Delitos Informáticos en Latinoamérica: Un estudio de derecho comparado. 2da. Parte.

Abog. Marcelo G. I. Temperini[1]

Abstract en Español. La expansión de los delitos informáticos no sólo puede advertirse del incremento en la cantidad de delitos cometidos, sino que además, los mismos son cada vez más variados y complejos. La combinación de la delincuencia con las posibilidades de las nuevas tecnologías, ha generado que muchos países latinoamericanos optaran por la generación de nuevas figuras penales de acciones relacionadas a la informática. El presente trabajo ofrece la segunda parte de un estudio cuyo objeto ha sido el análisis de la situación de los delitos informáticos en Latinoamérica, en su aspecto material sustantivo. A modo de resultado, se ha construido un cuadro comparativo (mapa) que permite identificar que delitos informáticos se encuentran tipificados penalmente en cada país abordado en el estudio. Debido a la extensión de los resultados, la primera parte sólo ha incluido la publicación de los delitos considerados como más comunes, de acuerdo a una interpretación basada en las recomendaciones del Convenio de Cibercriminalidad de Budapest. En esta ocasión, se presenta la continuación de dicha tarea, pretendiendo la publicación de la segunda parte del mapa de los delitos informáticos tipificados en Latinoamérica hasta la fecha. Las conclusiones incluyen nuevas estadísticas, que permitirán acceder a una perspectiva actualizada sobre la situación de la regulación penal sobre el cibercrimen en Latinoamérica.

Keywords: delitos informáticos, cibercrimen, derecho comparado, legislación, latinoamérica

1 Abogado (UNL). Doctorando CONICET con especialización en Delitos Informáticos. Co-Director de la Red Elderechoinformatico.com. Analista de Seguridad y CEO de AsegurarTe – Consultora en Seguridad de la Información. Contacto: mtemperini@asegurarte.com.ar

Introducción

De acuerdo a un informe [1] elaborado por la empresa Norton, las actividades informáticas delictivas están en crecimiento a nivel global, incluyendo por supuesto a América Latina. En las estadísticas citadas, las víctimas de los delitos informáticos aumentaron de un 10% a un 13% sólo entre el año 2011 a 2012. Tal como expresa Nir Kshetri en una de sus obras [2], "*El crecimiento meteórico del cibercrimen ha sido un tema de preocupación apremiante para nuestra sociedad*"[2]

Sin embargo, la expansión de los delitos informáticos no sólo puede advertirse en el incremento en la cantidad de delitos cometidos, sino que además, los mismos son cada vez más variados y complejos, dando lugar -en determinados casos que veremos- a tipos penales más específicos.

Las posibilidades que brindan las nuevas tecnologías, en combinación en con la "creatividad" de los delincuentes para engañar y atacar a sus víctimas, dan como resultado una gama compleja de acciones que pueden ser consideradas como delictuosas. En ese contexto, se inserta la multiplicidad de criterios político-criminales al momento de optar por la tipificación de dichas conductas, produciendo en consecuencia una amplia y variada gama de delitos informáticos tipificados a lo largo de Latinoamérica.

En palabras del Dr. Marcelo Riquert [3], *"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"*.

Este trabajo, apunta precisamente a determinar el nivel de homogeneización legislativa que existe en Latinoamérica en materia de delitos informáticos.

Primera parte

A fin de que el lector pueda comprender de mejor manera el estudio, daremos un breve repaso sobre los resultados expuestos en la primera parte de la investigación [4], publicada en el año 2013. Como ya hemos adelantado, su objeto de estudio ha sido 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. En esa oportunidad se ha publicado una primera tabla con el resultado de las legislaciones encontradas en los países que formaron parte del estudio. Por otro lado, se publicó el cuadro comparativo de los delitos considerados como "básicos", de acuerdo a una interpretación basada en las recomendaciones del Convenio de Cibercriminalidad de Budapest [5]. El presente

[2] Traducción propia, originalmente el autor expresó "*The meteoric rise in cybercrime has been an issue of pressing concern to our society*"."

trabajo, continúa dicha tarea a través de la segunda parte de dicha investigación, pretendiendo la publicación del resto del *"mapa"* de los delitos informáticos tipificados en Latinoamérica hasta la fecha.

