Informática y Delito

Reunión preparatoria del XIX Congreso Internacional de la Asociación Internacional de Derecho Penal (AIDP)

Grupo argentino, Facultad de Derecho, UBA, marzo de 2014

Infojus
SISTEMA ARGENTINO DE INFORMACIÓN JURÍDICA

Asociación Internacional de Derecho Penal
Grupo Argentino

Informática y Delito

Reunión preparatoria del XIX Congreso Internacional
de la Asociación Internacional de Derecho Penal (AIDP)

Grupo argentino, Facultad de Derecho, UBA, marzo de 2014

Infojus
SISTEMA ARGENTINO DE INFORMACIÓN JURÍDICA

Asociación Internacional de Derecho Penal
Grupo Argentino

De Luca, Javier Augusto
Informática y delito : Reunión preparatoria del XIX Congreso Internacional de la Asociación Internacional de Derecho Penal -AIDP / Javier Augusto De Luca y Joaquín Pedro da Rocha. - 1a ed. - Ciudad Autónoma de Buenos Aires : Infojus, 2014.
312 p. ; 23x16 cm.

ISBN 978-987-3720-08-6

1. Derecho Penal. I. da Rocha, Joaquín Pedro. II. Título.
CDD 345

Fecha de catalogación: 31/07/2014

ISBN: 978-987-3720-08-6
Informática y Delito.
Reunión preparatoria del XIX Congreso Internacional de la Asociación Internacional de Derecho Penal AIDP.
1ra. edición - Agosto 2014

Editorial Ministerio de Justicia y Derechos Humanos de la Nación, Sarmiento 329, C.P. 1041AFF, C.A.B.A.

Los artículos que integran esta publicación se encuentran disponibles en forma libre y gratuita en: www.infojus.gob.ar

AUTORIDADES DE LA ASOCIACIÓN INTERNACIONAL DE DERECHO PENAL [1]

JOSÉ LUIS DE LA CUESTA (ESPAÑA)
PRESIDENTE

REYNALD OTTENHOF (FRANCIA)
VICEPRESIDENTE

HELMUT EPP (AUSTRIA)
SECRETARIO GENERAL

RENÉ ARIEL DOTTI (BRASIL)
EUGENIO R. ZAFFARONI (ARGENTINA)
VICEPRESIDENTES AMÉRICA LATINA

CARLOS E. A. JAPPIASSÚ (BRASIL)
SECRETARIO GENERAL ADJUNTO AMÉRICA LATINA

(1) Véase [en línea] http://www.penal.org/

AUTORIDADES DE LA AIDP DE LA SECCIÓN ARGENTINA[1]

JAVIER AUGUSTO DE LUCA
PRESIDENTE

DANIEL ERBETTA
VICEPRESIDENTE

JOAQUÍN PEDRO DA ROCHA
SECRETARIO GENERAL

LUIS MARÍA BUNGE CAMPOS
SECRETARIO GENERAL ADJUNTO

MARÍA ÁNGELES RAMOS
TESORERA

FRANCISCO FIGUEROA
PROTESORERO

(1) Véase [en línea] http://www.aidpargentina.com.ar/

REUNIÓN PREPARATORIA
DEL XIX CONGRESO INTERNACIONAL DE LA AIDP

FACULTAD DE DERECHO (UBA)[1]

TEMA

"Sociedad de la Información y Derecho Penal"(Delitos Informáticos), desde las perspectivas del Derecho Penal (parte general y especial), Proceso Penal y Penal Internacional

En esta reunión, de singular importancia para el desarrollo del Derecho Penal en América Latina, buscamos aunar posiciones como grupo nacional, para llevarlas al XIX Congreso Internacional de la AIDP en Río de Janeiro.

Durante la jornada se realizarán cuatro paneles, de acuerdo a los ejes temáticos previstos en los coloquios preparatorios fijados por la AIDP, para lo cual hemos convocado a distintos especialistas. Expondrán, sometiendo a debate sus ideas, los Dres. Marcelo Riquert; Nora A. Cherñavsky; Marcos Salt; Luis María Bunge Campos; Horacio Azzolin; Daniela Dupuy, Christian Sueiro y E. Raúl Zaffaroni.

PROGRAMA

14 a 14.30 hs.:	Acreditaciones
14:30 hs.:	Presentación a cargo de los Dres. Javier A. De Luca y Joaquín P. da Rocha.
15 a 17 hs.:	Coloquios sobre Derecho Penal Parte General y Derecho Penal Parte Especial en la Sociedad de la Información.
17 hs.:	*Break*

(1) Celebrada el miércoles 12 de marzo de 2014 de 14 a 20 hs. en el Salón Azul.

17:30 a 19:30 hs.: Coloquios sobre Derecho Procesal Penal y Derecho Penal Internacional en la Sociedad de la Información.

19:30 hs.: Cierre a cargo del vicepresidente de la AIDP, Prof. Dr. E. Raúl Zaffaroni.

Auspiciaron:

Asociación Argentina de Profesores de Derecho Penal (AAPDP); Asociación Argentina de Profesores de Derecho Procesal Penal (AAPDPP); Asociación Latinoamericana de Derecho Penal y Criminología (ALPEC); Asociación de Magistrados y Funcionarios de la Justicia Nacional; Departamento de Derecho Penal y Criminología de la Facultad de Derecho (UBA); Fundación de Estudios para la Justicia (FUNDEJUS); Instituto de Derecho Penal y Criminología del Colegio Público de Abogados de la Capital Federal; Ministerio de Justicia y Derechos Humanos de la Nación (INFOJUS); Ministerio de Justicia y Derechos Humanos de la Provincia de Buenos Aires; Justicia Legítima; Universidad Nacional de La Matanza; y Universidad Nacional de Rosario.

PRESENTACIÓN

JAVIER AUGUSTO DE LUCA y JOAQUÍN PEDRO DA ROCHA

El miércoles 12 de marzo de 2014 tuvo lugar la reunión preparatoria para el 19° Congreso Internacional de Derecho Penal, organizada por la Sección Argentina de la Asociación Internacional de Derecho Penal (AIDP).

Asistieron al encuentro más de 120 personas, dentro de las cuales se incluyeron docentes y alumnos de distintas universidades, magistrados, funcionarios y empleados de la administración de justicia, abogados particulares y especialistas en la temática de delitos informáticos. Se destacó la presencia de los profesores David Baigún, Cecilia Grossman, Lucila Larrandart, Guillermo Llaudet, Daniel Erbetta, Julio Maier, Luis Niño, Carlos Caramuti, Gustavo Garibaldi, Patricio Sabadini, Marcelo Buigo, Mauro Divito, Valeria Lancman, Cristian Cabral, entre muchos otros.

El tema discutido fue el de "Sociedad de la Información y Derecho Penal (Delitos Informáticos", desde las perspectivas del Derecho Penal, Parte General; del Derecho Penal, Parte Especial; del Derecho Penal Internacional; y del Derecho Procesal Penal.

Luego de unas breves palabras de bienvenida del Dr. Javier A. De Luca, el Dr. Joaquín Pedro da Rocha distinguió al ex presidente y actual presidente honorario del Grupo Argentino, Dr. David Baigún, explicando sucintamente cómo habría de desarrollarse la reunión.

La jornada continuó con la conferencia del profesor emérito Dr. E. Raúl Zaffaroni, quien también rindió homenaje al profesor Dr. David Baigún, luego de haber recordado el origen y la función de la AIDP en el mundo y, especialmente, en América Latina.

Inmediatamente, se abrió el panel denominado Parte General. Aquí la Dra. Nora A. Cherñavsky desarrolló el tema de la responsabilidad penal de los proveedores de Internet. Luego, los Dres. Pablo Tello y Hernán

Kleiman analizaron la posible existencia de un bien jurídico particular en los delitos informáticos.

El segundo panel, Parte Especial, fue inaugurado por el Dr. Horacio Azzolin, quien observó los aspectos problemáticos de la adhesión al Convenio de Ciberdelincuencia de Budapest. Con posterioridad, el Dr. Christian Sueiro desarrolló cuestiones referidas a la criminalidad informática para la reforma del Anteproyecto de Código Penal de la Nación.

En el panel sobre Derecho Procesal Penal disertaron, por un lado, la Dra. Daniela Dupuy, acerca de los procedimientos informáticos para la investigación de delitos; y, por el otro, el Dr. Luis María Bunge Campos, sobre sociedad de la información y derecho a la intimidad.

El último de los paneles, Derecho Internacional Penal, estuvo a cargo de los Dres. Marcelo Riquert y Marcos Salt. El primero examinó los Convenios de Budapest y del MERCOSUR; y, el segundo, la cuestión relativa a la persecución de estos delitos en el Derecho Penal Internacional.

Antes de terminar la reunión, el Dr. Joaquín P. da Rocha destacó, en nombre de los organizadores, el éxito de la actividad, tanto por el elevado nivel de las exposiciones y ponencias como por la calificada concurrencia.

El evento contó con varios auspicios: Asociación Argentina de Profesores de Derecho Penal (AAPDP); Asociación Latinoamericana de Derecho Penal y Criminología (ALPEC); Asociación de Magistrados y Funcionarios de la Justicia Nacional (AMFJN); Departamento de Derecho Penal y Criminología, Facultad de Derecho (UBA), Fundación de Estudios para la Justicia (FUNDEJUS); Instituto de Derecho Penal y Criminología; Colegio Público de Abogados de la Capital Federal; Ministerio de Justicia y Derechos Humanos de la Nación; Dirección Nacional del Sistema Argentino de Información Jurídica (INFOJUS); Ministerio de Justicia y Derechos Humanos de la Provincia de Buenos Aires; Justicia Legítima; Universidad Nacional de La Matanza (UNLaM); y Universidad Nacional de Rosario (UNR).

Agradecemos a quienes se esforzaron para que la jornada fuera un éxito y para que de ella surgiera la presente publicación, que refleja su importancia. Entre ellos, Nadia Espina; Sebastián Zanazzi; Ayelén Trindade; Virginia Urquiza; Matías Eidem; María Ángeles Ramos; Ivanna Opacak; Anabel Solimando; Gabriela Gusis; Florencia Grajirena; Carolina Bressia; Guadalupe Piaggio, Agustín Antognoli y Francisco Figueroa. También agradecemos las contribuciones de los Dres. Patricio Sabadini, Luis Ángel Nócera y Diego Migliorisi.

INTRODUCCIÓN[1]

JAVIER AUGUSTO DE LUCA[2] y JOAQUÍN PEDRO DA ROCHA[3]

Javier De Luca. Buenas tardes a todos, muchas gracias por venir. Soy Javier De Luca, y en este caso, oficio de autoridad, por decirlo de algún modo, ya que por obra del honor que me han conferido varios colegas, soy el presidente del Grupo Argentino de la Asociación Internacional de Derecho Penal (AIDP). Estamos aquí con el "Chango" Da Rocha, que es el secretario general del Grupo Argentino, y con uno de los vicepresidentes de la AIDP, que es el profesor emérito Raúl Zaffaroni, a quien todos conocemos y quien va a estar a cargo de la apertura de este encuentro.

Esta jornada tiene el propósito de conocernos, de saber en qué estado estamos, en qué situación nos encontramos respecto de los llamados ciberdelitos o delitos informáticos. Sobre esto versará el próximo Congreso Internacional de la Asociación Internacional de Derecho Penal, que se va a desarrollar en Río de Janeiro entre el 31 de agosto y el 6 de septiembre.

Hemos recibido el auspicio de mucha gente que siempre nos acompaña, algunos nuevos y otros no. Los voy a mencionar porque así corresponde: la Asociación Argentina de Profesores de Derecho Penal, la Asociación

(1) El texto que sigue es la transcripción de la grabación obrtenida durante la presentación de la Reunión Preparatoria del XIX Congreso Internacional de la AIDP.

(2) Abogado y Doctor en Derecho Penal (UBA). Fiscal General ante la Cámara Federal de Casación Penal. Profesor Regular de la Cátedra de Elementos de Derecho Penal y Procesal Penal, Facultad de Derecho (UBA).

(3) Abogado y Doctor en Derecho Penal (UBA). Director de los posgrados de Maestría y Especialización en Administración de Justicia, Universidad de La Matanza. Director del Instituto de Derecho Penal del Colegio Público de Abogados de la Capital Federal. Secretario General de la Sección Argentina de la Asociación Internacional de Derecho Penal. Presidente de la Fundación de Estudios para la Justicia —FUNDEJUS—.

Argentina de Profesores de Derecho Procesal Penal, la Asociación Latinoamericana de Derecho Penal y Criminología, la Asociación de Magistrados y Funcionarios de la Justicia Nacional, el Departamento de Derecho Penal y Criminología de esta casa —aquí representado por su directora, Lucila Larrandart—, la Fundación de Estudios para la Justicia —también representada por nuestro secretario general y por algunos miembros muy característicos de ella—, el Instituto de Derecho Penal y Criminología del Colegio Público de Abogados —también representado por "El Chango"—, el Ministerio de Justicia y Derechos Humanos de la Nación, Infojus —sus revistas se pueden conseguir en sus Centros de Consulta y también se pueden descargar gratuitamente desde su página web—, el Ministerio de Justicia y Derechos Humanos de la Provincia de Buenos Aires, la asociación Justicia Legítima, la Universidad Nacional de La Matanza y la Universidad Nacional de Rosario, entre otros.

El "Chango" de Rocha quiere decir unas palabras.

Joaquín Pedro da Rocha. Creo que casi todo lo que tendría que decir, ya lo acaba de contar Javier. Lo que resta es resolver cómo darle continuidad a esta reunión acá en Argentina y cómo darle continuidad cuando estemos, los que vayamos el mes de agosto/septiembre, en Río de Janeiro, de manera que podamos integrar un todo coherente en la representación Argentina y quizás regional.

Pero lo que no quería dejar pasar y además quiero hacerlo ahora y en su presencia, es un especial homenaje y agradecimiento al profesor David Baigún, quien fue durante más de veinte años presidente del Grupo Argentino, y de quien nos consideramos humildes discípulos. Quiero agradecerle todo lo que ha hecho y seguirá haciendo, porque ahora es nuestro presidente honorario de la AIDP Sección Argentina. De modo que, ¡"Tute", muchas gracias! Queremos seguir contando con tu participación y decirte que trataremos de llevar adelante de la mejor manera todo lo que nos has enseñado.

CONFERENCIA INAUGURAL[1]

E. RAÚL ZAFFARONI[2]

Muchísimas gracias. Ante todo, adhiero a las palabras del "Chango" de hace un momento. Todos somos alumnos de "Tute". La primera vez que llegué al entonces Instituto de Derecho Penal, era el año 1960, yo era muy chiquitito, siempre fui muy precoz, y la primera clase era de "Tute". No me voy a olvidar nunca la primera recepción del Instituto, una clase de "Tute" Baigún. De eso pasaron 54 años y a lo largo de ellos "Tute" ratificó constante y permanentemente su vocación docente y una línea de conducta realmente admirable y coherente. De modo que, adhiero por razones afectivas e intelectuales y por admiración ideológica a su coherencia, con toda y absoluta sinceridad, al homenaje que le atributa el compañero "Chango".

