

Facultad de Derecho y Ciencias Sociales
Universidad Nacional de Córdoba
Segundo Congreso de Jóvenes Penalistas de la UNC
-Problemas actuales de Derecho Penal y Criminología-

Delitos Informáticos, Argentina y el Convenio de Budapest sobre el Ciberdelito

Autor:

Ab. Franco Daniel Pilnik Erramouspe

D.N.I. Nro: 26.313.280

franco.pilnik@gmail.com

CÓRDOBA, 2010

Delitos Informáticos, Argentina y el Convenio de Budapest sobre el Cibercrimen.

Introducción:

En el mes de marzo del año 2010, Argentina solicitó la adhesión al Convenio sobre Cibercrimen de Budapest¹. Se trata de la primera Convención internacional sobre el llamado “Cibercrimen” y fue redactada en 2001 por el Consejo de Europa, junto a Estados Unidos, Canadá, Japón, Costa Rica, México y Sudáfrica. Contiene regulación sobre delitos cometidos a través de Internet y las redes informáticas, implementando para los Estados firmantes políticas para luchar contra el cibercrimen a escala internacional, especialmente en materias como el Intrusismo Informático, Privacidad, Violación de la Propiedad Intelectual en Internet, Fraudes realizados vía Web o mediante las redes informáticas, Pornografía Infantil y Seguridad. En el presente trabajo se abordará sucintamente la regulación contenida en él, y su implementación en nuestro derecho, camino que ya se ha iniciado con la aprobación de la Ley Habeas Data y la reforma del Código Penal introducida por la Ley 26.388.-

El Convenio contiene normas de carácter tanto sustantivo como procesal, así como cuestiones relativas a cooperación entre los Estados parte. Las de carácter sustantivo contemplan (para la tipificación en la legislación interna a los Estados Parte) los denominados cibercrimen. Éstos se clasifican en cuatro grandes grupos: a) Delitos de intrusión (Arts. 2 a 6), en el que se integran infracciones penales contra la confidencialidad, integridad y disponibilidad de datos y sistemas informáticos; b) Delitos patrimoniales: falsificaciones y fraudes a través de Internet (Arts. 7 y 8), en el que se contemplan especialmente delitos económicos, sobre todo estafas y defraudaciones; c) Delitos relacionados con la pornografía infantil (Art. 9); d) Delitos de infracción de la propiedad intelectual y derechos conexos (Art. 10), que comprende todos los delitos contra la propiedad intelectual y de los derechos afines según la legislación de cada parte; y e) Responsabilidad penal de las personas jurídicas y otros delitos, en el que se insertan todos aquellos delitos que adquieran un forma comisiva informática o a través de Internet. En cuanto a las normas de carácter procesal, se refieren principalmente: a la conservación rápida de los datos informáticos almacenados, a la orden de presentación, al registro y confiscación de los mismos y, a la obtención en tiempo real de los datos informáticos.

Intentaré desarrollar sintéticamente los principales aspectos de la normativa contenida en el Convenio, su aplicación en el derecho argentino, y la necesaria armonización con nuestro sistema legal.

¹ El texto completo en español se puede consultar en línea. **Dirección URL:** <http://conventions.coe.int/Treaty/en/Treaties/html/185-SPA.htm> (consulta 18/06/10)

Convenio de Budapest sobre el Cibercrimen

Normas de carácter sustantivo.

A. El Convenio, en su Art. Nro. 1º determina el alcance de las expresiones contenidas en él. Allí se define al, "sistema informático", "dato informático", "proveedor de servicio" y "dato de tráfico".

La Ley Nro. 26.388, modificatoria del Código Penal (en adelante C.P.), incorporó algunos conceptos en la nueva redacción del Art. Nro. 77, aunque no lo hizo respecto de los contenidos en el Convenio. En este último, se definió al "sistema informático", como al dispositivo aislado o conjunto de dispositivos interconectados, para el tratamiento automatizado de datos en ejecución de un programa. El "dato informático", se trata de la representación de hechos, información o conceptos expresados de cualquier forma que se preste al tratamiento informático. Se entendió por "proveedor de servicio", a la entidad pública o privada que ofrezca a los usuarios la posibilidad de comunicarse a través de un sistema informático; o bien a cualquier entidad que procese o almacene datos informáticos para dicho servicio de comunicación o para los usuarios del mismo. Por último "dato de tráfico" es entendido como la comunicación realizada por medio de un sistema informático, generando la cadena de comunicación y que indique el origen (IP), destino, ruta, hora, fecha, tamaño, y la duración de la comunicación.