Estadísticas en el cibercrimen

Si bien al comenzar el artículo, citamos una de las estadísticas más conocidas en el ámbito de la seguridad de la información, debemos realizar algunas consideraciones que estimamos pertinentes en relación a lo que observamos como uno de los desafíos a combatir en el problema de la cibercriminalidad.

La falta de estadísticas oficiales en la materia, es al menos para criterio de este autor, un aspecto sustancialmente problemático, toda vez que ello impide un trabajo serio de observación, análisis y elaboración de estrategias o planes de corto, mediano y largo plazo orientados a combatir el cibercrimen.

Para no extendernos demasiado en este punto, que será tema de estudio de otros trabajos, nos parece adecuado citar las reflexiones expresadas en el estudio sobre cibercrimen encargado por la Organización de Estados Americanos [6], en el cuál se reconoció que el cibercrimen ha crecido (entre 2011 y 2012) entre el 8 a 12 % en algunos países, y en el caso más extremo, de cerca del 40%. Más allá de la estadística, y en relación a la propia problemática de la recolección seria de datos que permitan analizar el estado de situación, el estudio afirma que "o*bviamente, los incidentes cibernéticos incluidos en los informes de los gobiernos de los Estados miembros de la OEA representan solamente una fracción del número total de incidentes y otras formas de delincuencia cibernética que se llevan a cabo en la región. Pero sigue siendo sencillamente imposible en este momento recopilar datos que permitan obtener una imagen verdaderamente exhaustiva y detallada de la extensión de todos estos incidentes y actividades en las Américas y el Caribe, o en cualquier otro sitio. Como ya dijimos, el intercambio de información dentro de los gobiernos —incluso aquellos con la capacidad más avanzada en materia de seguridad cibernética— sigue quedando corto, en gran parte debido a las realidades prácticas de que múltiples organizaciones tengan que responder simultáneamente a una gama de amenazas y blancos en constante evolución. Y muchas empresas privadas y otras entidades no gubernamentales siguen mostrándose reacias a reportar ataques o violaciones. Contabilizar el número de incidentes que afectan a los ciudadanos individuales plantea un desafío incluso mayor, en vista del porcentaje incluso más alto de ellos que pasan desapercibidos y no se reportan. Por último, la falta de colaboración generalizada y persistente entre las partes interesadas en todos los niveles dificulta todavía más recoger información sobre violaciones de datos."*

Internacionalidad de los delitos

Entre los diferentes desafíos inherentes o característicos de los delitos informáticos a nivel mundial, encontramos la posibilidad de que estos puedan ser cometidos sin respetar barreras geográficas o jurisdiccionales. Esto implica que cualquier delincuente informático puede ejecutar acciones desde un determinado lugar,

conectándose 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.

Sin dejar de destacar la importancia que representa, cabe destacar que el elemento de la internacionalidad en los delitos informáticos no es esencial, en consideración que el mismo puede perfeccionarse dentro de la misma red local, en la misma ciudad, Provincia o País. Sin embargo, la inexistencia de barreras geográficas en Internet, permite que los mismos delitos sean realizados desde cualquier lugar del mundo, hacia cualquier otro lugar del mundo.

A los fines de la investigación y persecución de este tipo de delitos, este aspecto puede convertirse en un verdadero obstáculo cuando el delincuente utiliza sus conocimientos para ocultar o simular el verdadero lugar desde donde se realiza el ataque. Esto es posible con una relativa[3] facilidad técnica, donde por ejemplo, un delincuente informático de Argentina, pueda utilizar un servidor *proxy*[4] ubicado en otro país, para atacar un objetivo argentino. A nuestro criterio, esta realidad representa para el Derecho un verdadero desafío a vencer.

La OEA y la lucha contra los delitos cibernéticos

En la Resolución AG/RES. 2004 [7] que plantea la Estrategia de Seguridad Cibernética por parte de la Organización de los Estados Americanos (OEA), se reconoce "*La necesidad de crear una red interamericana de alerta y vigilancia para diseminar rápidamente información sobre seguridad cibernética y responder a crisis, incidentes y amenazas a la seguridad de las computadoras y recuperarse de los mismos*". En el citado documento, existe un apartado especial sobre la "*Redacción y promulgación de legislación en materia de delito cibernético y mejoramiento de la cooperación internacional en asuntos relacionados con delitos cibernéticos"*.

