 283 a 286 y 421. Adicionalmente posee la Ley 51/2008 de Firma Electrónica, en la cuál se regula penalmente sobre la falsificación de documentos.
Paraguay	Código Penal – Ley 1.160 (1997), Ley 2.861	No se ha encontrado legislación especial referida a la materia. Sin embargo, a partir de distintas reformas al Código Penal Paraguayo, se han adaptado algunos delitos para la posibilidad de comisión a través de las nuevas tecnologías y en otros casos se ha incorporado tipos penales específicos (como el caso del art. 175 de Sabotaje de Computadoras). Los artículos son 144, 146, 173 a 175, 188, 189, 220, 239, 248 y 249.
Perú	Ley 27.309 (2000), Ley 28.251 (2004)	La Ley 27309 incorpora al Código Penal del Perú los Delitos Informáticos, a través de un artículo único que modifica el Título V del Libro Segundo del Código Penal, promulgado por Decreto Legislativo No 635, introduciendo allí los artículos 207 – A – B y C y 208. En otro orden, la Ley 28.251 actualizó e incorporó distintos delitos contra la integridad sexual, entre ellos, tipificando la pornografía infantil, a través de la modificación del art 183-A. Además Perú posee la Ley 28.493 (2005) que regula el uso del correo electrónico no solicitado (spam), sin embargo en la misma no incluye ningún tipo de sanción penal.
Puerto Rico	Ley 146/2012 (Código Penal) + Ley de Espionaje Cibernético 1165 (2008)	No se ha encontrado legislación especial al respecto. Sin embargo, Puerto Rico ha optado por la modificación de los tipos penales clásicos, a fin de adaptarlos para su comisión a través de las nuevas tecnologías. Por otro lado, a través de la Ley de Espionaje Cibernético Nº 1165/2008 si se han incorporado algunos delitos penales especiales para estas figuras relacionados con el espionaje.
República Dominicana	Ley Nº 53-07 (2007)	Posee una Ley Especial contra Crímenes y Delitos de Alta Tecnología. Dicha norma regula una parte general, conteniendo algunos principios y conceptos, y posteriormente tipifica los delitos informáticos según el bien jurídico afectado. Además, incluye un capítulo dedicado al aspecto procesal penal, así como en la propia normativa genera un órgano encargado de la recepción de denuncias, investigación y persecución de los delitos informáticos.
Uruguay	Ley 18.600 (2009), Ley 17.520 (2002), Ley 17.815 (2004), Ley 18.383 (2008), Ley 18.515 (2009)	Si bien no se ha encontrado legislación especial en la materia, se han encontrado diferentes normativas parcialmente aplicables a la materia. El art. 7 de la Ley 17.815, afirma que "constituye delito de comunicación la comisión, a través de un medio de comunicación, de un hecho calificado como delito por el Código Penal o por leyes especiales.", permitiendo así la aplicación de los tipos clásicos del CP. La Ley N° 17.520, penaliza el uso indebido de señales destinadas exclusivamente a ser recibidas en régimen de abonados. La Ley Nº 17.815 regula la violencia sexual, comercial o no comercial cometida contra niños, adolescentes e incapaces que contenga la imagen o cualquier otra forma de representación.
Venezuela	Gaceta Oficial Nº 37.313 (2001)	Posee una ley especial sobre Delitos Informáticos. Contiene 33 artículos y están clasificados en 5 Capítulos a saber: Contra sistemas que utilizan TI; Contra la propiedad; Contra la privacidad de las personas y las comunicaciones; Contra niños y adolescentes; Contra el orden económico.

Tabla Nro 1. Cuadro de Derecho Comparado sobre Delitos Informáticos en Latinoamérica.

País	Acceso ilícito	Interceptación ilícita	Atentado contra la integridad de los datos	Atentado contra la integridad del sistema	Abuso de los dispositivos	Falsedad informática	Fraude o estafa informática	Pornografía infantil
Argentina	Art. 153 bis	Art. 153	Art. 183 2do párrafo	Art. 183 2do párrafo y Art. 197.	No encontrado..	Art. 292	Art. 173 inc. 16	Art. 128
Bolivia	Art. 363 ter	No encontrado.	Art. 363 ter	No encontrado.	No encontrado.	No encontrado.	Art. 363 bis	Art. 281 quater
Brasil	Art. 154A	No encontrado.	Art. 154A.	Art. 266 Inc. 1	Art. 154A Inc. 1	No encontrado..	No encontrado.	Art. 241 A y B Ley 11.829
Chile	Art.2	Art.2	Art. 3	Art. 1	No encontrado.	No encontrado.	No encontrado.	Art. 374 bis CP
Colombia	Art. 269 A	Art. 269 C	Art. 269 D	Art. 269 B y D	No encontrado.	No encontrado.	Art. 269J	Art. 218
Costa Rica	Art. 196	Art. 196	229 bis	Art. 229 ter	No encontrado.	217 bis	217 bis	Art. 167
Cuba	No encontrado.	No encontrado.	No encontrado.	No encontrado.	No encontrado.	No encontrado.	No encontrado.	No encontrado.
Ecuador	Art. 202.1	No encontrado..	Art. 415.1	No encontrado.	No encontrado.	Art. 353.1	Art. 563 inc. 2	Ley 2005-2 Art. 18
El Salvador	Art. 184 y 185	Art. 186	Art. 221 y 222	No encontrado.	No encontrado.	No encontrado.	Art. 216 inc. 5	Art. 172 y 173 A
Guatemala	Art. 274 F	No encontrado.	Art. 274 A	Art. 274 B	No encontrado.	Art. 274 E	No encontrado.	No encontrado.
Haití	No encontrado.	No encontrado.	No encontrado.	No encontrado.	No encontrado.	No encontrado.	No encontrado.	No encontrado.