B. Respecto a las figuras delictivas en particular, se puede afirmar que, con relación a los artículos 2º (Acceso ilícito), 3º (Intercepción ilícita), 4º (Atentados contra la integridad de los datos) y 5º (Atentados contra la integridad del sistema), los supuestos allí descriptos se encuentran ya contemplados en la Ley Nro. 26.388 aprobada en nuestro país en el año 2008.

De esta manera, el acceso ilícito a un sistema o dato informático, se ve abarcado en la redacción actual del Art. Nro. 153bis del C.P., y es lo que comúnmente se denomina "Hacking". Así también, la interceptación ilícita de una comunicación electrónica se encuentra penada por el Art. Nro. 153 C.P., castigando la intercepción o captación de comunicaciones electrónicas o telecomunicaciones, donde no sólo se incluyen a los correos electrónicos, sino también, a los mensajes enviados desde o hacia cualquier dispositivo móvil (teléfono celular, *palm*, *blackberry*, etc.). Por último, los atentados contra la integridad de datos o de un sistema informático, se previó con la nueva redacción del segundo párrafo, primera parte, del nuevo Art. Nro. 183 C.P., que castiga la alteración, destrucción o inutilización de los datos, documentos, programas o sistemas informáticos. Estos últimos

delitos se producen principalmente de manera automatizada por la intromisión de los denominados “virus” dentro del ordenador.

B.1. En relación al artículo 6º, en el mismo, se persigue al abuso de equipos e instrumentos técnicos. Así es que prescribe: “*inc. 1º: a. la producción, venta, obtención para su utilización, importación, difusión u otras formas de puesta a disposición: i. de un dispositivo, incluido un programa informático, principalmente concebido o adaptado para permitir la comisión de una de las infracciones establecidas en los artículos 2 a 5 arriba citados; ii. de una palabra de paso (contraseña), de un código de acceso o de datos informáticos similares que permitan acceder a todo o parte de un sistema informático, con la intención de utilizarlos como medio para cometer alguna de las infracciones previstas en los artículos 2 a 5; y b. la posesión de alguno de los elementos descritos en los párrafos (a) (1) o (2) con la intención de utilizarlos como medio para cometer alguna de las infracciones previstas en los artículos 2-5. Los Estados podrán exigir en su derecho interno que concurra un determinado número de elementos para que nazca responsabilidad penal (5). Inc. 2º, Lo dispuesto en el presente artículo no generará responsabilidad penal cuando la producción, venta, obtención para la utilización, importación, difusión u otras formas de puesta a disposición mencionadas en el párrafo 1 no persigan la comisión de una infracción prevista en los artículos 2 a 5 del presente Convenio, como en el caso de ensayos autorizados o de la protección de un sistema informático. Inc. 3º Las Partes podrán reservarse el derecho de no aplicar el párrafo 1, a condición de que dicha reserva no recaiga sobre la venta, distribución o cualesquiera otras formas de puesta a disposición de los elementos mencionados en el párrafo 1 (a)(2)”.*

En cuanto al párrafo a.i) de este artículo, se condice con el segundo párrafo, última parte, del nuevo Art. Nro. 183 del C.P., donde se castiga la conducta de quien “vendere”, “distribuyere”, “hiciera circular” o “introdujere en un sistema informático”, cualquier programa destinado a causar daños. Mientras que el párrafo a.ii), castiga la producción, venta, u obtención de un “password” o clave de acceso, permita el ingreso ilegítimo a un sistema informático. Se persigue de esta manera, la circulación o tráfico, de elementos que posibilitan la comisión de los delitos mencionados.