Las afirmaciones realizadas en este capítulo son contundentes: "*Si no cuentan con leyes y reglamentos adecuados, los Estados Miembros no pueden proteger a sus ciudadanos de los delitos cibernéticos. Además, los Estados Miembros que carecen de leyes y mecanismos de cooperación internacional en materia de delito cibernético corren el riesgo de convertirse en refugios para los delincuentes que cometen estos delitos."*

Estas iniciativas de respaldo a la Estrategia Interamericana Integral de Seguridad Cibernética han sido realizadas en el marco de las recomendaciones formuladas por el Grupo de Expertos [8]. En relación a la internacionalidad de los delitos informáticos, la resolución reconoce que "*La naturaleza sin fronteras de las redes mundiales significa que un único acto delictivo relacionado con una computadora puede afectar o dirigirse a computadoras en varios países"*.

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.

---

3 Considerando que no son necesarios conocimientos avanzados en informática para poder realizarlo.

4 La palabra en inglés "*proxy*" significa "*intermediario"* en español.

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, por razones de extensión.

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 general, 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 [9], 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 algunos de los delitos analizados pueden ser sancionados a través de la aplicación de los tipos penales “clásicos”.

A partir del análisis de cada una de esas normativas, se ha configurado la realización de un cuadro comparativo que permite identificar a los países que poseen sanción penal para determinados delitos informáticos.

Construcción de categorías

Entre las distintas precisiones que son necesarias de realizar de acuerdo a la ambiciosa tarea planteada en la investigación, es necesario adelantar al lector que la variedad de denominaciones para los delitos por un lado, sumado a la multiplicidad de formas de criminalización de las conductas analizadas que se dan en los distintos países incluídos en el estudio, han representado un problema al momento de la construcción del cuadro comparativo o mapa de delitos.

A fines de adoptar un criterio para la construcción de estas categorías, tomamos el concepto de delito informático desarrollado por el Dr. Julio Tellez Valdes [10], quien los clasifica en sus formas 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”*. Si bien existen otros tantos conceptos en la doctrina, tomamos el citado toda vez que su simple clasificación entre típicos y atípicos es útil a los fines de este trabajo. Aquí, solamente consideraremos como “delito informático” a aquellos dentro de las categorías de los típicos, es decir, como una conducta penalmente sancionada.

Para comenzar, debemos destacar que este trabajo no pretende realizar un análisis exhaustivo de todos y cada uno de los delitos informáticos tipificados en cada uno de los países que forman parte del estudio, toda vez que ello hubiese sido de realización imposible para este autor (al menos en plazos razonables). En conclusión, la primera decisión fue adoptar tipos penales informáticos reconocidos[5], que sean útiles como denominadores comúnes que hagan a los fines del objeto de estudio.

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.

No se pretende en este estudio 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, debemos expresar que con la finalidad de "categorizar" 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, teniendo en consideración la existencia de los elementos esenciales de cada figura en sí, no contemplando características secundarias o adicionales propias de cada código penal. Es decir, 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).

A continuación, se listan los tipos penales considerados como delitos informáticos para la presente investigación: Violación de Datos Personales; Difusión de Malware; Hurto Informático; Difusión maliciosa de información; Suplantación de Identidad Digital; Grooming; Captación o venta ilegítima de datos; Carding; Espionaje Informático; Violación a la Intimidad. En una última columna, se ha también dejado constancia de aquellas normativas que poseen algún tipo de regulación sobre agravantes generales para este tipo de delitos, por considerarlo como un aspecto de interés a los fines del presente trabajo.

Por último, 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.

5 Sólo a título de ejemplo, citamos figuras especiales encontradas, tales como la extorsión informática en Costa Rica, la difamación o injurias electrónicas en República Dominicana, o el delito de oferta electrónica engañosa en Venezuela. Dada esta variedad de tipos penales, se ha optado por seleccionar una gama de delitos informáticos más reconocidos a nivel general.