Me alegra muchísimo que el Grupo Argentino de la Asociación Internacional de Derecho Penal cobre vitalidad en este momento con este tipo de actividades. Creo que tenemos una tarea importante que cumplir. Voy a tratar de sintetizarla un poco en estos minutos. No quiero que se depriman por la magnitud de la tarea que les voy a plantear, pero estamos en un momento complicado del mundo y en un momento complicado de la región.

La Asociación Internacional de Derecho Penal nace a fines del siglo XIX, en 1890, como Unión Internacional de Derecho Penal, de la mano de Gerard van Hammel, Adolph Prins y Franz von Liszt. Luego se interrumpe con la Primera Guerra Mundial y reaparece por los años 20, reorganizada como la Asociación Internacional de Derecho Penal, hasta ahora. El mundo ha transitado muchísimo desde entonces.

(1) El texto que sigue es la transcripción de la grabación obrtenida durante la Conferencia Inaugural de la Reunión Preparatoria del XIX Congreso Internacional de la AIDP

(2) Ministro de la Corte Suprema de Justicia de la Nación de la República Argentina. Profesor Emérito de la Universidad de Buenos Aires.

El 2014 es el año del centenario de la primera etapa del suicidio europeo. Hace cien años daba la impresión de que todo estaba estable y marchaba hacia un progreso. Había una serie de testas coronadas que se casaban entre ellos. De pronto Europa decide suicidarse y se suicidó en una conflagración que empezó en 1914 y que, en definitiva, terminó treinta años después, en 1945, del modo que todos sabemos. Realmente el siglo que pasó ha sido un terrible siglo de genocidios. Y en este momento, después de todo el proceso de descolonización, hay —sin lugar a dudas— una tensión en el mundo entre lo que es el Norte y lo que es el Sur.

Estamos amenazados por nuevos conflictos, nuevos conflictos bélicos, estamos amenazados por nuevas masacres, y hay masacres en curso.

Realmente creo que una asociación como la AIDP no puede dejar de mirar e incorporar al Sur. Si vemos su estructura actual, estamos muy poco representados, quizá también la culpa sea parcialmente nuestra. Hace dos años organizamos la Asociación Latinoamericana de Derecho Penal y Criminología, no con el objeto de hacer una disidencia respecto de la AIDP, de la de Criminología, de la de Defensa Social, ni de la Fundación Internacional Penal y Penitenciaria —que son las grandes asociaciones mundiales—, sino con el objeto de convocar regionalmente, para que toda la región de América Latina tenga en las cuatro asociaciones una política coherente.

En este momento la situación de América Latina es compleja, seriamente compleja. Creo que los medios de comunicación monopolizados u oligopolizados nos están escondiendo gran parte de la realidad, o por lo menos, la están deformando considerablemente.

Desde la Argentina no lo percibimos porque, por suerte, no tenemos los índices de violencia que tiene gran parte del resto de nuestra región. Pero diría que hoy en América Latina, estamos con una masacre en curso, una masacre por goteo, que a veces incluso son chorros. Si vemos los números son pavorosos. Nosotros estamos teniendo en la República Argentina, por lo menos en Buenos Aires y en el conurbano bonaerense, un índice de homicidios cuyo máximo toca el 7.5 por cien mil. Brasil, acá al lado, tiene una media nacional de 27 por cien mil. México, en los últimos seis años, ha tenido oficialmente algo más de 70 mil muertos, y digo oficialmente porque hay cifra negra. Cada dos por tres se descubren posos con cadáveres. Algunos dicen que son 90 mil, otros dicen que son 100 mil, no importa. Aunque tomemos las cifras oficiales se nos está indicando un orden de 12 mil

muertos por año. La publicidad que se está haciendo en este momento y la versión oficial es que están mejorando porque han alcanzado una meseta, no suben, siguen siendo 12 mil por año. Si vemos, como se han dado las cifras, hasta el año 2007 el índice era mucho más bajo, no se registraba ese número de muertos. A partir del año 2007, que se desequilibra todo lo relativo al narcotráfico, es cuando se dispara y cuando se produce el brote que lleva a 12 mil muertos anuales. Si vemos el panorama de Centroamérica, Honduras se lleva el campeonato de los índices de homicidios —40 y tantos por 100 mil— y San Pedro Sula más de 80 por 100 mil. Esta es la realidad de la violencia en nuestra región. En el Cono Sur, que estamos más o menos geopolíticamente protegidos de lo que llaman el crimen organizado, es donde tenemos los índices más bajos. Pero cuidado, la situación regional es sumamente delicada, estamos hablando de miles y miles de muertos. Esto es masacre por goteo en curso. No podemos pensar el derecho penal o la dogmática jurídica como un juego de ajedrez que estamos haciendo en un tablero cuando es indispensable volver a pensarla como una estructura que indique cómo decidir casos, tratando o procurando resolver conflictos con la menor violencia posible.

El neokantismo, que nos dice que no incorporemos ningún otro dato de la realidad sino que nuestro saber es una especie de fisicalismo que podemos hacer en el laboratorio, no funciona. Podemos pasar por encima estos miles y miles de muertos pero la realidad es que, si no retomamos un camino que pueda contribuir a contener de alguna manera la violencia, esto va a seguir, no sé hasta cuándo. Lo cierto es que esta violencia está desempeñando hoy exactamente el mismo papel que despeñó la violencia política hace cuarenta años. Aquella violencia que sirvió de pretexto para el establecimiento de sangrientas dictaduras de seguridad nacional, está sirviendo de motivo para la policización de los distintos países de la región. ¿Qué quiero decir con policización? Centralización de fuerzas policiales, policización y control de toda la población y policización y control de toda la exclusión social en toda nuestra región.

Esta policización ha llegado al extremo de que en un país de la región se ha sancionado una ley sometiendo a pruebas de confiabilidad a los jueces. Prueba de confiabilidad que incluye el sometimiento al polígrafo, detector de mentiras. Semejante lesión a la privacidad y a la dignidad de los magistrados ya nos está indicando que estamos tocando niveles muy bajos y muy graves. Creo que se juega en esto una disyuntiva sobre el modelo de

Estado directamente y también sobre el modelo de sociedad que quiere configurar el Estado. Me parece que está claro que en el mundo hay, en este momento, básicamente dos modelos, con todas las variables folklóricas que podamos tener. De un lado, un modelo de sociedad incluyente, y del otro, un modelo de sociedad excluyente. El Norte nos está tratando de imponer el modelo de sociedad excluyente. Yo no sé si a esta altura, el llamado "Crimen Organizado" es crimen organizado o es "Organización del Crimen" para controlarnos. No lo sé exactamente. Creo que es una cuestión a meditar seriamente. Lo cierto es que nos estamos enfrentando con una base absolutamente autoritaria, de un derecho penal represivo y de medidas policiales represivas que cada día van rompiendo más límites, cada día van avanzando más y, en el fondo, lo que hay detrás de eso es el proyecto de sociedad excluyente. Este proyecto exige permanentemente un aumento de represión y, consiguientemente, un desplazamiento de recursos de programas sociales a programas represivos. El resultado de esto, al final del camino, siempre es la masacre.

No vamos a hacer milagros desde el derecho penal, por supuesto. No podemos vender un producto con calidades falsas, como lo venden los otros. El derecho penal tiene límites. Pero nuestra contribución a ponerle coto al avance represivo del Estado creo que es muy importante y creo que vale la pena intentarlo y que, si se une a otros factores, puede evitar este destino patibulario. Soy optimista en ese sentido, siempre creo que el ser humano no es racional, pero tiene posibilidades de serlo. Siempre tiene posibilidades de ejercer su razón y creo que, aunque los caminos no sean sencillos ni sean rectos, esta posibilidad siempre existe.

En este sentido creo en la función del trabajo regional internacional, en la función que podamos cumplir en los foros mundiales, en el contacto Sur-Sur; no solo reunirnos y tratar de regionalmente tener una política y una conducta común en las asociaciones internacionales sino también en la relación con otros países del Sur, fundamentalmente con África, creo que es sumamente importante.

El Sur plantea problemas que son interesantísimos y que no han sido resueltos. Estamos jugando a una ficción de sociedad homogénea con una homogeneidad cultural, pero solo son ficciones. Vemos a los países de África y vemos a sus estructuras judiciales, que son muy débiles y pequeñas, y cuando preguntamos cómo funciona el control social, nos damos cuenta que en la realidad el control social sigue funcionando como

control social comunitario. Son los consejos de ancianos o las estructuras culturales originarias las que siguen realizando el control social. En algunos países de nuestra región pasa lo mismo, aunque no en la misma medida; pero algunas constituciones ya están reconociendo la justicia comunitaria. Creo que en nuestro país, en algún momento, tendremos que reconocerla para evitar una doble punición. Porque el que pertenece a una cultura originaria sufre la sanción de su cultura originaria —guste o no guste— y la sanción del Estado. Por eso hay una doble punición. De modo que estos problemas son problemas que vamos a tener que resolver y vamos a tener que hacerlo dogmáticamente. Es decir, ha llegado el momento en que nuestra ciencia penal se nutra de una base de realismo con el objetivo de buscar soluciones que disminuyan los niveles de violencia, en la medida de que de nosotros dependa, por lo menos.

No podemos ignorar que en este momento, este modelo de sociedad incluyente que nos está presionando o nos están mandando los poderes hegemónicos mundiales es un modelo que, en cuanto a nuestro saber, fabrica un enemigo. En este momento el principal enemigo que está fabricando son los jueces. Frente a avances demagógicos, mediáticos, generación de victimas héroes, incitación de discursos de venganza, generación de alarma social y pánico moral; hay un enemigo, los jueces. Seamos o no jueces, somos juristas y es nuestro sindicato el que está siendo atacado. No nos equivoquemos, para esta construcción de realidad somos los que protegemos a los delincuentes, somos los que impedimos que se haga justicia, somos los obstáculos para que se erradique el mal, somos algo así como aquellos que —en la época de la Inquisición— negaban el poder de las brujas. No somos las brujas, somos peores enemigos que las brujas porque somos los que negamos el poder de las brujas y por lo tanto, negamos el poder de los inquisidores. En ese contexto es en el que tenemos que pelear. Por eso les decía, no se depriman, pero reconozcamos el contexto.

No estamos en un momento favorable para el avance de los derechos humanos ni estamos en un momento favorable para el avance de la garantías penales, estamos en un momento de abierta agresión. No es la agresión del período entre guerras, no es la agresión de los totalitarismos entre guerras; no está el fascismo, el estalinismo, ni está el *Gulag*. Pero vamos camino a la creación de sociedades *Gulag*, ese es el proyecto; sociedades en las cuales, en cuanto queramos acordarnos, esta policización habrá hecho de nuestra región un enorme *Gulag*, donde todos estemos

controlados —incluso a través del detector de mentiras—, así como el colonialismo hizo de nuestra región un enorme campo de concentración.

Llega el momento de reconstruir nuestro saber penal, no tirando por la borda lo que es la ciencia jurídico penal, de ninguna manera, no podemos desperdiciar la experiencia ni la técnica. Lo que sí tenemos que hacer es reconstruirla conforme a nuestras necesidades. Por supuesto, algunos dirán ¿tenemos que tirar la dogmática alemana? Y no, cuidado. La dogmática es un método universal —puede utilizarse o no, pero se puede usar en cualquier país— eso es lo que le da el carácter de universal. Lo que no es universal son los problemas que se plantean, la agenda. Ella no se dicta desde Alemania ni desde Europa, tenemos que determinarla nosotros. Y nuestra agenda —con esta síntesis bastante caótica que les exponía muy brevemente, porque les podría exponer otros problemas— es mucho más complicada, es propia y es muy distinta de la que nos bajan. No niego la importancia de lo que se va a discutir en Río de Janeiro y hay que ir a discutirlo perfectamente, pero creo que esto no es lo más urgente para discutir entre nosotros. Creo que tenemos temas mucho más urgentes y que hacen al número de cadáveres que se van amontonando en nuestra región.

Estos son justamente los temas por los cuales tenemos que intervenir en las asociaciones internacionales. El Norte no es algo compacto y tampoco es el mal; hay gente inteligente y con buena voluntad, hay mujeres y hombres con visiones universales y hay personas generosas. Tenemos que llevar nuestro discurso para universalizar la AIDP y todas las asociaciones internacionales. Universalizar porque significa contribuir a lo que es el discurso mundial, llevar nuestro aporte, llevar nuestra voz. Pero cuidado, como decía Vasconcelos, no sea el caso que estemos construyendo al hombre cósmico en nuestra región. No, no lo estamos construyendo pero sí estamos construyendo el hombre descolonizado. Muchos me mirarán y dirán que hablo de América Latina y que América Latina es tan diferente y sí, es cierto. América Latina es muy diferente pero tiene un rasgo común. Les recomiendo que tomen la filosofía de la historia de Hegel, la den vuelta y van a encontrar a América Latina. Todo lo que Hegel tira al borde del camino mientras avanza su *Geist*, su espíritu —que más que espíritu siempre me pareció un espectro—, y va tirando muertos al lado del camino; todo eso fue dando o estaba, en nuestra región. Somos los marginados del mundo o resultados de la marginación mundial, del avance de ese *Geist* imperialista que interaccionamos acá, en el mismo continente, casi

en la misma lengua. Somos la síntesis de las culturas que ese espectro letal fue acumulando a la vera de su camino, somos los pueblos originarios que no tenían historia, somos los africanos que se parecían más a los animales que a los seres humanos, somos los árabes sensuales, somos los judíos al servicio de un Dios tiránico y que no conocían la libertad, somos los latinos que no llegan a la verdad absoluta, somos los orientales que están sometidos a la teocracia, somos todo eso que Hegel va tirando y lo tenemos junto e interaccionando. Esa interacción y el sincretismo de todo eso es lo que nos da nuestro producto. Eso es lo que tenemos en común y eso es lo que tenemos que hacer valer a esta hora del mundo, donde parece que los dueños del *Geist* perdieron la punta de la flecha.

En su época Hegel escribía, supuestamente, sentado en la punta de la flecha de lo que él consideraba la Historia. Estar sentado en la punta de la flecha siempre fue una posición incómoda, pero hoy en día la punta de la flecha desapareció. Si miramos lo que está pasando en Europa es para aterrarnos. Si tenemos en cuenta el riesgo del conflicto que se ha producido con Ucrania en este momento, es serio. Si tenemos en cuenta lo que está haciendo Europa con los que huyen de la miseria, del hambre, de la violencia y los deja ahogar en el mar, es como para mirar la civilizada Europa y decir: ¿qué les paso?, ¿qué están haciendo? Se terminaron o han querido archivar para siempre los discursos inclusivos. Europa se olvidó del discurso incluyente de la social democracia —eso ya no corre— y los sociales demócratas se parecen mucho más a los de extrema derecha, y cada día se parecen más. En Estados Unidos, si Roosevelt se levantara, se agarraría la cabeza. ¿Dónde quedo su *New Deal*, su sociedad incluyente con defectos pero con un ciudadano medio trabajador? Cuidado, porque se están radicalizando posiciones de una manera muy grave. En definitiva, se juega a si hay una sociedad en donde quienes detentan la mayor parte de la renta van a repartir un poco o no. Y si se decide que no, a los de abajo hay que tenerlos controlados a garrotazos. Ese es el avance que tiene el derecho penal en este mundo.