País	Acceso ilícito	Interceptación ilícita	Atentado contra la integridad de los datos	Atentado contra la integridad del sistema	Abuso de los dispositivos	Falsedad informática	Fraude o estafa informática	Pornografía infantil
Honduras	Art. 214	Art. 214	Art. 254 2do párrafo	No encontrado.	No encontrado.	No encontrado.	No encontrado.	Art. 149D
México	Art. 211 bis 1	Art. 168 bis	Art. 211 bis 1	Art. 167, 211 bis 2 y 3	Art. 424 bis	No encontrado.	No encontrado.	Art. 202
Nicaragua	No encontrado.	No encontrado.	No encontrado.	No encontrado.	No encontrado.	No encontrado.	No encontrado.	No encontrado.
Panamá	Art. 289	Art. 290	Art. 290	Art. 290	No encontrado.	Art. 366 y Art. 61 Ley 51/2008	Art.. 226 y 243	Art. 184 y 185
Paraguay	Art. 144 y 146	Art. 144 y 146	Art. 174	Art. 175 y 220	No encontrado.	Art. 188	Art. 188	Ley 2861 – Art. 1, 2 y 6
Perú	Art. 207 A	Art. 207 A	Art. 207 B	Art. 207 B	No encontrado.	No encontrado.	No encontrado.	Ley 28.251 – Art. 183 A
Puerto Rico	Art. 171	Art. 171	Art. 172 y 198	Art. 186 y Art. 240	Art. 218	Art. 213 y Art. 217	Art. 203	Art. 146 y 147
República Dominicana	Art. 6 y 7	Art. 9	Art. 10	Art. 11	Art. 8	Art. 18	Art. 14 y 15	Art. 24
Uruguay	No se encontró legislación.	Ley Nro. 17.520 – Art. 1	Ley 18.600 Art. 4	Art. 217 CP (Mod. Por Ley 18.383).	Ley Nro. 17.520 Art. 1	No encontrado.	No encontrado.	Ley 17.815. Art. 2
Venezuela	Art. 6	Art. 21	Art. 7 2do párrafo	Art. 7. 1er párrafo	Art. 10 y 19	Art. 12	Art. 14	Art. 24

Tabla Nro 2. Cuadro de Derecho Comparado clasificado de acuerdo a los delitos informáticos analizados, en países de Latinoamérica.

Delito Informático	%
Acceso Ilícito	19%
Interceptación Ilícita	33%
Atentado contra la integridad de los datos	14%
Atentado contra la Integridad del sistema	33%
Abuso de los dispositivos	71%
Falsedad Informática	57%
Fraude o Estafa Informática	48%
Pornografía Infantil	19%

Tabla Nro 3. Estadísticas que indican el porcentaje de los países que aún no tienen sanción penal según cada delito informático analizado.

País	%
Argentina	88%
Bolivia	50%
Brasil	63%
Chile	63%
Colombia	75%
Costa Rica	88%
Cuba	0%
Ecuador	63%
El Salvador	63%
Guatemala	50%
Haití	0%
Honduras	50%
México	75%
Nicaragua	0%
Panamá	88%
Paraguay	88%
Perú	63%
Puerto Rico	100%
República Dominicana	100%
Uruguay	63%
Venezuela	100%

Tabla Nro 4. Estadísticas que expresan el nivel de sanción penal de los delitos analizados, por país.

Discusión

Para comenzar, es necesario destacar el concepto de delito informático sobre el cuál se ha trabajado. El Dr. Julio Tellez Valdes [11] conceptualiza al "delito informático" en forma típica y atípica, entendiendo por la primera a "las conductas típicas, antijurídicas y culpables en que se tienen a las computadoras como instrumento o fin" y por las segundas "actitudes ilícitas en que se tienen a las computadoras como instrumento o fin".