Resultados alcanzados

País	Violación de Datos Personales	Difusión de Malware	Hurto Informático	Difusión maliciosa de información	Suplantación de Identidad Digital	Grooming	Captación o venta ilegítima de datos	Carding	Espionaje Informático	Violación a la Intimidad	Agravantes especiales
Argentina	Art. 157 bis	Art. 183 2do párrafo	No encontrado	Art. 155	No encontrado	Art. 131	No encontrado	No encontrado	No encontrado	No encontrado	No encontrado
Bolivia / Haití / Paraguay	No encontrado	No encontrado	No encontrado	No encontrado	No encontrado	No encontrado	No encontrado	No encontrado	No encontrado	No encontrado	No encontrado
Brasil	Art. 154-A Inc. 3	Art. 154-A Inc. 1.	No encontrado	Art. 154-A – Inc. 4	No encontrado	No encontrado	No encontrado	No encontrado	No encontrado	No encontrado	No encontrado
Chile	No encontrado	No encontrado	No encontrado	Art. 4	No encontrado	Art. 366 quáter	No encontrado	Art. 5 Ley 20.009.	No encontrado	Art. 161-A	No encontrado
Colombia	Art. 269 F	Art. 269 E	Art. 269 I	No encontrado	No encontrado	No encontrado	Art. 269G	No encontrado	No encontrado	No encontrado	269 H
Costa Rica	Art. 196 bis	Art. 232	No encontrado	Art. 236. A	Art. 230	Art. 167. A	Art. 196 bis. Y Art. 233	No encontrado	Art. 231 y Art. 288	No encontrado	No encontrado
Cuba	No encontrado	No encontrado	No encontrado	No encontrado	No encontrado	No encontrado	No encontrado	No encontrado	No encontrado	No encontrado	No encontrado
Ecuador	Art. 202.2	No encontrado	Art. 553.1	Art. 202.1	No encontrado	No encontrado	No encontrado	No encontrado	No encontrado	Art. 606.20	No encontrado
El Salvador	No encontrado	No encontrado	Art. 208 inc. 2	Art. 184 y 185	No encontrado	No encontrado	No encontrado	No encontrado	No encontrado	No encontrado	No encontrado

País	Violación de Datos Personales	Difusión de Malware	Hurto Informático	Difusión maliciosa de información	Suplantación de Identidad Digital	Grooming	Captación o venta ilegítima de datos	Carding	Espionaje Informático	Violación a la Intimidad	Agravantes
Guatemala	Art. 274 D	Art. 274 G	No se encontró tipificación.	No encontrado	No encontrado	No encontrado	No encontrado	No encontrado	No encontrado	Art. 274 D	No encontrado
Honduras	No encontrado	No encontrado	Art. 223	Art. 215	No encontrado	No encontrado	No encontrado	No encontrado	No encontrado	No encontrado	No encontrado
México	No encontrado	No encontrado	No encontrado	No encontrado	No encontrado	Art. 202	No encontrado	No encontrado	No encontrado	No encontrado	No encontrado
Nicaragua	No encontrado	No encontrado	No encontrado	No encontrado	No encontrado	No encontrado	No encontrado	No encontrado	No encontrado	Art. 175	No encontrado
Panamá	No encontrado	No encontrado	No encontrado	No encontrado	No encontrado	Art. 187	No encontrado	No encontrado	No encontrado	No encontrado	Art. 291 y 292
Perú	No encontrado	No encontrado	No encontrado	No encontrado	No encontrado	No encontrado	No encontrado	No encontrado	No encontrado	No encontrado	Art. 207 C
Puerto Rico	Art. 167 y Art. 172	Ley de Espionaje Cibernético 1165/2008	Art. 181	Art. 173	Art. 208 y Art. 209	Art. 148	Art. 192	Art. 205 y Art. 229	Ley de Espionaje Cibernético 1165/2008	Art. 168 y Art. 178	No encontrado
República Dominicana	No encontrado	Art. 8	No encontrado	Art. 6 Párrafo I	Art. 17	Art. 23	No encontrado	Art. 5	No encontrado	Art. 19	No encontrado
Uruguay	No encontrado	No encontrado	No encontrado	Art. 301 CP y Art. 8 de Ley 18.515.	No encontrado	No encontrado	No encontrado	No encontrado	No encontrado	No encontrado	No encontrado
Venezuela	Art. 20	Art. 7	Art. 13	Art. 22	No encontrado	No encontrado	No encontrado	Art. 16	Art. 11	No encontrado	Art. 27, 28 y 29