El párrafo b), plantea una situación no contemplada en nuestro derecho. Así, se propone penar a quien tuviera posesión de alguno de los elementos incluidos párrafos a.i) y a.ii), con intención de cometer alguno de los delitos previstos en los Arts. 2-6 del Convenio. La redacción de este artículo y su inclusión en nuestro derecho, deberá ser especialmente cuidadosa, a los fines de no castigar meros actos preparatorios y convertir esta figura de “peligro” en una norma reñida con los mínimos principios constitucionales vigentes en

nuestro país. El tipo, deberá requerir el conocimiento del carácter de dichos objetos y la voluntad de tenerlos como medio para la comisión de alguna de las conductas previstas. De lo contrario dichas conductas quedarán encuadradas dentro de las “*acciones privadas*” del Art. Nro. 19 de nuestra Constitución Nacional.

Resulta importante detenernos en el inciso 2º, en cuanto lo novedoso del mismo. Ello por cuanto establece que: “*Lo dispuesto en el presente artículo no generará responsabilidad penal cuando la producción, venta, obtención para la utilización, importación, difusión u otras formas de puesta a disposición mencionadas en el párrafo 1 no persigan la comisión de una infracción prevista en los artículos 2 a 5 del presente Convenio, como en el caso de ensayos autorizados o de la protección de un sistema informático*”. Considero que aquí se pretende la no persecución y punición del llamado “*ethical hacking*”. Éste ha sido descrito por el autor Pablo A. Palazzi², al explicar que se trata de un testeado que expertos en seguridad realizan sobre las falencias de redes informáticas mediante herramientas de *software* dedicadas a tal fin, que permiten acceder sin permiso, para “*pescar claves, puertos abiertos, en una red u ordenador*”. Sucede que la configuración de un ordenador no es una ciencia exacta y la única forma de detectar vulnerabilidades en los sistemas informáticos, es buscándolas, testeando las fallas y reparándolas.

El inc. 3º, deja a voluntad de las partes, la aplicación o no del párrafo 1, siempre que dicha reserva no recaiga sobre la venta, distribución o cualesquiera otras formas de puesta a disposición de los elementos mencionados en el párrafo 1 (a).

B.2. El Art. 7º, prevé como infracción penal, la introducción, alteración, borrado o supresión dolosa y sin autorización de datos informáticos, generando datos no auténticos, con la intención de que sean percibidos o utilizados a efectos legales como auténticos, con independencia de que sean directamente legibles e inteligibles.

Esta interesante descripción, no fue parte de la reforma al Código Penal, introducida por Ley Nro. 26.388, y se trataría de una figura de falsedad documental electrónica, no habiéndose hecho distinción respecto de si deben ser documentos públicos o privados, pero sí que deben ser usados con efectos legales. Cabe destacar que en nuestro país, existe una norma que contempla una situación similar, aunque circunscripta a la evasión fiscal. Así, la Ley Penal Tributaria Nro. 24.769, en su artículo número 12, castiga la modificación, adulteración o inutilización de los registros documentales o *informáticos* del fisco nacional, con el propósito de disimular la real situación fiscal de un obligado.

² PALAZZI Pablo A., Los Delitos Informáticos en el Código Penal – Análisis de la ley 26.388. Abeledo Perrot, Buenos Aires, 2009, pág. 108/109.

B.3. El Art. 8º, regula las denominadas “Estafas Informáticas”. Así es que se conmina, la producción de un perjuicio patrimonial a otro, de forma dolosa y sin autorización, a través de: a. la introducción, alteración, borrado o supresión de datos informáticos, y b. cualquier forma de atentado al funcionamiento de un sistema informático. Todo con la intención, fraudulenta o delictiva, de obtener sin autorización un beneficio económico para sí mismo o para tercero.

El inc. b) de este artículo, resulta claramente comprendido en las previsiones del actual inc. 16 del Art. Nro. 173 del Código Penal. Conductas como el denominado “*phishing*” se encuentran abarcadas dentro de estas previsiones.