Y en nuestra región, esto que no sabía cómo definir, que no sé si es el *Organized Crime* o *The Crime Organization*, es dramático. El país que es consumidor del producto de la economía primaria —que hemos metido en los mercados centrales—, la cocaína, tiene una red de distribución en la cual le queda el 60% del producto del tráfico. Desde el Río Bravo para el Sur tenemos producción en los países andinos, circulación hasta Centroamérica, introducción a través de México y competencia por alcanzar el mercado con-

sumidor entre distintas bandas narcos. Nos quedamos con el 40% de la renta. El país del Norte consume, y además le vende armas a los narcos del Sur, y además se queda con el 100% del monopolio del servicio ilícito del recicle del lavado del dinero. Nosotros nos quedamos con los muertos y ellos, con la renta. Y además usan la violencia que todo esto está produciendo para controlar y policizar nuestro países. Esa es la real situación en este momento.

Me preguntan ¿y qué pasa con nosotros? No lo sé. Hasta este momento si no se produce un cambio, que puede ser que se esté produciendo —cosa que no estoy afirmando—, a la larga todo producto de economía primaria es reemplazado por sintéticos. Si se está produciendo un cambio de consumo en el Norte por los sintéticos y si es cierto que está bajando el consumo de cocaína en el Norte, es probable que se busquen nuevos mercados y una triangulación a través del cono Sur. No lo sé, no lo afirmo. Es muy difícil tener datos exactos y reales de esto, pero ese es el único riesgo que corremos de momento en esta subregión.

Pero no seamos egoístas, no seamos mezquinos, no dejemos de ver lo que está sucediendo en toda la región. Y me pregunto ¿qué es lo que mata más? ¿los tóxicos prohibidos —dejando de lado el alcohol que mata— o la prohibición misma? Creo que México hubiera necesitado doscientos años para tener 70 mil muertos por sobredosis de cocaína, ahora los tuvo en cinco años por concentración de plomo. Esa es la realidad de la región. Pensemos en términos regionales. Pensemos que es indispensable que nos insertemos en las grandes asociaciones internacionales para llevarles este discurso. Es necesario que nos entendamos con las otras regiones del planeta, que nos metamos a saber qué pasa en los otros Sures, qué pasa en África, qué pasa en las zonas del hemisferio Sur que nos parecen extrañas y exóticas. Siempre el dominio del Norte hacia el Sur se basó en la incomunicación Sur-Sur. Creo que lo elemental para nuestra política, en este aspecto, es tomar conciencia regional, unificar discursos, llevar el discurso a los planos mundiales y relacionarnos con los otros dramas que se viven en el propio hemisferio Sur.

No desprecio que se trate el tema que se va a tratar en Río de Janeiro, por supuesto. Pero espero que, y lo he hablado con agentes de la directiva internacional de la AIDP, de este modo logremos volver a mundializar la Asociación Internacional de Derecho Penal y volver a priorizar los temas que deben preocuparnos ante todo. Porque ante todo, lo que debe preocuparnos, es la vida humana.

Muchísimas gracias.

ÍNDICE

Perspectiva del Derecho Penal. Parte General

Sección 1

Panel 1

Perspectiva del Derecho Penal. Parte Especial

Sección 2

Panel 2

Perspectiva del Derecho Procesal Penal

Sección 3

Contribuciones a la Jornada

Perspectiva del Derecho Penal

Parte General

COLOQUIOS PREPARATORIOS PARA EL XIX CONGRESO INTERNACIONAL DE DERECHO PENAL: "SOCIEDAD DE LA INFORMACIÓN Y DERECHO PENAL" (1)

Sección 1

Documento de reflexión y cuestionario de la AIDP
Relator General: **THOMAS WEIGEND**

Respuestas del Grupo Nacional Argentino:
JAVIER A. DE LUCA, MARCELO RIQUERT, CHRISTIAN C. SUEIRO, MARÍA ÁNGELES RAMOS y **FRANCISCO FIGUEROA**

(A) Objeto del cuestionario

Las preguntas de esta Sección tratan generalmente del "ciberdelito". Este término se entiende en el sentido de dar cobertura a las conductas criminales que afectan a intereses asociados con el uso de la tecnología de la información y comunicación (TIC), como el funcionamiento adecuado de los sistemas de ordenadores y de internet, la intimidad y la integridad de los datos almacenados o transferidos a o a través de las TIC o la identidad virtual de los usuarios de internet. El denominador común y rasgo característico de todas las figuras de ciberdelitos y de la investigación sobre estos, puede hallarse en su relación con sistemas, redes y datos de ordenadores, de un lado, y con los sistemas, redes y datos cibernéticos, del otro. El ciberdelito cubre delitos que tienen que ver con los ordenadores en sentido tradicional y también con la nube del ciberespacio y las bases de datos cibernéticas.

Si se precisa cualquier aclaración, por favor, contactar con el Relator General, Prof. Dr. Thomas Weigend por email: thomas.weigend@uni-koeln.de

(B) Criminalización

Nótese, por favor, que en este cuestionario solo son de interés las cuestiones relativas a las características generales de las tipificaciones de las figuras delictivas del ciberdelito. Las cuestiones específicas concernientes

(1) AIDP, Río de Janeiro, Brasil, 31 de agosto al 6 de septiembre de 2014.

a las definiciones de figuras individuales serán objeto de debate en la Sección II del Congreso.

(1) ¿Qué bienes jurídicos específicos se considera que deben ser protegidos por el derecho penal (e. g. integridad de los sistemas procesadores de datos, privacidad de los datos almacenados)?

La legislación de la República Argentina, en particular la ley 26.388 en materia de criminalidad informática, no creó bienes jurídicos autónomos o específicos de delitos informáticos.

Los bienes jurídicos que han sido alcanzados por la reforma son: 1) Delitos contra la integridad sexual; 2) Delitos contra la libertad, específicamente la violación de secretos y de la privacidad; 3) Delitos contra la propiedad (antes, también por ley 25.930); 4) Delitos contra la Seguridad Pública; 5) Delitos contra la Administración Pública.

Es así que la ley 26.388 alcanzó con su reforma un número muy limitado y específico de tipos penales como lo son: 1) Ofrecimiento y distribución de imágenes relacionadas con pornografía infantil (art. 128 del Código Penal; en adelante, CP); 2) Violación de la correspondencia electrónica (art. 153 CP); 3) Acceso ilegítimo a un sistema informático (art. 153 *bis* CP); 4) Publicación abusiva de correspondencia (art. 155 CP); 5) Revelación de secretos (art. 157 CP); 6) Delitos relacionados con la protección de datos personales (art. 157 *bis* CP); 7) Defraudación informática (art. 173, inc. 16 CP); 8) Daño (arts. 183 y 184 CP); 9) Interrupción o entorpecimiento de las comunicaciones (arts. 197 CP); 10) El tipo penal de alteración, sustracción, ocultación, destrucción e inutilización de medios de prueba (art. 255 CP), a lo cual debe agregarse las modificaciones terminológicas realizadas en el art. 77 CP.

Además, a través de modificaciones e inserciones en leyes especiales, se han considerado otros bienes jurídicos, a saber: a) secreto empresarial (por ley 24.766); b) hacienda pública (por leyes 24.769 y 26.735); c) propiedad intelectual (por ley 25.036); d) servicios de comunicaciones móviles (por ley 25.891).

(2) Por favor, dar ejemplos típicos de leyes penales relativas a:

(a) ataques contra sistemas TIC

Puntualmente, se contempla el ataque a los sistemas informáticos tanto tangibles (Hardware) como intangibles (Software) en el tipo penal de daño simple y agravado (arts. 183 y 184 CP).

En similar dirección, se contempla la alteración dolosa de registros fiscales y la adulteración de controladores fiscales (arts. 12 y 12 *bis* de la ley 24.769); la alteración de número de línea, de número de serie electrónico o mecánico del equipo terminal o módulo de identificación removible de usuario de Servicios de Comunicaciones Móviles (SCM); la alteración de componente de una tarjeta de telefonía, el acceso a los códigos informáticos de habilitación de créditos de servicio SCM o el aprovechamiento ilegítimo de estos últimos (arts. 10 y 11, ley 25.891).

(b) violación de la privacidad TIC

Específicamente, el Código Penal de la Nación Argentina, previó en su título Violación de Secreto y de la privacidad, los siguientes tipos penales: 1) Violación de correspondencia electrónica (art. 153 CP), 2) Acceso ilegítimo a un sistema informático (art. 153 *bis* CP), 3) Publicación abusiva de correspondencia (art. 155 CP), 4) Revelación de secretos (art. 157 CP), 5) Delitos relacionados con la protección de datos personales (art. 157 *bis* CP).

Los arts. 2 y 12 de la ley 24.766/97 protegen la violación de la confidencialidad sobre información y productos que estén legítimamente bajo control de una persona y se divulgue indebidamente, de manera contraria a los usos comerciales honestos.

(c) falsedad forgery *y manipulación de los datos almacenados digitalmente*

Puntualmente, se prevé la figura de defraudación informática (art. 173, inc. 16 CP), que es más específica que la de defraudación a sistemas automatizados o con tarjetas de crédito y débito (art. 173, inc. 15 CP).

(d) distribución de virus de ordenadores

El tipo penal de daño previsto en el art. 183, 2° párr CP, prevé como conducta típica "la venta, distribución, puesta en circulación o introducción en un sistema informático, de cualquier programa destinado a causar daños".

(e) delitos relativos a las identidades virtuales de los usuarios, e. g., forging, *sustracción o daño de personalidades virtuales*

No existe una figura específica, pero cualquier adulteración de datos personales puede quedar subsumida en los delitos relacionados con la protección de datos personales (art. 157 *bis* CP).

El 13/05/10, por disposición 7/2010, la Dirección Nacional de Protección de Datos Personales creó el "Centro de Asistencia a las Víctimas de Robo de Identidad".

(f) otras prohibiciones penales innovadoras en el área de las TIC y de Internet, e. g., incriminación de la creación y posesión de ciertas imágenes virtuales, violación de derechos de autor en la esfera virtual

La producción, financiación, ofrecimiento, comercialización, publicación, facilitación, divulgación y distribución de imágenes de toda representación de actividades sexuales explícitas o toda representación de sus partes genitales con fines predominantemente sexuales en el que participaren menores (art. 128 CP).

La defraudación de derechos de propiedad intelectual está prevista en el art. 71 y ss. de la ley 11.723 (ver mod. por ley 25.036).

(3) ¿Cómo se define típicamente la conducta criminal (actus reus) en estos delitos (describiendo el acto, el resultado, otros)? ¿Cómo se define el objeto ("dato", "escritos", contenidos)?

El legislador ha sido muy respetuoso del principio de legalidad y, en la mayoría, de los tipos penales ha descripto la conducta o acción típica.

Desde una perspectiva criminológica, la ley 26.388, de reforma en materia de criminalidad informática al Código Penal de la Nación, no exhibe una remisión terminológica y conceptual a la Escuela Positivista de la Criminología y, en tal sentido, no ha recurrido a una clasificación biotipológica o, en este caso puntual, cibertipológica de autores.

En tal sentido, la presente ley 26.388 en ninguno de los tipos penales contemplados ha recurrido al empleo de una Biotipología de autores de la criminalidad informática o Cibertipología como pueden ser las designaciones de: 1) *Hacker*;[2] 2) *Cracker*;[3] 3) *Preaker o Phreaker*;[4] 4) *Phisher*;[5] 5) *Sniffer*;[6]

(2) Ver Chiaravalloti Alicia y Ricardo Levene (h.), "Delitos informáticos. Segunda Parte", en *La Ley* 1998-F, 976; Fillia, Leonardo C.; Monteleone, Romina; Nager, Horacio S.; Sueiro, Carlos C., *Análisis integrado de la Criminalidad Informática*, prólogo de Carlos Alberto Elbert, Bs. As., Editorial Fabián J. Di Plácido, 2007, p. 117; Tobares Catalá, Gabriel H. ; Castro, Argüello Maximiliano J., *Delitos Informáticos*, prólogo de Marcelo J. Sayago, Córdoba, Advocatus, 2010, p. 97.

(3) Ver Chiaravalloti Alicia y Ricardo Levene (h.), *ibid.*; Fillia, Leonardo C.; Monteleone, Romina; Nager, Horacio S.; Sueiro, Carlos C., *ibid.*, p. 118; Tobares Catalá, Gabriel H. ; Castro, Argüello Maximiliano J., *ibid.*, p. 99.

(4) Ver Chiaravalloti Alicia y Ricardo Levene (h.), *ibid.*; Fillia, Leonardo C.; Monteleone, Romina; Nager, Horacio S.; Sueiro, Carlos C., *ibid.*, p. 118.

(5) Ver Fillia, Leonardo C.; Monteleone, Romina; Nager, Horacio S.; Sueiro, Carlos C., *ibid.*, p. 119.

(6) Rosende Eduardo E., "El intrusismo informático. Reflexiones sobre su inclusión en el Código Penal", en *Suplemento La Ley Penal y Procesal Penal*, Bs. As., La Ley, 27/05/2008, p. 21.

6) *Virucker*;[7] 7) *Propagandista informático*,[8] 8) *Pirata Informático*,[9] o 9) *Cyberbullyng o Ciber-Acosador*.

La mayoría de los tipos penales son tipos penales de resultado; por ejemplo daño, defraudación, interrupción de comunicaciones, etc.

Sin perjuicio de la utilización de referencias al objeto como "datos", "documentos", "información registrada", en la parte general del Código, se incorporaron por la ley 26.388 estos tres últimos párrafos al art. 77 CP:

> "El término documento comprende toda representación de actos o hechos, con independencia del soporte utilizado para su fijación, almacenamiento, archivo o transmisión.
>
> Los términos firma y suscripción comprenden la firma digital, la creación de una firma digital o firmar digitalmente.
>
> Los términos instrumento privado y certificado comprenden el documento digital firmado digitalmente".

(4) ¿Se limita a determinados grupos de autores y/o víctimas la responsabilidad penal por ciertos ciberdelitos?

Nuestra legislación penal no posee tipos penales con sujetos activos calificados o grupos de autores.

No obstante, la calidad personal del agente puede operar como calificante. Así, en el art. 157 *bis* CP, cuando el autor sea funcionario público, sufrirá, además, pena de inhabilitación especial. La ley 25.891 establece un agravante genérico que incrementa las penas mínimas y máximas en un tercio: la autoría por dependientes de empresas licenciatarias de SCM o por quienes, atento al desempeño de sus funciones, posean acceso a las facilidades técnicas de aquellas.

---

(7) Ver Riquert Marcelo A., *Informática y Derecho Penal Argentino*, Bs. As., Ad-Hoc, 1999, p. 57; Fillia Leonardo César, Monteleone Romina, Nager Horacio Santiago, Sueiro Carlos Christian, *Análisis integrado de la Criminalidad Informática*, Prólogo Carlos Alberto Elbert, Bs. As., Fabián J. Di Plácido, 2007, p. 120; Tobares Catalá Gabriel H., Castro Argüello Maximiliano J.; *Delitos Informáticos*, Prólogo de Marcelo J. Sayago, Córdoba, Advocatus, 2010, p. 101.