Tabla Nº 1: Cuadro de Derecho comparado sobre los delitos informáticos analizados en Latinoamérica

Delito Informático	%
Espionaje Informático	86%
Captación o venta ilegítima de datos	86%
Suplantación de Identidad Digital	86%
Carding	81%
Violación a la Intimidad	71%
Grooming	67%
Hurto Informático	62%
Difusión de Malware	62%
Violación de Datos Personales	62%
Difusión maliciosa de información	48%

Tabla Nº 2: Ranking de los delitos informáticos menos sancionados penalmente en Latinoamérica.

País	Pje
Bolivia	0%
Cuba	0%
Paraguay	0%
Perú	0%
Haití	9%
México	9%
Nicaragua	9%
Panamá	9%
Uruguay	9%
El Salvador	18%
Honduras	18%
Brasil	27%
Argentina	36%
Chile	36%
Colombia	36%
Ecuador	36%
Guatemala	36%
Venezuela	55%
Costa Rica	64%
República Dominicana	64%
Puerto Rico	91%

Tabla Nº 3: Estadísticas sobre el nivel de sanción penal de los delitos analizados, por país.

Conclusiones

Los resultados del presente trabajo permiten llegar a distintas conclusiones. Considerando solamente los datos publicados en esta segunda y última parte, los resultados estadísticos de la Tabla Nº 3 pueden llegar a verse como desalentadores, toda vez que como puede observarse, salvo excepciones, la mayoría de los países poseen un bajo nivel de regulación: el 81% de los países analizados poseen sanción penal para menos del 40% de los delitos incluídos en el estudio. Entre las excepciones de los países con mayor nivel de regulación, el cuál merece destacarse, debemos mencionar a tres países centroamericanos, tales como Puerto Rico, República Dominicana y Costa Rica.

Dentro de las posibles deducciones que es posible realizar de los resultados expuestos, coinciden con aquellas alcanzadas en la primera parte de la investigación, en el sentido que los mismos permiten observar y afirmar la falta homogeneización en el ámbito sustantivo de la normativa penal aplicable a los delitos informáticos en Latinoamérica en general.

Por otro lado, e incluso habiéndose asumido las posibles divergencias en cuanto al criterio de interpretación amplio utilizado, los números estadísticos de la tabla Nº 2 también parecen ser contundentes y desalentadores, en cuanto revelan el bajo nivel de adaptación o sanción penal a las categorías de delitos informáticos considerados en el estudio. Sin embargo, a los fines de una mejor comprensión, consideramos apropiado leer dichos datos a la luz de ciertas premisas que destacamos a continuación:

1) Las diferencias entre las estadísticas obtenidas entre los distintos grupos de delitos analizados entre la primera y la segunda parte, tiene su razón de ser. A criterio de este autor, ello encuentra explicación a raíz de que el grupo de delitos analizados de la primera parte del estudio, fue seleccionada buscando determinar los delitos informáticos más comunes o clásicos, determinados en concordancia con los delitos que la Convención de Cibercrimen de Budapest considera como obligatorios para los Estados adheridos. A diferencia de este primer grupo, las categorías de delitos analizadas en este trabajo pueden ser consideradas como de delitos informáticos de *"segunda generación"*, en el sentido que buscan condenar conductas más específicas y/o modernas, como la suplantación de identidad digital, grooming, carding, entre otras. A nuestro criterio, la diferencia entre las estadísticas sobre el nivel de sanción penal por país entre ambos grupos, encuentra explicación precisamente en este aspecto sobre los tipos de delitos informáticos incluídos en cada grupo.