Diferente es el caso el inciso a), porque si bien, de la lectura del mismo, parecería que nos encontramos frente a las acciones previstas en el Art. Nro. 183 segundo párrafo del C.P., el dolo específico de la obtención de un rédito económico, no se encuentra en este último. Es por ello que entiendo que, frente a una acción de “introducción”, “alteración”, “borrado” o “supresión” de datos informáticos, con la intención fraudulenta de obtener un rédito económico, también debemos recurrir a las previsiones del Art. Nro. 173 inc. 16 del C.P. Y es que, dichas acciones no hacen más que alterar “*el normal funcionamiento de un sistema informático o la transmisión de datos*”, tal como lo prevé dicho inciso

B.4. El Art. 9º, regula lo relacionado a la Pornografía Infantil. Éste establece lo siguiente:

1. Las Partes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias para prever como infracción penal, conforme a su derecho interno, las siguientes conductas cuando éstas sean cometidas dolosamente y sin autorización: a) la producción de pornografía infantil con la intención de difundirla a través de un sistema informático; b) el ofrecimiento o la puesta a disposición de pornografía infantil a través de un sistema informático; c) la difusión o la transmisión de pornografía infantil a través de un sistema informático; d) el hecho de procurarse o de procurar a otro pornografía infantil a través de un sistema informático; e) la posesión de pornografía infantil en un sistema informático o en un medio de almacenamiento de datos informáticos.

2. A los efectos del párrafo 1 arriba descrito, la «pornografía infantil» comprende cualquier material pornográfico que represente de manera visual: a) un menor adoptando un comportamiento sexualmente explícito; b) una persona que aparece como un menor adoptando un comportamiento sexualmente explícito; c) unas imágenes realistas que representen un menor adoptando un comportamiento sexualmente explícito.

3. A los efectos del párrafo 2 arriba descrito, el término «menor» designa cualquier persona que no alcanzare los 18 años de edad. Las Partes podrán exigir un límite de edad inferior, que deberá ser como mínimo de 16 años.

4. Los Estados podrán reservarse el derecho de no aplicar, en todo o en parte, los párrafos 1 (d) y 1 (e), y 2 (b) y 2 (c).

Las conductas aquí descritas, y la utilización de Internet y otros medios de comunicación para su cometido, se ven en su mayoría contempladas en la nueva redacción del Art. Nro. 128 del C.P.. Afortunadamente, el Convenio ha dejado librado a los Estados contratantes, la aplicación de los párrafos 1 (d) y 1 (e), toda vez que los mismos, podrían estar reñidos con el principio de reserva (Art. 19 C.N.) y pueden merecer el mismo reproche que en general tienen las figuras de “simple tenencia” y de “peligro abstracto”, que tanto debate han generado en la doctrina nacional. Incluso jurisprudencialmente existen fallos en contra, por ejemplo la Cámara Nacional de Casación Penal, Sala 1, ha señalado lo siguiente: *“La figura de la distribución de imágenes pornográficas de menores de dieciocho años de edad que regula el artículo 128, 2º párrafo del Código Penal, castiga la distribución de imágenes pornográficas de menores de dieciocho años de edad y no el mero hecho de recibir este tipo de fotografías. Es necesario no sólo recibir, sino además, enviar a otras personas imágenes pornográficas de menores de edad. Aquí también es importante señalar que la descripción penal alude a la voz distribución de imágenes, hecho éste que descarta el mero envío de textos sólo referidos a ella”*³. Destáquese que, con la nueva redacción del Art. Nro. 128, en su segundo párrafo, se requiere, no la simple posesión de las imágenes, sino la tenencia de las mismas con fines inequívocos de distribución o comercialización.

En cuanto a la exclusión de los párrafos 2 (b) y 2 (c), nos enfrentamos nada más y nada menos, que ante el concepto de “Pornografía Infantil”. Con la sanción de la Ley Nro. 25763, nuestro país aprobó el *“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, sesión plenaria del 25 de mayo de 2000). El art. 2º inc. c) 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”*.