Tomamos este concepto (existen otros tantos en la doctrina, la cual aún no considera resuelta la cuestión) toda vez que su simple clasificación entre típicos y atípicos es útil a los fines de este trabajo. Aquí, solamente se considera como delito informático a aquellos dentro de las categorías de los típicos, es decir, con sanción penal.

Párrafo aparte merecen los aspectos relativos a la interpretación sobre los tipos penales vigentes en cada país, en relación a su clasificación en las figuras ya presentadas. Por cuestiones atinentes a cada país en particular, su cultura jurídica penal en cuanto a la forma de redacción de los tipos penales, así como los diferentes bienes jurídicos que se protegen a través de ellos, hacen que las redacciones sean en algunos casos sustancialmente diferentes, incluso tratando de reprimir penalmente la misma conducta.

Este trabajo no pretende realizar algún tipo de análisis o crítica sobre dichas redacciones o técnicas legislativas utilizadas, toda vez que como ya se ha mencionado, excede por un lado los alcances de la investigación, y por otro, la misma responde a aspectos propios de cada país, de manera que merece su atención en ello.

No obstante lo ensayado, es necesario destacar que a fines de encasillar cada tipo penal dentro de algunas de las categorías propuestas, ha sido necesario realizar un trabajo de interpretación por parte del autor. En este sentido, se ha utilizado un criterio de interpretación amplio. Para ello, se ha considerado siempre que se conserven los esenciales de la actividad delictual en sí, no contemplando características secundarias o adicionales propias de cada código penal. Muchos artículos penales encontrados suelen tipificar más de una figura en su texto (en miras a la clasificación tradicional de los delitos informáticos). En conclusión, en aquellos casos donde podía existir una duda razonable sobre si la redacción alcanzaba o no a reunir todos los elementos necesarios para considerar que determinado delito se encontraba tipificado, se ha optado por una interpretación a favor del país analizado, considerando como positivo dicho caso (es

decir, que dicha acción se encuentra sancionada penalmente).
Vale un ejemplo para aclarar la teoría. El primer delito de la lista, corresponde al acceso ilícito. En la lista de países analizados, se pueden encontrar las más variadas posturas acerca de este delito. Por ejemplo, además de los elementos básicos (acceder sin consentimiento a un sistema o dato informático), Bolivia considera que debe existir perjuicio para un tercero. Algunos países como Argentina, exigen que el sistema o dato sea de acceso restringido. Otros como Chile, no lo mencionan. Colombia, expresa en su redacción que el sistema puede ser o no de acceso restringido. Costa Rica comienza afirmando que será delito si hay peligro para la intimidad o privacidad de un tercero. Y otra larga lista de características especiales, que como el lector podrá observar, un análisis técnico-jurídico riguroso sobre ellos es realmente interesante, pero cuya extensión excede los límites del presente trabajo. No obstante, dicho análisis será realizado a futuro.
Finalmente, una aclaración importante. No sería correcto considerar que los resultados expuestos en la Tabla Nº 2 permitan concluir que técnicamente un país determinado se encuentra o no en cumplimiento de las disposiciones materiales en materia penal que dispone la Convención de Cibercriminalidad de Budapest. Dicha afirmación encuentra fundamento en que, las figuras penales consideradas, si bien han sido tomadas de la citada Convención, ello no implica que se ha hecho un análisis pormenorizado de todos los requisitos que se establecen en cada artículo material penal de la misma. Los delitos informáticos considerados para el estudio sólo han sido tomados a modo de referencia, sin contrastar los requisitos técnicos legales que la Convención exige para considerarlos como correctamente tipificados.
Es decir, si bien es posible que los resultados arrojados por el estudio, indiquen una tendencia de dicho país sobre la situación penal material en relación a los delitos informáticos en relación a la Convención de Budapest (recordar no obstante la exclusión en el estudio del art. 10 ya desarrollada), ello no permite deducir que dicho país cumpla o no con los requisitos de la Convención, tarea que no ha sido objeto de la presente investigación.

Conclusiones

Los resultados del presente trabajo permiten llegar a dos tipos distintos de conclusiones. En el primer grupo, identificado desde un punto de vista cuantitativo, es posible concluir con la realización de un ranking de países de acuerdo al nivel de protección penal en relación a los delitos informáticos analizados (a través de la reorganización de los datos arrojados por la Tabla Nº 4).

Nº	País	%
1	Puerto Rico	100%
2	República Dominicana	100%
3	Venezuela	100%
4	Argentina	88%
5	Costa Rica	88%
6	Panamá	88%
7	Paraguay	88%
8	Colombia	75%
9	México	75%
10	Brasil	63%
11	Chile	63%
12	Ecuador	63%
13	El Salvador	63%
14	Perú	63%
15	Uruguay	63%
16	Bolivia	50%
17	Guatemala	50%
18	Honduras	50%
19	Cuba	0%
20	Haití	0%
21	Nicaragua	0%

Tabla Nro 5. Ranking de países con más sanción penal para los delitos informáticos considerados.