(8) Riquert Marcelo A., *ibid.,* p. 57; Fillia Leonardo César, Monteleone Romina, Nager Horacio Santiago, Sueiro Carlos Christian, *Análisis integrado de la Criminalidad Informática*, Prólogo Carlos Alberto Elbert, Bs. As., Fabián J. Di Plácido, 2007, p. 120.

(9) Ver Riquert Marcelo A., *ibid.,* p. 57.

Respecto a las víctimas, solo se destaca la protección de los menores respecto de la venta, producción, difusión, facilitación y publicidad de material pornográfico.

En el art. 153 *bis* CP se califica (agrava) la conducta de intrusismo cuando el acceso fuese en perjuicio de un sistema o dato informático de un organismo público estatal o de un proveedor de servicios públicos o de servicios financieros.

A su vez, el art. 184 CP considera agravado el daño cuando recae sobre datos, documentos, programas o sistemas informáticos públicos (inc. 5) o en sistemas informáticos destinados a la prestación de servicios de salud, de comunicaciones, de provisión o transporte de energía, de medios de transporte u otro servicio público (inc. 6).

(5) ¿Se extiende la responsabilidad penal en el área de las TIC a las conductas meramente imprudentes o negligentes?

La legislación penal argentina posee un tipo penal imprudente en materia de criminalidad informática.

Este tipo penal doloso abarca la alteración, sustracción, ocultación, destrucción e inutilización de medios de prueba. Esta figura prevé su modalidad imprudente en el segundo párrafo del art. 255 CP:

> "Será reprimido con prisión de un (1) mes a cuatro (4) años, el que sustrajere, alterare, ocultare, destruyere o inutilizare en todo o en parte objetos destinados a servir de prueba ante la autoridad competente, registros o documentos confiados a la custodia de un funcionario público o de otra persona en el interés del servicio público. Si el autor fuere el mismo depositario, sufrirá además inhabilitación especial por doble tiempo.
>
> Si el hecho se cometiere por imprudencia o negligencia del depositario, éste será reprimido con multa de pesos setecientos cincuenta ($750) a pesos doce mil quinientos ($12.500)".

(6) ¿Hay diferencias específicas entre la definición de los ciberdelitos y los delitos "tradicionales"?

No existe distinción en nuestra legislación. Más allá de haberse producido la reforma legislativa en forma asistemática y mediante normas no contemporáneas, mediando una suerte de diáspora de tipos penales en leyes

especiales y en el Código Penal, al producir una actualización integral del último por la ley 26.388, no se marcaron diferencias.

(C) Técnica legislativa

(1) ¿Hay problemas específicos respecto del principio de legalidad (e. g., vaguedad, remisiones abiertas por parte del tipo penal a otras normativas)?

En general, los tipos penales resultan sumamente respetuosos del principio de legalidad. Es más, para evitar la constante remisión a otras normas, se ha introducido, a través del art. 77 CP, un glosario de terminología.

(2) ¿Cómo evita la legislación los efectos chilling indebidos sobre el uso legítimo de las TIC o de internet?

No se advierten medidas expresas en la legislación vigente dirigidas a evitar que las tipicidades asumidas pudieran tener alguna derivación negativa, inhibitoria o restrictiva sobre los usos legítimos de las TIC o de Internet.

(3) ¿Cómo evita la legislación penal el peligro de convertirse en obsoleta a la vista de la rápida innovación tecnológica?

- ¿cómo se tienen en cuenta los cambios en el uso de internet y las redes sociales?

En particular el uso de Internet, de las redes sociales como así también de gran parte de dispositivos móviles, no modifica las conductas típicas. A lo sumo, son nuevas herramientas para realizar las acciones ya contempladas en los tipos penales previstos por la reforma.

En algún caso, como en la regulación del SCM por la ley 25.891, se incorporó en los tipos penales, como el art. 12, una fórmula como la siguiente: "o la tecnología que en el futuro la reemplace".

- ¿cómo se adapta la legislación al progreso tecnológico (e. g., mediante la remisión a las normas administrativas)?

A través de muy paulatinas reformas al Código Penal de la Nación.

O mediante modificaciones en algunas de las numerosísimas leyes especiales penales vigentes (alrededor de 70, al presente), por lo que la nota distintiva sería la de falta de sistema, armonía y coherencia, aun cuando esto no sería algo particular de los delitos vinculados a las TIC, sino del ordenamiento punitivo nacional.

(D) Alcance de la incriminación

(1) ¿En qué medida la legislación penal alcanza a meros actos preparatorios que conllevan un riesgo de abuso ulterior, p. e., adquisición o tenencia de software que puede ser empleado para "hacking", "phishing", fraude de computadoras o elusión de las barreras de protección? En caso afirmativo ¿la introducción de tales leyes suscitó controversias? ¿Se han hecho esfuerzos legislativos específicos para prevenir la sobrecriminalización?

Nuestra legislación pena la mera intrusión informática o acceso ilegítimo a un sistema informático (art. 153 *bis* CP).

No hubo mayores controversias públicas, habiéndose ceñido la discusión a ámbitos académicos reducidos y sin mayor impacto externo. Los esfuerzos legislativos en adaptar la normativa a las nuevas modalidades de ataque a los viejos bienes jurídicos protegidos ha sido tardía y se ha producido luego de un largo reclamo de solución a problemas de lagunas de punición verificados jurisprudencialmente.

(2) ¿En qué medida la mera posesión o tenencia de ciertos datos resulta incriminada? ¿En qué áreas y con base en qué fundamentos? ¿Cómo se define la "posesión" o "tenencia" de datos? ¿Incluye la definición la posesión temporal o el mero visionado?

La posesión de datos personales resulta criminalizada. El elenco de figuras típicas vigentes no pune la mera posesión o tenencia de datos, sino otras conductas vinculadas como, por ej., el acceder a ellos, destruirlos, modificarlos con posible perjuicio o difundirlos públicamente (siendo privados) o facilitar su acceso a no autorizados.

(3) En la medida en que la posesión o el favorecimiento del acceso a ciertos datos hayan sido definidas como infracciones penales, ¿la responsabilidad penal se extiende a los proveedores de servicios (e. g., proveedores de acceso o alojamiento)? ¿Cuáles son las exigencias para su responsabilidad, especialmente en lo que se refiere al tipo subjetivo (mens rea)? ¿Están los proveedores obligados al seguimiento y control de la información que suministran o para la que ofrecen acceso? ¿Están obligados a dar información sobre la identidad de los usuarios? ¿Están obligados a impedir el acceso a ciertas informaciones? En caso afirmativo, ¿en qué condiciones y a qué coste? ¿Puede generar responsabilidad penal la violación de esas obligaciones?

La responsabilidad penal de los proveedores se rige por las reglas generales de la participación criminal. No hay normas particulares con relación a

ellos en el ámbito penal. Sí existen numerosas previsiones administrativas, incluyendo las de orden sancionatorio, vinculadas al ejercicio de su rol dentro del sistema de comunicaciones.

(4) ¿Qué limitaciones generales y, en particular constitucionales, han sido objeto de debate al incriminar conductas relativas a los crímenes concernientes a las TIC y a internet (e. g., libertad de expresión, libertad de Prensa, libertad de asociación, intimidad, "principio de ofensividad", exigencia de un acto, no mera responsabilidad por resultado (exigencia de mens rea)?

Las principales objeciones han resultado como consecuencia de la posible afectación a la libertad de expresión y prensa.

En menor nivel, medió preocupación por posibles afectaciones a la intimidad (así lo entendió la Corte Suprema Justicia Nación en el caso "Halabi", al declarar inconstitucional a la ley 25.873 en cuanto preveía la preservación por diez años de los datos de tráfico).

(5) ¿Prevé la ley sanciones penales específicamente dirigidas a los ciberdelincuentes (e. g., inhabilitación o suspensión temporal del el uso de internet)?

No existe una legislación que distinga tipos de autores y, en función de ellos, penas específicas.

(E) Alternativas a la criminalización

(1) ¿Qué papel juega el derecho penal en relación con otras formas de combate del abuso de TIC y de internet? ¿Qué relación existe entre las sanciones civiles y administrativas (pago de los daños, cierre de la empresa, etc.) y las sanciones penales en el área de las TIC?

Ninguno específico distinto a cualquier otro campo de la criminalidad.

(2) ¿Qué medios no penales de combate contra las websites ofensivas se usan/difunden (e. g., cierre de las websites, bloqueo del acceso a las websites)?

Ninguno.

(3) ¿En qué medida se espera de los usuarios de las TIC que apliquen medidas de autoprotección (p. e., encriptación de mensajes, uso de passwords, uso de software de protección)? ¿Se prevén sanciones para la no protección del propio ordenador hasta cierto punto, ej, usando software antivirus o protegiendo con password el acceso a redes

privadas? ¿La ausencia de razonable autoprotección supone un medio de defensa de los acusados por entrada ilícita o por abuso ilícito de la red de otra persona o de sus datos?

No existen hasta el momento campañas de autoprotección públicas en las cuales se concientice a los usuarios sobre el uso de programas de encriptación o protección de datos.

(F) Límites al anonimato

(1) ¿Hay leyes o reglamentos que obliguen a los proveedores de internet a almacenar los datos personales de los usuarios, incluyendo el historial del uso de internet? ¿Pueden los proveedores ser obligados a suministrar esos datos a la policía?

Por el contrario, a partir de la sentencia de la CSJN en el caso "Halabi, Ernesto", se declaró la inconstitucionalidad del almacenamiento de información personal por parte de los proveedores de Internet.

Se hizo hincapié en que el problema era la previsión excesiva, de 10 años, cuando en derecho comparado son 1 o 2 años.

(2) ¿Obligan las leyes o reglamentos a los suministradores de servicios de internet al registro de los usuarios con carácter previo al suministro de los servicios?

No se encuentra previsto en forma legal. Sin embargo, existen una gran cantidad de resoluciones administrativas y de reglamentaciones que regulan la prestación de servicios de Internet.

(3) ¿Limitan las leyes o reglamentos las posibilidades de encriptación de archivos o mensajes en internet? ¿Pueden los sospechosos ser obligados a disclose los passwords que usan?

La República Argentina no posee una figura específica que sancione la encriptación de archivos como ocurre en los Estados Unidos de América o Gran Bretaña e Irlanda del Norte. La mera encriptación de archivos no es delito en la República Argentina. Por el contrario, es una eficiente medida de autoprotección de datos personales.

(G) Internacionalización

(1) ¿Se aplica la legislación doméstica a los datos ingresados en internet desde el extranjero? ¿Hay una exigencia de "doble incriminación" para el ingreso de datos desde el extranjero?

(2) ¿En qué medida el derecho penal de su país en el área de las TIC y de internet se ha visto influido por los instrumentos jurídicos internacionales?

La ley 26.388 también ha seguido los lineamientos establecidos por el Convenio sobre la Ciberdelincuencia de Budapest, del 23 de noviembre de 2001.[10]

En este sentido, ha incorporado definiciones terminológicas en el art. 77 CP, teniendo en consideración las definiciones suministradas por el "Convenio sobre la Ciberdelincuencia de Budapest", en su art. 1 destinado a "Definiciones", perteneciente al Capítulo I, dedicado a la "Terminología".

En particular, también ha tenido presente este instrumento internacional para la redacción y descripción de la conducta típica del delito de ofrecimiento y distribución de imágenes relacionadas con pornografía infantil y tenencia de imágenes con fines de distribución (art. 128 CP), incorporando los verbos típicos establecidos su art. 9. En general, en lo referente a la modificación de los tipos penales alcanzados por la ley 26.388, ha tomado en consideración el Capítulo II —"Medidas que deberán adoptarse a nivel nacional"—, Sección 1 —"Derecho penal sustantivo"—, para delimitar qué figuras penales indefectiblemente debían ser abarcadas por la reforma.

(3) ¿Participa su país en debates sobre la armonización de la legislación relativa a los ciberdelitos (como el grupo de expertos intergubernamentales de las NN.UU sobre cibercrimen)?

Puntualmente, la Argentina participa de debates de armonización de su legislación en el MERCOSUR y UNASUR.

(H) Desarrollos futuros

Indique, por favor, las líneas actuales del debate jurídico y legislativo en su país concerniente a los delitos de internet y relativos a la TIC.

En la actualidad, a través de la ley 26.685 se prevé la implementación gradual del expediente digital, firma, notificación y constitución de domicilios electrónicos. De igual forma, la CSJN, por medio de su Acordada 31/11, estipula la introducción gradual de la notificación electrónica.

(10) Ver Convenio sobre la ciberdelincuencia, Budapest, 23/11/2001, Serie de Tratados Europeos nº 185, *Council of Europe / Conseil de L´Europe*.

Se ha presentado un proyecto[11] para tipificar en el CP la figura del robo de identidad digital, insertándola como art. 138 *bis* con la siguiente redacción:

> "Será reprimido con prisión de seis meses a tres años o multa de pesos veinte mil a pesos doscientos mil, el que sin consentimiento, adquiriere, tuviere en su posesión, transfiriere, creare o utilizare la identidad de una persona física o jurídica que no le pertenezca a través de Internet o cualquier otro medio electrónico, y con la intención de dañar, extorsionar, defraudar, injuriar o amenazar a otra persona u obtener beneficio para sí o para terceros".

También son objeto de debate la posible incriminación de conductas tales como: 1) La ciberocupación o registro impropio de nombres de dominio;[12] 2) El *spamming* o correo basura o publicidad no solicitada;[13] 3) La captación ilegal y difusión de datos, imágenes y sonidos;[14] 4) La posesión simple de material pornográfico infantil; 5) La responsabilidad de los proveedores.[15]

(11) Por los senadores Marías de los Ángeles Higonet y Carlos Verna. Fuente: *Diario Judicial* del 28/05/2012.

(12) Ver Riquert Marcelo A., *Delincuencia Informática en Argentina y el Mercosur*, Prólogo de David Baigún, Bs. As., Ediar, 2009, pp. 202/204.

(13) Ver Riquert Marcelo A., *ibid.*, pp. 204/206.

(14) Ver Palazzi Pablo A., *"Los Delitos Informáticos en el Código Penal. Análisis de la ley 26.388"*, Bs. As., Editorial Abeledo Perrot, Bs. As., 2009, pp. 159/166, quien se inclina por su no punición y su amparo a través del derecho civil. También ver Riquert Marcelo A., *Delincuencia Informática en Argentina y el Mercosur*, *ibid.*, pp. 206/207, quien considera prudente y acertado postergar su punición hasta que exista un serio debate en torno a esta figura penal.

(15) Ver Tomeo, Fernando, "Responsabilidad penal de los administradores de sitios Web. El caso Taringa!", en *La Ley,* Bs. As., 1 de junio de 2011. También se sugiere ver Granero, Horacio R., "La naturaleza jurídica de la nube (*cloud computing*)", en el *elDial.com,* Suplemento de Alta Tecnología, 09/09/2009, elDial.com DC11A9; Velazco San Martín Cristo, "Aspectos jurisdiccionales de la computación de la nube", en el *elDial.com,* Suplemento de Alta Tecnología Suplemento de Alta Tecnología, 14/04/2010, elDial.com DC1304; Elizalde, Marín Francisco, "La prueba en la Cloud Computing: Cloud Computing & Service Level Agreements. El modelo en los Estados Unidos de América y su proyección al ámbito local argentino", en el *elDial.com,* Suplemento de Alta Tecnología, 08/06/2011, elDial.com DC15EE; Teijeiro, Nicolás, "La protección constitucional de la intimidad en Internet con especial referencia a redes sociales", en el *elDial.com,* Suplemento de Alta Tecnología, 08/06/2011, DC15EF.