Mucho más controvertido resulta aún, la inclusión en el tipo penal, de imágenes de mayores que parecen menores o bien de imágenes realistas que representen menores. El

³ Fallo del 25/4/02, causa N° 18108 “N.G.A.”

requisito objetivo del tipo en cuanto a la edad, excluiría esta clase de conductas y estimo que serían de difícil aplicación en nuestro derecho.

B.5. En el Art. 10º, se regulan los delitos relacionados con infracciones de la propiedad intelectual y derechos afines. Así es que se dispone:

1. Las Partes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias para prever como infracción penal, conforme a su derecho interno, los atentados a la propiedad intelectual definida por la legislación de cada Estado, conforme a las obligaciones que haya asumido por aplicación de la Convención Universal sobre los Derechos de Autor, revisada en París el 24 de julio de 1971, del Convenio de Berna para la protección de obras literarias y artísticas, del Acuerdo sobre los aspectos de los derechos de propiedad intelectual relacionados con el comercio y del Tratado de la OMPI sobre Derecho de Autor, a excepción de cualquier derecho moral conferido por dichas Convenciones, cuando tales actos sean cometidos deliberadamente, a escala comercial y a través de un sistema informático.

2. Las Partes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias para prever como infracción penal, conforme a su derecho interno, los atentados a los derechos afines definidos por la legislación de cada Estado, conforme a las obligaciones que haya asumido por aplicación de la Convención Internacional sobre la Protección de los Artistas Intérpretes o Ejecutantes, los Productores de Fonogramas y los Organismos de Radiodifusión, hecha en Roma (Convención de Roma), del Acuerdo sobre los aspectos de los derechos de propiedad intelectual relacionados con el comercio y del Tratado de la OMPI sobre interpretación o ejecución y fonogramas, a excepción de cualquier derecho moral conferido por dichas Convenciones, cuando tales actos sean cometidos deliberadamente, a escala comercial y a través de un sistema informático.

3. Las Partes podrán, de concurrir determinadas circunstancias, reservarse el derecho de no imponer responsabilidad penal en aplicación de los párrafos 1 y 2 del presente artículo, siempre que se disponga de otros recursos eficaces para su represión y que dicha reserva no comporte infracción de las obligaciones internacionales que incumban al Estado por aplicación de los instrumentos internacionales mencionados en los párrafos 1 y 2 del presente artículo.

Las conductas aquí descriptas, ya se encuentran previstas en los artículos Nros. 71 a 78 de la Ley Nro. 11.723, en cuanto se prevé la aplicación de la misma pena del Art. Nro. 172 del Código Penal, a quienes vendan, reproduzcan o editen una obra sin el consentimiento de su autor.

Una de las cuestiones más controvertidas que puede plantear este artículo, es la necesidad que las conductas deban ser realizadas a escala comercial. Con esto se deja fuera de

la punición, al particular consumidor que descarga obras con protección legal y luego las comparte mediante los sistemas “*puerto a puerto*” (*p2p= peer to peer*)⁴. Este tema, seguramente generará un gran debate, toda vez que en todo el mundo se discute sobre la persecución o no, de los consumidores hogareños que a diario descargan música, películas y programas protegidos desde la red. Incluso se han sucedido numerosos fallos donde se ha llegado a condenar a ciudadanos por la excesiva descarga de material con *copyright*.

B.6. El Art. 11º, trata sobre la participación y tentativa, cuestiones todas ya contempladas en nuestro Código Penal en los artículos Nros. 42 a 49.

B.7. Mucho más compleja resulta la inclusión en nuestro país, de lo normado por el Art. 12º, toda vez que el mismo versa sobre la responsabilidad penal de las personas jurídicas, por los delitos previstos en el Convenio, cuando sean cometidos por una persona física, ya sea actuando en forma individual o como miembro de un órgano de dicha persona jurídica, ejerciendo funciones directivas en virtud de un poder o autorización. Incluso llega a exigírsele responsabilidad (a la persona jurídica), por la ausencia de vigilancia o control que haya permitido la comisión de algunos de los delitos previstos en el Convenio.