Por otro lado, esta vez a partir de la reorganización ascendente de los datos de la Tabla Nº 3, es posible determinar un ranking de los delitos informáticos con menor nivel de sanción penal en los países latinoamericanos.

Nº	Delito Informático	%
1	Abuso de los dispositivos	71%
2	Falsedad Informática	57%
3	Fraude o Estafa Informática	48%
4	Interceptación Ilícita	33%
5	Atentado contra la Integridad del sistema	33%
6	Acceso Ilícito	19%
7	Pornografía Infantil	19%
8	Atentado contra la integridad de los datos	14%

Tabla Nro 6. Ranking de los delitos informáticos menos sancionados penalmente en Latinoamérica.

De la misma, puede inferirse que los delitos informáticos más reconocidos como tales a nivel latinoamericano, son por un lado aquellos más tradicionales (atentado contra la integridad de los datos y acceso ilícito), y por otro, el delito de pornografía infantil, probablemente por la importancia del bien jurídico protegido.

En el otro grupo de conclusiones, en base a los resultados obtenidos, es posible afirmar:

a) Que, los países latinoamericanos presentan una falta de homogeneización en el ámbito sustantivo de la normativa penal aplicable a los delitos informáticos.

b) Que, los países latinoamericanos han optado por diferentes posturas en relación a sus formas de regular. Algunos han optado por la sanción de leyes especiales, donde en los casos más destacados (caso de República Dominicana) incorporan conceptos propios, principios, parte penal material, parte procesal penal, e incluso se han generado los organismos dedicados a su investigación y persecución. Otros tantos países (mayoría) han optado por modificaciones parciales a sus Códigos Penales vigentes, adaptando las figuras penales clásicas a fin de que sea posible su aplicación en los delitos informáticos.

c) Que la falta de armonización reconoce diferencias en dos niveles. En el primero de ellos, se puede observar diferencias entre los países sobre los criterios políticos para la consideración sobre si tal acción lesiva debe ser o no sancionada como delito penal. En un segundo nivel, dentro de aquellos países que han dado respuesta positiva al primer nivel, pueden observarse diferencias en cuanto a los criterios penales considerados como necesarios para la configuración del tipo.

d) Que se destaca la necesidad de mejorar los niveles de armonización y actualización legislativa en la materia, a fin de mitigar la existencia de paraísos legales en la región que favorezcan la ciberdelincuencia.

Referencias

[1] Norton, *Informe sobre delitos informáticos 2011*, URL: http://norton.com/cybercrimereport. - Las víctimas de los delitos informáticos aumentaron de un 10% a un 13% este año entre 2011 a 2012.

[2] Palazzi, Pablo Andrés, Delitos Informáticos, Ad-Hoc, Buenos Aires, 2000.

[3] Panda Security. *The Cyber-Crime Black Market*. 2011. Url: http://cybercrime.pandasecurity.com/ blackmarket. Consultado: 28/07/2013

[4] Symantec Corporation, *Informe de Norton sobre delitos informáticos* para el año *2012*, septiembre de 2012: http://www.norton.com/2012cybercrimereport

[5] "Internet, libertad y sociedad: una perspectiva analítica", Conferencia inaugural del curso académico 2001-2002 de la UOC.

[6] Phil Williams, "Organized Crime and Cybercrime: Synergies, Trends, and Responses", International Information Programs, Electronic Journal of the U.S. Department of State – August 2001 Volume 6, Number 2.

[7] Riquert, Marcelo Alfredo, "Estado de la Legislación contra la Delincuencia Informática en el Mercosur" (en línea), URL: http://www.pensamientopenal.com.ar/node/27142 Consulta: 25/07/13

[8] Portal Interamericano de Cooperación en Materia de Delito Cibernético. Organización de los Estados Americanos. Url: [http://www.oas.org/juridico/spanish/cybersp.htm]. Consultado: 29/07/2013

[9] Council of Europe. "Convenio de Cibercriminalidad de Budapest". Budapest, 23 de noviembre de 2001. http://www.coe.int/t/dghl/standardsetting/t-cy/ETS_185_spanish.PDF Consultado: 08/03/2012

[10] Protocolo Facultativo de la Convención sobre los derechos del niño relativo a la venta de niños, la prostitución infantil y la utilización de niños en la pornografía, Asamblea General de Naciones Unidas, 25/5/00

[11] Téllez Valdés, Julio, *Derecho Informático*, 3ª.ed., Ed. Mc Graw Hill, México, 2003, Pág. 8