Panel 1

Responsabilidad penal de los proveedores de servicios de Internet

NORA A. CHERÑAVSKY[1]

1. Introducción

El presente trabajo tiene por objeto abordar el espinoso tema de la responsabilidad penal los Prestadores de Servicios de Internet (en adelante, ISP).

Se analizarán las tensiones entre el derecho a la información y libre circulación de contenidos y el derecho a la preservación de la seguridad, la privacidad, la confidencialidad y la integralidad de los datos y contenidos de los usuarios y de terceros que circulan por las redes globales.

Por último, se intentará aportar fundamentos en favor de un criterio de política criminal consistente en el reconocimiento de los ISP como sujetos de imputación de normas penales en tanto tienen gran capacidad tecnológica para cometer infracciones y afectar bienes jurídicos, y porque tienen un rol preponderante en el acceso, alojamiento y facilitamiento de búsqueda e intercambio de contenidos que circulan por la red global.

---

(1) Abogada. Profesora Adjunta Regular del Departamento de Derecho Penal y Procesal Penal (UBA). En el Ministerio de Justicia fue designada Punto Focal en materia de Ciberdelito durante los años 2006 y 2009. Fue integrante de la Comisión Interministerial que redactó Proyecto de Ley de Delitos Informáticos del año 2006. Participó como asesora en la Comisión de Reforma al Código Penal del año 2006 y como Asesora en el Senado para la sanción de la Ley de Delitos Informáticos del año 2008 (de reforma al Código Penal). Asimismo, participó de la Comisión Interministerial de análisis de la Convención de Budapest durante el año 2008. Directora General de Asuntos Jurídicos de ANSES.

2. Discusión previa

A nivel internacional la discusión en torno a la responsabilidad penal de las corporaciones parte de la existencia de dos grandes modelos: el anglosajón que consagra la responsabilidad vicaria o funcional para imputar a la corporación por los hechos de sus representantes y el romano-germánico que parte de la culpa del sujeto individual y establece consecuentemente que las sanciones criminales pueden imponerse solo a las personas físicas que actúan con autoconciencia y libertad en el seno de la persona jurídica, sin perjuicio de aceptar alguna consecuencia accesoria o medida de seguridad si se considera al ente como un sujeto peligroso, incapaz de culpabilidad.(2)

Sin embargo, puede señalarse una evolución en el derecho europeo continental que tiende a ampliar la responsabilidad de las personas jurídicas al ámbito penal, sin perjuicio de la correspondiente responsabilidad civil o administrativa, según sea la intensidad de la afectación del bien jurídico.

A nivel del derecho europeo continental se puede observar un giro de las legislaciones hacia al establecimiento de la Responsabilidad Penal de las Personas Jurídicas (RPPJ) a partir del modelo adoptado por Holanda hacia mediados de los setenta, Francia y Bélgica en los noventa y España que adopta un sistema de consecuencias accesorias, Italia que en 2001 introdujo la RPPJ, aunque sin darle esa denominación, y Alemania que sigue adscribiendo a un sistema de responsabilidad de tipo administrativo o contravencional para las personas jurídicas.

En el marco de la Unión Europea y en el ámbito regional se recomienda implementar este tipo de responsabilidad para la delincuencia organizada transnacional, el cohecho de funcionarios públicos extranjeros, los delitos ambientales, terrorismo, ciberdelito, criminalidad económica y corrupción, recomendando la adopción por parte de los Estados de sanciones para las personas jurídicas a concretarse tanto por la vía administrativa o penal, pudiendo ser las mismas de diverso contenido, pero adecuadas tanto a la

(2) Véase la referencia a la discusión en Cherñavsky, Nora, "Fundamentación del castigo a las personas corporativas", *Revista de Derecho Penal y Procesal Penal*, fasc. 7, Bs. As., 2008. Algunos autores sostienen que la reacción penal es la más idónea para combatir a este factor criminógeno que es la empresa. Defienden la aplicación de medidas preventivo-especiales basadas en la peligrosidad objetiva o instrumental de la agrupación aplicados por órganos jurisdiccionales penales. Ver Feijoó Sánchez, Bernardo, "Sobre el fundamento de las sanciones penales para Personas Jurídicas", en la obra *La Responsabilidad Penal de las Personas Jurídicas, Órganos y Representantes*, Ara Editores, 2002, p. 263.

prevención del delito como proporcionadas al patrimonio de la empresa y eficaces para contrarrestar los hechos delictivos y conjurar los peligros inherentes a la "sociedad de riesgos".

De este modo ha quedado definida en las principales convenciones internacionales la responsabilidad de los Estados para dar adecuada respuesta a los riesgos creados por las personas jurídicas, tal como se expresa en sentencia del Tribunal Europeo de Derechos Humanos en el caso *Öneryildiz v. Turquía*.[3]

En la evolución son en principio las leyes dictadas en el campo de los delitos económicos (aduanero, tributario, del consumidor, de medio ambiente) las que van a reconocer en forma acumulativa o subsidiaria la cualidad de autor y la punibilidad de las personas jurídicas.

Así, la RPPJ comienza a ser reconocida por las acciones u omisiones dolosas de sus directores, empleados u otros agentes en el marco de la relación de empleo, es decir, en forma transferida o inclusive directa a través del modelo del "defecto de organización" que refiere a la culpabilidad organizacional.

El mundo anglosajón , con un sentido más utilitario, considera al derecho penal como una herramienta regulatoria de la vida social, y que como tal, debe controlar a los diferentes actores sociales (sean entes físicos o personas morales o colectivas).

En el derecho continental, en cambio, prevalece la idea de que el único sujeto capaz de ser moralmente responsable de sus actos es la persona física dotada de autoconciencia y libertad,[4] razón por la cual ha receptado más tardíamente este tipo de responsabilidad penal colectiva o de organización.

3. Responsabilidad penal de la persona jurídica en el ciberespacio

El ciberdelito es pluriofensivo y tiene características transnacionales, ya que puede cometerse mediante una computadora o una red de computadores u otros dispositivos móviles situados dentro de un territorio nacional, pero con capacidad ofensiva para afectar a sujetos que se encuentran fuera del ámbito territorial del que proviene el ataque.

(3) Ver sitio oficial del TEDH, [en línea] www.echr.coe.int

(4) Engisch, Karl, *Teoría de la libertad de la Voluntad*, Montevideo, BdeF, p. 62 y ss., Schopenhauer, Arthur, *Ensayo sobre el Libre Albedrío*, Colección Pensadores Universales, Bs. As., Gradifco, p. 7 y concordantes.

En el mundo virtual, hasta hace poco tiempo se carecía de legislación sobre delitos informáticos para responsabilizar siquiera a personas físicas que cometieran delitos a través del medio digital.

Actualmente, casi la totalidad de los países poseen legislación contra el ciberdelito, incluida la Argentina que en el año 2008 sancionó la Ley de Delitos Informáticos que reformó el Código Penal,[5] adaptando delitos tradicionales al entorno digital.

Si bien hay acuerdos de armonización en la tipificación de los hechos delictivos cometidos por la red global, no los hay acerca de los sujetos que pueden infringir la ley penal.

Los autores señalan una serie de problemas teóricos y prácticos ligados a la determinación de responsabilidad penal en aquellos ordenamientos jurídicos en los que rige el principio *societas delinquere non potest*. No obstante, países como España han consagrado la RPPJ para el daño informático (LO 5/2010); la ley chilena 20.903 del 2009, para delitos de lavado de dinero y cohecho; al tiempo que en Argentina se consagra la misma en leyes especiales como las de abastecimiento, control de cambios, código aduanero, etc.

La problemática de la responsabilidad penal de las personas colectivas en el ámbito de Internet no puede dejar de reflejar estos problemas teóricos generales y aquellos autores que niegan la responsabilidad penal de las personas jurídicas lo fundamentan particularmente en el mundo virtual, en tanto pueda llegar a convertirse en un discutible expediente de política criminal para la transformación de los proveedores de acceso o de servicios de red en responsables criminales en sustitución de los autores materiales, a la vista de los obstáculos para la punición de las comunicaciones ilícitas vía Internet. Aconsejan, por tanto, como necesario un análisis de los principios del derecho penal moderno y su proyección en el ámbito de la criminalidad informática.[6]

3.1. Casos en los que la responsabilidad penal de los ISP procede

3.1.1. Por pérdida o manipulación incorrecta de información

Proyectando precisamente los fundamentos político-criminales de la RPPJ al ámbito de la criminalidad informática; y vistas las distintas modalidades y servicios de comunicación prestados, entendemos que la

(5) Ley 26.388, modificación al CP, sancionada: 04/06/2008, promulgada de hecho: 24/06/2008.

(6) Ver [en línea] http://www.emagister.com/responsabilidad-penal-personas-juridicas-ambito-criminalidad-informatica-portugal-cursos-1110780.htm

pérdida de información o la difusión de información confidencial —tanto dolosa como por **culpa o negligencia del proveedor de acceso o almacenamiento— determinará su responsabilidad civil y también la penal en la medida en que la misma sea generada por una deficiencia organizacional o por falta de implementación de los controles debidos, de acuerdo a la actividad y/o complejidad de la misma.**(7)

En tal sentido, la empresa deberá responder no solo ante el cliente, sino también ante terceros por los daños y perjuicios que se deriven de la manipulación incorrecta o no autorizada que puedan provocar averías o deterioros en el servicio o pérdida, modificación o destrucción de la información por deficiencia organizacional y/o falta de controles.

En los países cuyo sistema constitucional sea compatible con la responsabilidad penal de personas jurídicas, las mismas podrán ser responsabilizadas penalmente por la pérdida o alteración de la información por un actuar falto de diligencia o doloso (en tanto proveedoras de alojamiento), y en el caso de los llamados "buscadores", que brindan un sistema de acceso y de indexación de contenidos, también cabría su penalización en la medida en que una programación defectuosa permita indexar contenidos ilícitos y vincularlos a personas o imágenes a través de su software de búsqueda, si cuentan con las herramientas tecnológicas para evitarlo.

Esta posibilidad de imputar a la empresa deriva de la que se conoce en la doctrina europea como responsabilidad de la empresa por defecto de organización.(8)

3.1.2. Por falta de protección de la información de parte de los proveedores

Es común la expresión "la información cuesta", lo que refleja el atractivo económico que en la actualidad representa el manejar datos claves o tener acceso a bases de datos privadas o públicas en la medida en que la información es considerada como elemento de conocimiento, poder y riqueza en la llamada Sociedad de la Información.

Cuando la información se convierte en objeto de apropiación, manipulación y, en definitiva, en blanco lucrativo del delincuente, se ven afectados

(7) Freeman, Edward H., "*Third-Party Liability: Who Pays for Computer Damages?*", en *Legally speaking*, marzo/abril, EBSCO Publishing, 2002; *"ISP Liability for Third-Party Defamation"*, *Legally speaking*, noviembre/diciembre, 2002.

(8) Silva Sánchez, Jesús María, *La expansión del derecho penal*, BdeF, p. 13 y concordantes, con cita de la noción de sociedad de riesgo de Ulrich Beck.

valiosos bienes jurídicos, desde la intimidad, el orden socioeconómico y la fe pública hasta la seguridad del Estado, entre muchos otros.

La doctrina española ha definido al computador como un factor criminógeno de primera magnitud que aporta a la conducta criminal, algunas veces, un nuevo objeto (la información misma, potenciada y revaluada por los nuevos sistemas de procesamiento de datos y los programas) y otras, un nuevo instrumento: ofreciendo un inmenso abanico de técnicas y estrategias que pueden ponerse al servicio del delito, enriqueciendo el repertorio criminal, a lo que podría agregarse que requiere de la organización criminal para multiplicar sus efectos.(9)

Esta acertada distinción permite precisar cuándo la tecnología es medio y cuándo objeto del delito, de acuerdo a las diferentes definiciones brindadas en relación al delito informático.

El tema de la informatización y de la garantía de privacidad en la red es uno de los que debe enfrentar el derecho y, dentro de este, por supuesto, el derecho penal. El principal aspecto que se discute es el del acceso y utilización de la información privada de las personas. La reglamentación sobre estos aspectos se basa fundamentalmente en acuerdos internacionales sobre telecomunicaciones, comunicaciones vía satélite, protección de software, construcción de equipos, dispositivos y otras.(10)

3.2. Alcance del deber de protección de la información

Internet, para la legislación argentina, es un servicio de telecomunicaciones ofrecido por un prestador licenciado que brinda el soporte físico y el lógico para la colocación de los contenidos de los usuarios.(11)

En tal sentido, existen distintos tipos de prestadores o proveedores de servicios: de acceso, de alojamiento, buscadores de contenidos, proveedores de aplicaciones o software, etc.

Partiré de la premisa más general: aquel que maneja riesgos sociales derivados de su actividad debe responder por la lesión o puesta en peligro

(9) Jaen Vallejos, Manuel, *Cuestiones Actuales del Derecho Penal Económico,* Capítulo II, Bs. As., Ad Hoc, 2004, p. 76.

(10) Ver al respecto Directiva 2002/21/CE del Parlamento Europeo y del Consejo, 07/03/2002, relativa a un marco regulador común de las redes y los servicios de comunicaciones electrónicas (Directiva marco).

(11) Ley Nacional de Telecomunicaciones 19.798, 22/08/1972, BO 23/08/1972, reformada por la ley 22.285.

de los bienes jurídicos producidos en ocasión de la prestación de dicha actividad o servicio, en tanto tenga —como es el caso de los ISP—capacidad tecnológica y capacidad de organizar la información y de relacionar los contenidos que circulan por la red de modo no delictivo.

Tomo también como punto de partida el hecho de que quien posee el gobierno de la información y la capacidad técnica de acceder, analizar y seleccionar contenidos debe asumir el costo de los riesgos que se producen por defectuoso control organizacional de los servicios brindados.

Asumiendo que los servicios de Internet deben ser programados éticamente por hombres, no es menos cierto que las empresas proveedoras manejan herramientas técnicas y humanas para prevenir, detectar y controlar los abusos de las TIC (Tecnologías de la Información) y que una correcta organización debe (por tener las herramientas) poder controlar los desvíos que se producen en la prestación del servicio en perjuicio de los usuarios o de terceros.

También debe asumirse que la empresa (la persona jurídica corporativa) tiene gran capacidad ofensiva respecto de los bienes jurídicos protegidos mediatamente por las normas cuyas prohibiciones y mandatos infringe, todo lo que viene siendo objeto de debate jurídico desde el siglo pasado y en los últimos años, tanto a través del desarrollo del derecho ambiental y económico como también —y más recientemente— debido al desarrollo del medio digital y su regulación.