Sin embargo, el inciso tercero deja librado a las Partes, la posibilidad que la responsabilidad se de tipo Civil o Administrativa, independientemente de la penal que le pueda caber a la persona física.

Normas de carácter procesal.

A. En cuanto a las normas adjetivas establecidas por el Convenio, si bien exceden lo requerido por este trabajo dada la materia de que tratan, resulta interesante realizar una mínima revisión de las mismas. También es importante destacar que, conforme nuestro sistema constitucional, el dictado de normas procesales es una facultad reservada por las provincias y serán ellas quienes deberán adoptar estas medidas.

El Art. 14º regula el ámbito de aplicación de las medidas de derecho procesal, alcanzando a los tipos penales resultantes de la primera sección del Convenio, como así también al conjunto de tipos penales vigentes en un Estado contratante, siempre que los

⁴ Peer to Peer: “*Forma coloquial de referirse a las denominadas redes entre iguales, redes entre pares o redes punto a punto. En estas redes no existen ni ordenadores cliente ni ordenadores que hagan de servidor. Las redes P2P permiten el intercambio directo de información, en cualquier formato, entre los ordenadores interconectados. El hecho de que sirvan para compartir e intercambiar información de forma directa entre dos o más usuarios ha propiciado que hayan sido, y estén siendo, utilizadas para intercambiar archivos cuyo contenido está sujeto a las leyes de copyright, lo que ha generado una gran polémica entre defensores y detractores de estos sistemas.*” (en línea) Dirección URL: <http://es.wikipedia.org/wiki/P2p> (consulta: 16/06/10)

medios comisivos sean informáticos, o que la evidencia con la que se cuente o se pretenda reunir, sea digital.

El art. 15°, aparece como salvaguarda de las Condiciones y Garantías, con el propósito de evitar que la puesta en funcionamiento de los poderes y procedimientos, afecte derechos de raigambre constitucional.

El art. 16°, permite a las autoridades, a exigir la conservación rápida de datos informáticos almacenados. Cuando esta sea requerida por parte de la autoridad, la persona deberá conservar y proteger la integridad de los datos durante el lapso de tiempo necesario, hasta un máximo de 90 días, con el fin de que las autoridades puedan obtener su revelación.

Mediante el art. 17°, se obliga a garantizar la conservación rápida de los datos relativos al tráfico, a uno o varios proveedores de servicios que hayan participado en la comunicación.

Los artículos 18° y 19°, regulan sobre la orden de presentación, el registro y confiscación de los datos informáticos y datos relativos al tráfico, y la obtención en tiempo real de los datos informáticos.

Luego, los arts. 20° y 21°, permiten la obtención e interceptación en tiempo real de los datos informáticos, así como los datos relativos al tráfico.

Muchas críticas se han recibido, principalmente en referencia a los artículos 17°, 18°, 24° y 25°, en cuanto requieren que los proveedores de acceso a Internet, mantengan registros de las actividades de sus clientes, ello por cuanto podría significar un riesgo considerable para la privacidad de los mismos. Aún así, existen en el mundo normas de carácter similar, por ejemplo la controvertida USA *Patriot Act*, dictada luego de los atentados del 11 de Septiembre, incluye como *ciberterrorismo* todos aquellos ataques vía Internet que causen pérdidas superiores a los 5.000 U\$\$, de modo que los *hackers* pueden sufrir condenas de hasta 20 años de cárcel, y se obliga a las empresas de Internet a entregar el registro de actividad y los correos electrónicos de quien resulte sospechoso.

El procedimiento, debería contemplar que se ordene averiguar la identidad del usuario. Primero, mediante la obtención de la dirección electrónica y el momento de conexión dirigida al proveedor de acceso, como empresa que permite acceder a las redes de comunicación entre ordenadores, poniendo a su disposición una conexión TCP/IP. Y luego, para averiguar la identidad del abonado, dirigida al proveedor de servicios, como empresa titular de la infraestructura de comunicaciones. Establecidos estos datos, se procederá a la interceptación de comunicaciones, mediante la grabación en el correspondiente soporte de las transferencias telemáticas (normalmente mensajería electrónica).