2) Más allá de la diferencia de criterios para considerar la necesidad de tipificación penal de una conducta en uno u otro país, consideramos necesario además tener en cuenta el aspecto cronológico. Es decir, más allá del lugar, consideramos apropiado considerar el momento, la fecha de sanción de las normas dictadas a fin de tipificar los delitos informáticos. A modo de ejemplo, vale citar que los tres países con mejores estadísticas, poseen regulación con menos de 7 años de vida: Costa Rica (2012), República Dominicana (2007) y Puerto Rico (2008). Sumando otro dato a este criterio cronológico, puede observarse que más de la mitad de los países analizados, poseen regulación en la materia sancionada desde el año 2004 hacia atrás[6]. En concreto, este elemento destaca la importancia de la regulación penal con adecuada técnica legislativa, a fin que se permita dotar de mayor vida y utilidad a las normas establecidas.

3) Incluso en aquellos países que han dado respuesta positiva sobre la penalización una determinada conducta (es decir que a prima facie existe homogeneización), pueden observarse diferencias en cuanto a los criterios o elementos del tipo penal necesarios para su configuración. Lamentablemente, los límites del presente trabajo no es la suficiente para extenderse sobre los fundamentos de esta conclusión. No obstante, invitamos al lector interesado a elegir cualquiera de las categorías trabajadas, hacerse de los textos de los artículos señalados en cada país, y comprobar las diferencias (importantes en algunos casos) existentes al momento de tipificarse una misma conducta en distintos países. Justamente de esta problemática, se desprende la necesidad de haber adoptado un criterio de interpretación amplio al momento de clasificación de las conductas penales tipificadas para el estudio, toda vez que la búsqueda última era poder obtener una fotografía actualizada de la situación macro sobre la situación de Latinoamérica en la materia..

6 Dicha afirmación puede comprobarse a partir de la observación de la Tabla Nº 1 de la primera parte de la investigación, en la cuál se ha hecho un listado de la legislación vigente en cada uno de los países que formaron parte del estudio.

Para finalizar, y a modo de cierre, los resultados publicados expresan con claridad la falta de homogeneización legislativa en la materia, un desafío que necesita ser atendido por todos los Estados. Es prioritario que los países adopten decisiones políticas serias a mediano o largo plazo que permitan mejorar los niveles de coordinación, armonización y actualización normativa a fin de mitigar la existencia de paraísos legales en la región que favorezcan la ciberdelincuencia. Por otro lado, destacamos la necesidad de adopción de decisiones que destinen recursos necesarios para gestionar una estructura adecuada para la detección, investigación, persecución eficaz de los delitos informáticos.

Referencias

[1] SYMANTEC CORPORATION, "2012 Norton Cybercrime Report"", septiembre de 2012; Url: http://www.norton.com/2012cybercrimereport, Consulta: 15/04/2014

[2] KSHETRI, Nir, The Global Cybercrime Industry, C Springer-Verlag Berlin Heidelberg 2010, ISBN 978-3-642-11521-9

[3] 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: 15/04/2014

[4] TEMPERINI, Marcelo; “Delitos Informáticos en Latinoamérica: Un estudio de derecho comparado. 1ra. Parte”, 1er. Congreso Nacional de Ingeniería Informática / Sistemas de Información. 2013 (CoNAIISI 2013). ISSN 2346-9927

[5] 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: 15/03/2014

[6] TREND Micro; "Tendencias en la seguridad cibernética en América Latina y el Caribe y respuestas de los gobiernos", 2013, Secretaría de Seguridad Multidimensional de la OEA. ISBN 978-0-8270-6061-6

[7] ORGANIZACIÓN DE LOS ESTADOS AMERICANOS, AG/RES. 2004-XXXIV-O/04.

[8] ORGANIZACIÓN DE LOS ESTADOS AMERICANOS, Tercera Reunión del Grupo de Expertos Gubernamentales en Materia de Delito Cibernético, OEA/Ser.K/XXXIV, CIBER-III/ doc.4/03.

[9] ORGANIZACIÓN DE LOS ESTADOS AMERICANOS, Portal Interamericano de Cooperación en Materia de Delito Cibernético. Url: [http://www.oas.org/juridico/ spanish/cybersp.htm]. Consultado: 29/03/2014

[10] TÉLLEZ VALDÉS, Julio, "Derecho Informático", 3ª.ed., Ed. Mc Graw Hill, México, 2003, Pág. 8