3.2.1. Particularidades de la responsabilidad según el tipo de proveedor de servicio

Últimamente —a nivel mundial y, puntualmente, en nuestro país— se ha puesto en debate el tema de la responsabilidad civil de los buscadores de Internet,[12] la que representa solo una parte de un ámbito de discusión más amplio: la responsabilidad administrativa y eventualmente penal de los prestadores de servicios de telecomunicaciones y de Internet en general, en función de su capacidad infractora tanto para la puesta en peligro como para la lesión de bienes jurídicos

(12) Ver JNAc. Civ. N° 95, "Rodríguez, María Belén c/ Google Inc. s/ Daños y Perjuicios", 24/03/2010, Expte. N° 99.613, Sentencia no firme. Es interesante el informe pericial obrante a fs. 631 en cuanto señala refiriéndose a la responsabilidad del buscador: "Quien gobierna la información es el buscador, de cualquier otra manera sería imposible administrar las relaciones de búsqueda…". Concluye que es técnicamente posible, en virtud de la capacidad de los filtros que posee el buscador, acceder y seleccionar los contenidos de las páginas web.

En el caso citado la jurisprudencia local ha sentado posición respecto de la responsabilidad civil de los llamados "motores de búsqueda" o "buscadores" que son aquellos que tienen a su cargo el acceso, búsqueda e indexación de contenidos dispersos por la red, responsabilidad que se genera en la medida de su conocimiento.

Por otro lado, existen otras categorías de empresas proveedoras de servicios de red a quienes compete, en principio, resguardar la privacidad de los datos que alojan en sus servidores (la integralidad y confidencialidad de toda la información) y en caso de violaciones a la privacidad derivadas de la defectuosa preservación podrían también ser responsabilizadas tanto civil como penalmente en forma directa, sin perjuicio de la responsabilidad que recaiga conjuntamente sobre las personas físicas, cuya responsabilidad penal pueda determinarse en la investigación. La mayor capacidad tecnológica de estos entes colectivos las dota de mayor capacidad ofensiva, como así también de poder para auxiliar y cooperar con las investigaciones dentro y fuera de los ámbitos nacionales, dada la desterritorialización que caracteriza al servicio de Internet y como consecuencia de ello, al ciberdelito.[13]

Lo que parece más claro en torno a la obligación de preservar la integralidad, confidencialidad y privacidad de los datos alojados en los servidores de Internet resulta más vidrioso respecto de la responsabilidad penal de los motores de búsqueda, entendiendo que se trata de proveedores de servicios que brindan acceso a los diversos contenidos dispersos por la web o que vinculan o facilitan el acceso a los mismos, surgiendo el problema de la responsabilidad por dichas violaciones tanto en su aspecto civil como penal cuando se afecta el derecho a la privacidad de las personas o se afecta la intimidad o el honor de las mismas cuando se vinculan o indexan contenidos lícitos o autorizados, subidos incluso por la víctima, a otros de contenido ilícito o injuriante dispersos por la red.

Los buscadores que actúan como intermediarios y facilitadores necesarios de datos y que buscan eventualmente multiplicar sus ganancias a merced de los vastos datos que colectan, brindan y enlazan y que están diseminados

(13) Denominación que le da al ilícito informático la Convención sobre Cibercrimen del Consejo de Europa, celebrada en Budapest el 23/11/2001, suscripta en el marco del Consejo de Europa junto a Estados Unidos, Canadá, Japón, Costa Rica, México y Sudáfrica. Nuestro país adhirió a ella en marzo de 2010, por tratarse de una convención europea de adhesión mundial.

por la red, pueden también menoscabar el honor de las personas mediante la indexación de imágenes o contenidos lícitos a otros ilícitos.

El factor de atribución de responsabilidad a estos proveedores resulta, en general, del hecho de ser facilitadores de acceso a contenidos, contando con gran capacidad ofensiva, puesto que vinculan a cientos de miles de usuarios de la red y con su accionar deficiente pueden exponer a los usuarios de estas tecnologías a nuevos riesgos e incluso a la efectiva producción de daños morales, físicos y económicos, los que, siendo ocasionados en el curso de la prestación del servicio, deben ser asumidos por quien lo brinda, en tanto que el sujeto prestador obtiene ingentes ganancias debido, justamente, a la potencialidad de las tecnologías que manejan y de su capacidad de acceder, analizar, seleccionar y hacer disponibles diversos contenidos a millones de usuarios, siempre que dicho menoscabo a los bienes sea directamente el producto de un déficit de programación o por el deficiente control del servicio que ofrecen o por no brindar las herramientas tecnológicas necesarias para la seguridad de los datos de los usuarios, estando en capacidad de hacerlo.

Postularé —entonces— un factor de atribución de responsabilidad penal fundado en que, como prestadores de Internet, reúnen los factores humanos y tecnológicos que les permite brindar un servicio fundamental en la producción, circulación, indexación y filtrado de contenidos, alojamiento y distribución de datos (lo que les confiere capacidad tecnológica de acción) a través de una organización que debe ser ética y no delictiva en el manejo de la actividad empresarial.

Tomo por base doctrina, jurisprudencia y lineamientos de las directivas para los Estados miembro de la Unión Europea —tanto en materia civil como penal— que permite formular la premisa de que quien gobierna la información debe asumir los costos de la eventual dañosidad social que la prestación de tal servicio genere a los usuarios, como así también el deber de colaborar en el esclarecimiento de los ilícitos de contenido o de tráfico cometidos por la red, precisamente por estar en las mejores condiciones para ello.

Como conclusión, entendemos que por el rol de las empresas proveedoras de servicios de red (proveedoras de acceso, alojamiento y de herramientas de búsqueda) poseen responsabilidad civil por daños ocasionados en la medida de su capacidad dañosa objetiva y poseen capacidad de

cometer ilícitos y de ser punibles en la medida en que no utilicen todos los factores organizacionales de que disponen (conjunto de herramientas técnicas y humanas) para prevenir, brindar seguridad, y utilizar activamente su posibilidad de detectar y controlar los abusos de las tecnologías informáticas y de las comunicaciones a través de la programación ética de los servicios que brindan y de los resguardos y controles que implementan en función de la complejidad y magnitud de dicho servicio.

4. Criterios de colaboración empresaria conforme a lineamientos internacionales

A fin de brindar un marco ético normativo al presente análisis, corresponde señalar que en la Comunidad Europea se han elaborado distintos lineamientos para la Cooperación entre los ISP y las autoridades de control a fin de tornar más seguro el uso de la red global y para evitar que la inmensa autopista de información[14] que constituye Internet sea utilizada para la comisión de delitos.[15]

Del mismo modo diferentes convenciones y sus protocolos facultativos,[16] como así también declaraciones de diversos foros internacionales como la de Río de Janeiro al Tercer Congreso Mundial contra la Explotación Mundial de Niños y Adolescentes del año 2008, han señalado la necesidad de exhortar a los Estados a:

> "tomar las medidas legislativas necesarias para requerir que los **proveedores del servicio de Internet, las empresas de telefonía móvil, los motores de búsqueda**[17] y otros actores pertinentes denuncien y retiren los sitios web de pornografía infantil y las

(14) Ver exposición de motivos, ley 26.032 (BO 17/06/2005) y decreto 1279/1997 (BO 01/12/1997). En este último, declárase comprendido en la garantía constitucional que ampara la libertad de expresión al servicio de Internet.

(15) *"Guidelines for the cooperation between law enforcement and internet service providers against cybercrime. Adopted by the global conference Cooperation against Cybercrime"*, Council of Europe, Strasbourg, 1 y 2 de abril, Octopus Conference 2008. En la citada conferencia la ponente participo como representante del Ministerio de Justicia y DDHH de la Nación. Ver www.coe.int/cybercrime

(16) Convención sobre los Derechos del Niño de 1989 y Protocolo Facultativo 129, aprobado por ley 25.763, relativo a la venta de niños, prostitución infantil y la utilización de niños en la pornografía por Internet.

(17) El resaltado me pertenece y el texto corresponde a un fragmento de la Declaración de Río de Janeiro y Llamado a la Acción para prevenir y Detener la Explotación Sexual de Niños, Niñas y Adolescentes, [en línea] http://resources.ecpat.net/EI/Updates/SPWCIIIOutcome.pdf

> imágenes de abuso sexual infantil, además de desarrollar indicadores para monitorear los resultados y mejorar los esfuerzos (...) y para que, asimismo, se urja a **los proveedores de Internet, las empresas de telefonía móvil, los cibercafés y otros actores pertinentes** 'a que desarrollen e implementen códigos de conducta voluntarios y otros mecanismos de responsabilidad social corporativa junto con el desarrollo de herramientas legales para permitir la adopción de medidas de protección de los niños en sus empresas'".

A idénticas conclusiones han arribado diferentes fallos domésticos[18] que han justificado la responsabilidad civil de los buscadores "por haber facilitado el acceso a sitios de contenido sexual, erótico y pornográfico en los cuales aparece el nombre, la imagen y fotografías de una modelo profesional, por la afectación de su derecho constitucional a la imagen..." y ello en función de que si bien "la dimensión de los buscadores de Internet como herramienta amerita su aliento para que puedan sostener un adecuado desarrollo de las comunicaciones, ello no implica que deba apoyarse tal crecimiento a expensas de los derechos individuales o con afectación de los mismos".[19]

Es claro el encuadre del art. 42 CN en cuanto a la responsabilidad civil de los buscadores, debido a que el usuario es consumidor de "servicios de red" y tiene el derecho —de rango constitucional—, desde el año 1994, a que se lo proteja de los daños y perjuicios ocasionados por las empresas propietarias de motores de búsqueda de Internet que dan acceso a determinados contenidos de sitios de terceros indexados en sus búsquedas que utilizan la imagen y/o vinculan los nombres de las personas con sitios vinculados a actividades ilegales o inmorales, tales como la pornografía, por citar el ejemplo de los fallos traídos a consideración.[20] Similar encuadre ofreció la jurisprudencia reciente al tratamiento de una medida cautelar aplicable en sede civil contra las llamadas "redes sociales" por

(18) Además del fallo citado —"Rodríguez, María Belén c/ Google Inc. s/ Daños y Perjuicios"—, ver JNAC. CIV. N° 75, "Da Cunha, Virginia c/ Yahoo de Argentina SRL y Otro", 29/07/2009, cita: MJ-JU-M-45549-AR|MJJ45549, Sentencia no firme.

(19) Ver JNAC. CIV. N° 75, "Da Cunha, Virginia c/ Yahoo de Argentina SRL y Otro", fallo cit., Consid. 9°.

(20) Ver JNAC. CIV. N° 95, "Rodríguez, María Belén c/ Google Inc. s/ Daños y Perjuicios", fallo cit.

el alojamiento de contenidos considerados dañosos[21] al analizar su procedencia para que se disponga el cese inmediato de un determinado grupo de menores, por promover objetivos que la actora consideraba disvaliosos para el interés superior de los niños, conforme lo dispuesto por la ley 26.061.[22] La jurisprudencia civil agrega la necesidad de que las empresas hayan tomado un **conocimiento efectivo** de que su sistema indexaba ese tipo de contenidos ilegales, pero afirma también lo contrario cuando sostiene que estas uentan con la tecnología para prevenirlo, el buscador:

> "proveía en la lista de resultados hipervínculos a sitios de terceros que infringían los derechos a la intimidad y al respeto de los datos personales de la reclamante, **y por la tecnología con que cuentan** se encontraban en condiciones técnicas de efectuar el control y selección de los contenidos para evitar, de este modo, que los resultados engañosos e injuriantes continúen apareciendo en sus listas, y al no hacerlo, incurrieron en una negligencia culpable que les genera la obligación de responder por las consecuencias dañosas, en tanto medie **adecuado nexo de causalidad entre esta y los daños probados**".[23]

5. Parámetros para imputar penalmente a la organización

Además de la responsabilidad civil, la doctrina deberá ampliar su análisis a fin de responsabilizar también penalmente a los proveedores de servicios de Internet, en la medida en que se den los parámetros que las legislaciones internacionales señalan para imputar a una organización:

a. que nos encontremos ante una actividad delictiva que se desarrolla en el ámbito de la empresa (el caso de los ISP son organizaciones cuyo objeto es prestar servicios en el entorno digital).

b. que por el producto de la actividad delictiva se produzcan beneficios que redunden o puedan redundar en un incremento del patrimonio de la empresa, es decir, la posibilidad del beneficio sobre el sujeto colectivo.

---

(21) Ver 2do JCiv., Com. y Minas Mendoza, "Protectora Asociación Civil de Defensa del Consumidor c/ Facebook Inc. p/ Sumario", 11/05/2010, autos N° 152.628.

(22) Ley 26.061 de Protección Integral de Derechos de las Niñas, Niños y Adolescentes, BO 26/10/2005.

(23) Ver JNac. Civ. N° 95, "Rodríguez, María Belén c/ Google Inc. s/ Daños y Perjuicios", fallo cit., Consid. 1°.

c. que el ilícito puede ocasionarse a través de la conducta activa de los representantes o supervisores de la actividad o por omisión de control de directivos o supervisores, de modo que puedan imputarse al ente colectivo.

En el caso de la teoría del órgano, la conducta de los representantes comprometería la de la empresa y, según la del defecto organizacional, dicho déficit podría ser imputado a la empresa cuando a consecuencia de ello se produzca la actividad delictiva de sus miembros en el seno de la misma.

La responsabilidad penal de los ISP, junto a la administrativa y civil, es una más de las consecuencias que se recomienda adoptar a los Estados firmantes de la Convención de Ciberdelito. Nótese que, en general, se recomienda la imputación a la empresa en convenciones internacionales en materia ambiental, crimen organizado, cohecho y lavado de dinero.

En un principio se observaba una reacción a nivel privado frente a las primeras manifestaciones del intrusismo informático o de acceso no autorizado,[24] pero simultáneamente se producía de parte de los transgresores un perfeccionamiento en sus técnicas de intrusión. Ante esta realidad se consideró muy necesaria la participación del Estado y sus organismos, para consolidar la adecuada complementación de los mecanismos de seguridad privados con normativas que establecieran una clara regulación y sanción de estas conductas, tipificándolas en los diversos códigos penales como delitos.

De este modo, en nuestro país se consagra la figura de los delitos informáticos a través de la ley 26.388, sancionada en junio de 2008,[25] la que si bien ha previsto nuevas incriminaciones para delitos cometidos en el entorno digital que afectan a diferentes bienes jurídicos, no **ha contemplado la sanción penal de los ISP,** ni siquiera de aquellos que alojan contenidos ilícitos (en la medida de su conocimiento) o que generan contenidos nocivos o que realizan intrusismo informático (espionaje), accediendo a sistemas o datos, violando normativas de privacidad.

La responsabilidad penal de la conducta del ISP podrá ser evaluada cuando el sitio haya conocido acerca de los contenidos ilícitos alojados

(24) Tal el caso de Sieber Ulrich, investigador sobre ciberdelito del Instituto Max Planck, uno de los que definió más tempranamente los ataques por Internet a partir de los años 70.

(25) Ley 26.388, BO 25/06/2008.

y eventualmente pudiera removerlos.[26] Así, en la confirmación de un procesamiento, la Sala VI considera que existen elementos suficientes para considerar que las infracciones que se producen en las causas que le son llevadas a juicio no se producirían en la magnitud y facilidad en que se producen si no se utilizare la plataforma tecnológica de Taringa!, que permite:

4. intercambio de oferta y demanda de contenidos violatorios de propiedad intelectual de terceros;
5. facilitación del carácter de anónimo de los usuarios que suben los contenidos;
6. el beneficio económico percibido por los titulares y/o administradores del sitio en virtud de las visitas que recibe el sitio y que precisamente son en su mayoría las relacionadas con el consumo de obras de propiedad intelectual, careciendo de licencias o derecho de uso de las mismas.