Resulta importante destacar que en nuestro país rige la ley 25.873, la cual obliga a las empresas de telecomunicaciones a registrar el tráfico de los usuarios, tanto electrónico como

telefónico, por diez años. Pero dicha ley y su decreto reglamentario 1563/04 han sido declarados inconstitucionales por la Corte Suprema de Justicia de la Nación en autos “Halabi, Ernesto c/PEN ley 25.873 y decreto 1563/04 s/amparo”⁵.

También puede resultar polémica, la aplicación del párrafo 4 del Art. 19º, en cuanto faculta a las autoridades competentes para ordenar a cualquier persona, que conozca el funcionamiento de un sistema informático o las medidas aplicadas para proteger los datos allí registrados o contenidos, que proporcione todas las informaciones razonablemente necesarias, para permitir la aplicación de las medidas previstas en los párrafos 1 y 2, ello por cuanto podría ser violatorio de la garantía de no obligatoriedad de declarar en contra de si mismo (Art. 18 C.N.).

Igualmente el Art. 22º, en su primer párrafo, establece el principio donde los Estados ejercerán la competencia. Así se prevé que será competente el Estado respecto de las infracciones que se produzcan, a) en su territorio, b) a bordo de una nave que ondee pabellón de ese Estado, c) a bordo de una aeronave inmatriculada en ese Estado, o d) por uno de sus súbditos, si la infracción es punible penalmente en el lugar donde se ha cometido o si la infracción no pertenece a la competencia territorial de ningún Estado. Pero, conforme lo establece el párrafo 5º, en caso en que varias partes reivindiquen jurisdicción, se celebrarán consultas, a los fines de decidir cuál es la más adecuada para entablar la acción penal.

Finalmente el art. 35º, instaura la Red 24/7, obligando a cada parte, a tener un punto de contacto localizable las 24 hs. del día, los siete días de la semana, con el fin de garantizar la asistencia inmediata para investigaciones relativas a sistemas y datos informáticos.

Conclusión.

Como se podrá observar, el Convenio que pronto será parte de nuestra legislación, significa un importante avance en la lucha contra las nuevas formas delictivas, posicionando al Estado Argentino, dentro de un sistema internacional contra el “Cibercrimen”. Esta política, que ya había comenzado con el dictado reciente de algunas leyes en la materia, no hace más que demostrar la constante necesidad de actualización y modernización a la que están sometidos los actores jurídicos. Será el Congreso de la Nación quien deberá encargarse de adecuar las normas establecidas en el Convenio, con las de derecho interno, teniendo especialmente en cuenta de no contravenir las mínimas garantías establecidas por la Constitución Nacional y demás tratados internacionales incorporados a la misma. El abrumador avance de la tecnología hace necesario adoptar las medidas adecuadas para poder

⁵ Fallos: 332:111 (LA LEY, 2009-B, 157)

afrontar los nuevos desafíos, con la firma de este Convenio, Argentina se pone a la vanguardia entre los países del cono sur, en la lucha contra las novedosas formas delictivas.

Ab. Franco Daniel Pilnik Erramouspe

D.N.I. Nro: 26.313.280

franco.pilnik@gmail.com

BIBLIOGRAFÍA

1. **ABOSO, Gustavo Eduardo – ZAPATA, María Florencia**, *Cibercriminalidad y Derecho Penal. B de f*, Buenos Aires, 2006.
2. **CREUS, Carlos -BUOMPADRE, Jorge Eduardo** “*Derecho Penal, Parte especial*” Astrea, Buenos Aires, 2007.
3. **DONNA, Edgardo**, *Derecho penal. Parte especial. Rubiznal- Culzoni, Santa Fe*, 2001.
4. **PALAZZI, Pablo A.**, *Delitos Informáticos. Ad Hoc*, Buenos Aires, 2000.
- *Delitos Informáticos en el Código Penal – Análisis de la ley 26.388. Abeledo Perrot*, Buenos Aires, 2009.
6. **RIQUERT, Marcelo A.**, *Protección penal de la intimidad en el espacio virtual*. Ediar, Buenos Aires, 2003.