Como vemos, no se los imputa a la empresa Taringa! como autora de las infracciones, sino como "facilitadora" o partícipe necesaria.[27]

Más claramente, podrá advertirse la responsabilidad penal de aquellas empresas que propiamente **generen** los contenidos nocivos.

También generará responsabilidad penal la pérdida o daño de la información almacenada en los servidores, puesto que la misma debe ser fidedigna y completa; nadie que no sea el usuario tiene derecho a cambiarla. En cuanto a su disponibilidad, el usuario debe tener la información en el momento en que la necesite, y confidencialidad porque sin consentimiento del usuario nadie debe tener acceso ni divulgar su información.[28]

Es muy interesante la Directiva europea que sirve de marco a la regulación de las comunicaciones en cuanto plantea la tutela de la privacidad:

---

(26) A raíz de los fallos dictados por la Sala VI de la Cámara de Nacional de Apelaciones en lo Criminal y Correccional, en virtud de lo cual confirma en tres casos el procesamiento a los titulares de un portal de Internet y administradores del sitio por actividad "presuntamente" realizada por terceros, se analiza por primera vez en la República Argentina la responsabilidad penal de los titulares de una persona jurídica por actividad desplegada por terceros (*v. gr.* JNAC. CRIM. DE INSTRUCC. N° 44, Sala VI, "www…….net y otros s/ procesamiento", sentencia interlocutoria, causa N° 41.181.

(27) LÓPEZ ROMERO, TATIANA, "*Internet Service Providers' Liability. For Online Copyright Infringement: The Us Approach*", en *Vniversitas*, Pontificia Universidad Javeriana, Colombia, n° 112, julio-diciembre, 2006, pp. 193/214, en el mismo sentido que el fallo local citado.

(28) En nuestro país funciona el ARCErt, dependiente de la Oficina Nacional de Tecnologías de la Información (ONTI). Debe tenerse en cuenta que estos principios son los que surgen de los Considerandos de la ya mencionada Convención de Budapest de 2001.

> "5. **Protección al usuario sobre violación de datos personales y spam**. Una de las prioridades del nuevo marco es la protección de los datos personales. Hay que mantener absolutamente seguros los nombres, direcciones de email e información bancaria de los usuarios y, sobre todo, se ha de evitar que, accidental o deliberadamente, caigan en manos incorrectas la información de cada llamada telefónica y sesión de Internet (IP/09/571). **Los operadores serán responsables del proceso y almacenamiento de ese tipo de información**. Por tanto, el nuevo marco incluye mandatos obligatorios para cuando se violen los datos personales. Quiere esto decir **que los operadores de comunicaciones estarán obligados a informar a las autoridades y a sus clientes de las violaciones de seguridad que afecten a los datos personales. Lo cual aumentará los incentivos a que los operadores protejan mejor los datos**".(29)

6. Regulación o autorregulación

Siendo tan grande el número de conductas delictivas y de contenidos ilícitos transmitidos a los usuarios a través de la red, los partidarios de la regulación de este entorno sostienen que este canal de comunicación mundial y red social que es Internet **debe ser regulada** y se debe impedir en ella la transmisión de contenidos nocivos o ilícitos. La otra teoría es la de **la autorregulación**, la cual exime de toda culpa a los proveedores de servicios en cuyas redes o servidores fluya dicho tipo de contenidos, siempre y cuando el proveedor haya advertido a su usuario del carácter ilícito de dichos mensajes o publicaciones, siendo cuando esté tecnológicamente a su alcance obligatorio el ofrecimiento de filtros para evitar el perjuicio a terceros por la circulación libre de tales contenidos ofensivos, o no apto para menores o que impliquen discriminación, odio racial o atenten contra la seguridad de los Estados.

Se sostiene que Internet es un medio de comunicación social, donde se establece una comparación entre los proveedores de acceso a Internet y los de hospedaje de páginas web con los **editores** en el sentido de que ambos proporcionan el soporte material que permite a los autores la divulgación de los contenidos generados. Entonces, las características que

(29) Directiva 2002/21/CE del Parlamento Europeo, cit.

definen a **un medio de comunicación social** son: a) prestar servicios de carácter audible, audiovisuales y/o impresos; y b) operar en el país.

No obstante la presencia de este ámbito regulatorio, rige en general la autorregulación y el anonimato como así también destaca la ausencia de controles por parte de los Estados.

De todas maneras tiene aceptación el principio de que el anonimato debe ceder frente a las investigaciones judiciales.

Como reflejo de esta autoregulación y anonimato se acepta, en general, el principio de limitación de responsabilidad de los proveedores, y se acepta que las medidas de los proveedores de servicio en defensa de los usuarios dependan de la denuncia que los mismos formulen, de modo tal que la obligación de control de contenidos se pone en cabeza del propio afectado.

7. A modo de conclusión

Los proveedores de servicios de Internet serán responsables por la integridad y la privacidad de las comunicaciones o contenidos que circulan por sus redes en tanto brinden acceso o alojamiento en sus servidores, y serán responsables por conductas o contenidos delictivos subidos por terceros en la medida que lo conozcan y lo faciliten a través de su plataforma tecnológica y además lucren con ello.

En cuanto a la publicación y divulgación en un sitio web de un aviso o mensaje con un contenido ilícito o nocivo también le cabe responsabilidad al proveedor de alojamiento de la página web respectiva cuando a sabiendas de la actividad ilícita que realizan los abonados a su servicio, no retire los datos o no imposibilite el acceso o lo filtre, dada la capacidad tecnológica con la que cuentan para programar tales restricciones.

Si bien la Convención de Budapest brinda en su art. 12 los lineamientos que permiten responsabilizar penalmente a las personas jurídicas con sanciones efectivas, proporcionadas y disuasorias, y que dicha responsabilidad incluye las conductas activas de quienes ostentan poderes de representación de la empresa como así también la responsabilidad por conductas omisivas o generadas por falta de controles o ausencia de medidas de vigilancia por parte de cualquier persona física que ostente un poder de dirección en su seno, la responsabilidad penal de las empresas prestadoras de servicios de red no ha sido claramente establecida en la legislación ni en la jurisprudencia, ya que la responsabilidad de un usuario

que carga material ilícito en la red y la exención de responsabilidad de los operadores que simplemente lo transmiten parece generalmente aceptada. Pero la cuestión de la responsabilidad de los estadios intermedios (especialmente donde se almacena el material, incluso temporalmente, en formato legible) está lejos de haber quedado establecida.

Tampoco ha quedado establecida la responsabilidad penal de los buscadores aun cuando ilegítimamente vinculen un sitio lícito a contenidos ilícitos, teniendo la posibilidad tecnológica de evitarlo. La cuestión consiste en averiguar qué es técnicamente factible y económicamente viable, y conseguir un equilibrio entre la protección de la libertad de expresión y la privacidad, por un lado, y la seguridad, protección de los menores y la dignidad de la persona humana, por otro.

En esta distribución de riesgos y responsabilidades debe cargar con la responsabilidad penal aquel que gobierna el uso de la información y tiene los mejores recursos humanos y tecnológicos para programar la actividad corporativa en forma no delictiva y ética.

Por último, entre el sistema de autorregulación de contenidos (equivalente a dejar la resolución de los problemas en manos del mercado)[30] y el regulatorio nos inclinamos en favor del segundo por cuanto, fijando los deberes de las ISP vinculadas a los diferentes servicios de los que son prestadores, se evita que sea la propia empresa la que evalúe según sus propios cálculos e intereses cuál es la mejor decisión frente a su conducta infractora. Fijando legalmente sus deberes se evita que la eficacia preventiva de las medidas administrativas o penales queden reducidas solo al momento en que los afectados tomen conocimiento y presenten sus reclamos, obligándolos, de ese modo, a constituirse en "policías" de sus derechos cuando en la actualidad es imposible individualmente controlar todo aquello que circule por la red, afectando derechos individuales o colectivos.

Podemos señalar como un avance del criterio propiciado en este trabajo la propuesta que trae el Anteproyecto elaborado por la Comisión para la Elaboración del Proyecto de Ley de Reforma, Actualización e Integración del Código Penal de la Nación (decreto 687/2012) respecto de los criterios de imputación de RPPJ, los que resultarían aplicables a los servidores de

(30) A igual conclusión o en relación a la regulación a la acción de retirada de los productos defectuosos del mercado arriba Sarrabayrouse, Eugenio en *Responsabilidad Penal por el Producto*, Bs. As., Ad-Hoc, 2007, p. 746.

Internet en la medida en que dicha propuesta sea especialmente consagrada por la ley.

Las sanciones a la persona jurídica son aplicadas en forma alternativa o conjunta con la de las personas físicas. No solamente consagra una responsabilidad penal "transferida" del representante o del interviniente en el hecho ilícito (el que debe ser debidamente comprobado y generar beneficio a la persona jurídica como punto de conexión entre el hecho de la persona física y la empresa), sino que también recepta la "culpabilidad de organización", aun cuando el hecho no implicara beneficios a la persona jurídica, cuando la comisión del delito hubiera sido posibilitada por el incumplimiento de los deberes de dirección y supervisión.

Por lo tanto, en la medida en que los deberes de los integrantes de las empresas estén establecidos y asignados y en el caso de tratarse de proveedores de servicios de red con estructuras y actividad compleja, podrán imputarse por defecto organizacional cuando no pueda individualizarse a la persona física responsable, aun cuando no se produzca el beneficio económico esperado en la empresa.

Por lo tanto, la recepción en nuestro ordenamiento interno de la responsabilidad penal de las ISP puede considerarse no solo por haber sido ya introducida en leyes especiales y en razón de la decisión político criminal del legislador (en la medida en que este Anteproyecto sea elevado y aprobado en el seno del Congreso de la Nación), sino también porque la RPPJ se justifica desde el punto de vista de las consecuencias de la regulación (la pena) como así también desde el punto vista del objeto de regulación del derecho penal (el ilícito) que puede cometerse por estos entes no solamente en la medida en que se pueda identificar a quien es responsable del hecho y de la obtención de los beneficios ilícitos para la empresa, sino también por el defecto organizacional (hecho propio de la empresa) fundado en la falta de cumplimiento de deberes y controles de los responsables que aumentan el factor criminógeno dentro de la misma mediante lo que los autores han dado en llamar "irresponsabilidad organizada".

Desde los fines de la pena, el castigo también se justifica tanto con medidas preventivas como con verdaderas penas pecuniarias por cuanto desde una teoría funcional de la pena, el prestador de servicios brinda un "modelo orientador" de conducta —que puede ser ética o delictiva— a todos los usuarios de la red y lucra con los servicios prestados mediante la organización y el manejo de la información, poseyendo los medios técnicos

para prevenir y controlar el delito tanto filtrando y/o procediendo a la baja de contenidos delictivos.

El beneficio de los proveedores de servicios de Internet es indudable en la medida que hoy todas las actividades productivas, educativas y otras básicas como la salud se encuentran informatizadas. Al manejar el uso de las tecnologías manejan ingentes sumas de dinero y por lo tanto es obligación de las corporaciones planificar su actividad en forma ética y no delictiva.

Resulta común la expresión "la información cuesta", lo que refleja el atractivo económico que en la actualidad significa manejar datos claves o tener acceso a bases de datos privadas o públicas en la medida en que la información es considerada como elemento de conocimiento, poder y riqueza en la sociedad de la información.

Podemos afirmar con autores como Lampe[31] que no solo es relevante el injusto como hecho individual en el que interviene un autor o un cómplice o incluso una asociación de personas físicas para delinquir, sino que también cobra relevancia todo proceso social u organizacional que ponga en riesgo la vida en común —sea en el territorio o en el mundo virtual— y que pueda ser valorado por el legislador **como injusto punible.**

Postulamos, entonces, que Internet, como expresión última de desarrollo social, es un sistema complejo, donde junto a la culpabilidad individual por el injusto se impone también la decisión del legislador de consagrar junto a la responsabilidad administrativa o contravencional la responsabilidad penal por defecto organizacional de las empresas prestadoras de servicios de red y de comunicación.

(31) Lampe, Ernst Joachim, "Sobre la estructura ontológica del injusto punible", en *Revista de Estudios Criminais*, n° 16, año IV, 2004.

¿Existe un bien jurídico para los delitos informáticos?

HERNÁN KLEIMAN[1] y PABLO L. TELLO[2]

1. Introducción

El tema de la presente exposición ya ha sido debatido en diversas oportunidades y está en boga en distintos ámbitos académicos y profesionales debido al enorme espacio que actualmente ocupa la informática en nuestras vidas. Al respecto, sabido es que la incalculable cantidad de información que circula en la red global, sumada a la inmensa cantidad de personas que utiliza dichas conexiones para comunicarse, genera un nuevo esquema de relaciones humanas que, lógicamente, obliga a las ciencias jurídicas a no permanecer expectantes y en la retaguardia de los cambios.

En efecto, 68 de cada 100 personas en Argentina son usuarias de internet.[3] A nivel mundial, en 2012 más de un tercio de la población mundial utilizaba dicha red, a lo que cabe agregar que en marzo de 2013, el número de usuarios de la red social Facebook trepaba a 1110 millones de personas en el

(1) Abogado (UBA). Ayudante en la materia "Elementos de Derecho Penal y Procesal Penal" en la Cátedra del Dr. Javier De Luca, comisión a cargo del Dr. Mauro Divito. Se desempeñó en diferentes cargos tanto en el Poder Judicial como en el Ministerio Público de la Nación.

(2) Abogado (UBA). Ayudante en la materia "Elementos de Derecho Penal y Procesal Penal" en la Cátedra del Dr. Javier De Luca, comisión a cargo del Dr. Mauro Divito. Cursa la carrera de especialización en Derecho Penal (UBA) y se desempeña en la Defensoría Oficial ante la Cámara Federal de Casación Penal N° 4.

(3) Fuente: [en línea] http://es.wikipedia.org/wiki/Anexo:Pa%C3%ADses_por_n%C3%BAmero_de_usuarios_de_Internet.

mundo. Por consiguiente, la interacción social en la actualidad no se limita a las relaciones "reales", sino que también debe abarcar aquellas que se desarrollan a través de las plataformas informáticas globales.

Por consiguiente, las reglas jurídicas no deben —ni pueden— desconocer estos cambios en la realidad, y tienen que adecuarse a ellos. De hecho, esta materia ha sido el espíritu de la Convención de Cibercrimen (Budapest, 2001), cuyo Preámbulo explica los motivos por los cuales se deben tipificar las conductas bajo análisis, indicando entre otras cuestiones:

> "... Convencidos de la necesidad de llevar a cabo, con prioridad, una política penal común destinada a prevenir la criminalidad en el ciberespacio y, en particular, de hacerlo mediante la adopción de una legislación apropiada y la mejora de la cooperación internacional;
>
> Conscientes de los profundos cambios suscitados por el incremento, la convergencia y la mundialización permanente de las redes informáticas;
>
> Preocupados por el riesgo de que las redes informáticas y la información electrónica sean utilizadas igualmente para cometer infracciones penales y que las pruebas de dichas infracciones sean almacenadas y transmitidas por medio de esas redes".

La misma Convención, en el Título I, consigna las "Infracciones contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos" y exhorta a las partes del tratado a adoptar las medidas que estimen necesarias para prever como infracción penal "el acceso doloso y sin autorización a todo o parte de un sistema informático", entre otras conductas.

Sin embargo, más allá del carácter positivo de la modernización del derecho penal —y también del procesal penal—, y de la admisible preocupación en que tanto los sistemas jurídicos como las agencias penales no queden obsoletas frente al avance científico y a las nuevas tendencias sociales, no debe dejar de advertirse que, paralelamente, esto generó un proceso de expansión del derecho penal. En este sentido, y frente a la innumerable cantidad de infracciones penales —fenómeno señalado como "administrativización de la ley penal"—,[4] deviene trascendental, en pos

(4) Zaffaroni, E. Raúl; Alagia, Alejandro y Slokar, Alejandro, *Derecho Penal. Parte General*, Bs. As., Ediar, 2008, p. 725.

de un mayor respeto de los principios del derecho penal liberal —cuyas ideas fueron receptadas en nuestra Constitución Nacional— someter a un análisis más profundo las nuevas formas delictivas.

Ya hace mucho tiempo —25 años precisamente— Ferrajoli nos alertaba de esta situación, al explicar que

> "Encontramos, ante todo, una proliferación cuantitativa de los intereses tutelados, ya que, por una parte, se asumen funciones autoritarias mediante el incremento de los delitos sin daño —es el caso de ofensas a entidades abstractas como la personalidad del Estado o la moralidad pública— y, por otra, se aumentan incontroladamente los delitos contravencionales e incluso de bagatela a menudo consistentes en meras desobediencias. En segundo lugar, se ha producido una ampliación indeterminista del campo de lo designable como bienes tutelados, a través de la utilización de términos vagos, imprecisos o, lo que es peor, valorativos, que derogan la estricta legalidad de los tipos penales y brindan un amplio espacio a la discrecionalidad y a la inventiva 'judicial'".

La cita continúa y el autor señala

> "En tercer lugar, hemos asistido a una creciente anticipación de la tutela, mediante la configuración de delitos de peligro abstracto o presunto, definidos por el carácter altamente hipotético y hasta improbable del resultado lesivo y por la descripción abierta y no taxativa de la acción, expresada con fórmulas como 'actos preparatorios', 'dirigidos a', o 'idóneos para poner en peligro', o similares (…) El resultado de tal inflación, apenas limada por las distintas leyes despenalizadoras de los últimos años, es, lisa y llanamente, la disolución del concepto de 'bien penal' como criterio axiológico de orientación y delimitación de las opciones penales. La multiplicidad, la casualidad, la contingencia y, a veces, la inconsistencia de los bienes equivalen, de hecho, a la devaluación de la idea misma de 'bien' e indican la sobrecarga de funciones que lastra a nuestra justicia penal".[5]

(5) Ferrajoli, Luigi, *Derecho y razón*, Madrid, Trotta, 2009, p. 475.

Frente a este complejo panorama —la vigencia de los principios del derecho penal ante los vertiginosos cambios sociales— consideramos que desde una óptica limitadora del poder punitivo, el punto de partida de la cuestión nunca puede dejar de ser el bien jurídico. Es decir, sin perjuicio de que —en nuestra opinión— las figuras penales no tutelan bienes jurídicos, no debe desconocerse que, mínimamente, cumplen una función acotante de la pulsión punitiva.

2. Bien jurídico y delitos informáticos

Retornando a la cuestión de los delitos informáticos, cabe preguntarnos si, para estudiar esta materia, es posible partir —o no— de la existencia de un bien jurídico común. Al analizar las recientes modificaciones que ha tenido nuestro Código Penal, hemos advertido que se han incluido nuevos tipos dentro de títulos ya existentes, que en algunos casos parecen ser tipos de peligro abstracto. Al respecto, corresponde recordar las enseñanzas de la Dra. Nora Cherñavsky, quien en el marco del XI Encuentro de Profesores de Derecho Penal de la República Argentina, sostuvo que inicialmente había que definir si los delitos informáticos son "nuevos delitos que afectan a nuevos bienes jurídicos o bien se trata de delitos tradicionales cometidos por medios informáticos".(6)

En relación a ello, Marcelo A. Riquert ha indicado que, ante la pregunta sobre la existencia autónoma de los delitos informáticos, correspondía optar por la respuesta negativa, pues, en definitiva, se trataba de nuevos modos de agresión a través de nuevos medios. No obstante, Riquert admite que otros optan por la respuesta afirmativa, al aseverar que existe de modo independiente un derecho informático, con su correspondiente rama penal, "que se ocupa de los 'ciberdelitos' que, a su vez, tienen un bien jurídico protegido que le es propio, siendo para algunos la 'información' en términos macrosociales y, para otros, la 'pureza' de la técnica informática. Finalmente, hay quienes postulan la protección de un 'orden público tecnológico'".(7)

En nuestro ordenamiento penal, al analizar los tipos penales que podrían englobarse en lo que comúnmente se denominan "delitos informáticos",

(6) Cherñavsky, Nora A., "El delito informático", en Javier De Luca (coord.), *XI Encuentro de Profesores de Derecho Penal de la República Argentina*, Bs. As., La Ley, 2013, p. 283.

(7) Riquert, Marcelo A., "Informática y Derecho Penal", en Javier De Luca (coord.), *ibid.*, p. 292.

advertimos que todos ellos fueron incorporados a tipicidades existentes, por lo cual entendemos que son herramientas de comisión para esos delitos. Por consiguiente, parecería que no existe un bien jurídico que pueda ser denominado como "orden informático" o "seguridad informática", lo que hubiera motivado la creación de un título especial en el Código Penal.

En efecto, y tan sólo analizando la más reciente de las reformas importantes que ha tenido nuestro Código Penal, a través de la ley 26.388, se advierte que —en cuanto a la parte especial— se han modificado y/o agregado los arts. 128, 153, 153 *bis*, 155, 157, 157 *bis*, 173 inc. 16, 183, 184, 197 y 255, y fue derogado el inc. 1 del art. 117 *bis*.

A modo de ejemplo, en el delito de facilitación de la pornografía se modificó la tipicidad para abarcar la ciberpornografía, mientras que el inc. 16 del art. 173 ha contemplado la defraudación mediante cualquier técnica de manipulación informática que altere el normal funcionamiento de un sistema informático o la transmisión de datos, como sería desviar fondos de una cuenta bancaria a otra a través del sistema *home banking*. Por ello, en cada caso, el bien jurídico sigue siendo el mismo: la integridad sexual, en el primer supuesto, y la propiedad, en el segundo.

Ello ilustra que la modificación de nuestro Código Penal no ha sido estructural en esta materia, sino que se han incorporado nuevos métodos para cometer los delitos ya existentes. Por ello, coincidimos en ese sentido con Carlos Christian Sueiro, quien afirma al analizar la ley 26.388 que

> "no se crearon nuevas figuras delictivas o tipos penales, sino que se modificaron ciertos aspectos de los tipos penales ya contemplados por nuestro ordenamiento jurídico con el objeto de receptar y captar las nuevas tecnologías como medios comisivos para su ejecución. De esta manera, se afirma que la tecnología de la informática y de las comunicaciones sólo constituyen nuevos medios comisivos para realizar las acciones o conductas ya descriptas por los tipos penales previstos por nuestro Código Penal de la Nación, sin dar lugar a por el momento a nuevas ontologías o conductas que deban ser receptadas por nuestro ordenamiento jurídico".[8]

(8) Sueiro, Carlos C., "La eficiencia de la ley 26.388", en De Luca, (coord.), en *op. cit.*, p. 317.

Ante esta situación —la incorporación de los delitos informáticos como medios comisivos de otras figuras cuyo bien jurídico que pretende tutelarse es autónomo—, creemos que no es saludable la forma en que fueron incluidos estos delitos, sobre todo cuando se crean figuras asociadas a otras, que en rigor constituyen adelantos de la punibilidad. En este sentido, si bien es correcto armonizar la ley penal con el avance informático —a través de nuevos medios comisivos— observamos con preocupación que la necesaria vinculación del delito informático con el "delito principal" —es decir, el primero como medio para cometer el segundo— genera, en una gran cantidad de casos, un adelantamiento de la punibilidad a los actos preparatorios, convirtiéndose así en delitos de peligro abstracto.

En otras palabras, el legislador, frente a la preocupación que genera la cada vez mayor utilización de medios informáticos para cometer delitos, y para no dejar al sistema jurídico a un lado de los cambios tecnológicos —o para dar una respuesta punitiva a la sociedad ante nuevas problemáticas que no tienen una solución inminente—, ha agregado al texto del Código Penal la posibilidad de que determinados delitos puedan ser cometidos a través de sistemas informáticos, redes sociales, Internet…, etc. Hasta este punto parecería que no hay problemas con la cuestión del bien jurídico.

Sin embargo, y como sostuvimos anteriormente, hemos constatado que, en muchos casos, la preocupación por modernizar el Código y abarcar todas las conductas posibles —supuestamente— merecedoras de pena, ha provocado que el legislador creara delitos de peligro abstracto. ¿De qué modo? Asignando una pena a la sola utilización del medio informático, con el agregado del fin delictivo. Ello genera que, en el estado actual de la legislación, sea posible investigar y condenar a una persona por utilizar internet con alguna finalidad delictiva aunque el delito tenido en miras no se configure, ni siquiera, en grado de tentativa.

Un claro ejemplo de esta situación es el tipo de *grooming*, introducido por el art. 131 del Código Penal —norma incorporada por el art. 1 de la ley 26.904—[9] que sanciona con prisión de seis meses a cuatro años —¡la misma que para el abuso sexual simple!— al que "por medio de comunicaciones electrónicas, telecomunicaciones o cualquier otra tecnología de transmisión de datos, contactare a una persona menor de edad, con el propósito de cometer cualquier delito contra la integridad sexual de la misma".

(9) BO, 11/12/2013.

Este nuevo tipo penal ha sido fuertemente criticado, entre otros, por la Asociación Pensamiento Penal, que en un comunicado del 20 de noviembre de 2013,[10] observó que la redacción de la norma era vaga e imprecisa, por lo que vulneraba el principio de legalidad y de máxima taxatividad, además de violar el principio de proporcionalidad, toda vez que la pena era la misma que para un abuso sexual simple. Asimismo, se destacó que la figura no tenía "coherencia sistémica con los restantes delitos contra la integridad sexual", pues un joven de entre 13 y 16 años podía consentir válidamente una relación sexual. También, esta nueva figura es de acción pública, cuando algunos delitos contra la integridad sexual —los que eventualmente planearía cometer el autor de *grooming*— son dependientes de instancia privada.

A ello cabe agregar que, a nuestro entender, el mayor riesgo que genera esta "preocupación" legislativa por los delitos informáticos consiste en la sanción de conductas que claramente no superan el umbral de los actos preparatorios, protegidos constitucionalmente a través del art. 19. Esto se advierte con facilidad en el citado caso del *grooming*, pues es evidente que la persona que solamente se contacta con un menor —aunque sea para menoscabar su integridad sexual— aún está lejos de alcanzar el nivel de la tentativa, por lo que con este nuevo tipo penal se están penalizando actos preparatorios de otros delitos.

Por otra parte —y saliendo de la problemática en particular del *grooming*—, es posible que este tipo no sea el primero de los que vaya a crear el legislador, pues probablemente y merced al contexto de inflación penal en el que vivimos, se incorporen nuevas figuras penales tipificando conductas que sólo irroguen peligros abstractos. De hecho, y como se mencionó anteriormente al analizar la Convención de Budapest sobre cibercrimen, se enfatizó en la necesidad de crear, precisamente, figuras de peligro abstracto, como el mero acceso doloso y sin autorización a un sistema informático (art. 2), o la interceptación ilícita de datos informáticos no públicos (art. 3), en cuyo caso hasta autoriza, sorpresivamente, a las partes a "exigir que la infracción sea cometida con alguna intención delictiva", es decir, podría penarse aún sin dicha finalidad. Copiaría al pie el texto de esa autorización para q se entienda bien la idea.

(10) Véase [en línea] http://www.pensamientopenal.org.ar/wp-content/uploads/2013/11/COMUNICADO-GROOMING-1.pdf

Por lo demás, dicho instrumento internacional también sugiere a los miembros sancionar la sola posesión de "un dispositivo, incluido un programa informático" o 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", siempre y cuando tengan finalidad delictiva en los términos de la convención.

Por ello, coincidimos con Marco Antonio Terragni, quien con suma claridad ha sostenido que en esta materia

> "sería preferible que hubiese pocos tipos penales, redactados con precisión, que sólo castigasen con prisión los hechos más graves. Para los demás, son suficientes las reacciones provenientes del derecho administrativo y del derecho civil (…) En síntesis: solamente deben ser privados de su libertad quienes utilizan la informática para cometer delitos comunes: los que también pueden llevarse a cabo por otros medios y quienes utilizan la informática para provocar intencionalmente daños graves".(11)

Por consiguiente, consideramos que la cuestión de los delitos informáticos y su necesaria inserción en el Código Penal —siempre con respeto a los principios constitucionales— no se solucionaría con la invención de un bien jurídico autónomo —como podría ser "el orden informático" o "la seguridad informática"—, pues la vaguedad y amplitud de dichos conceptos permitiría una mayor expansión del poder punitivo, encontrándonos frente a la misma problemática de los delitos de peligro abstracto, con la única diferencia de que estarían dentro de un capítulo específico.

A nuestro modo de ver, la única solución posible sería incorporar la cuestión informática como medio comisivo de un delito de resultado o de peligro concreto, pero no formulando adelantamientos de punibilidad, si no agravando aquellas conductas que sean cometidas a través de medios informáticos —más allá de las reservas (que no son pocas) que podrían formularse a la efectividad político-criminal que tendrían estas figuras—.

En síntesis, creemos que la gran mayoría de los "delitos informáticos", así como están redactados, no son respetuosos de los principios constitucionales. Sumado a ello —lo que vuelve aún más preocupante el panorama—, consideramos que esta mala redacción no se debe a una falla en

(11) Terragni, Marco Antonio, "Conferencia", en Javier De Luca (coord.), *op. cit.*, p. 304.

la técnica legislativa —que, aunque grave, puede ser pulido—, ya que, por ejemplo, en el caso de la ley 26.904 la Cámara de Diputados, como entidad revisora, propuso reformas trascendentales al proyecto de la Cámara de Senadores, que, en definitiva, eran mucho más respetuosas de los principios fundamentales del Derecho Penal.

Sin embargo, estas modificaciones fueron descartadas por la cámara de origen al insistir con el proyecto original, con lo cual nadie podrá argumentar que no fueron "advertidos" los problemas tratados. Por consiguiente, entendemos que estos tipos penales fueron redactados de esta forma con total intención de dar una "respuesta" a la sociedad, lo cual es sumamente grave y preocupante, por lo que los jueces deben aplicar, en su máxima expresión, el principio de limitación de la respuesta contingente, y de este modo ser muy cuidadosos al momento de aplicar las normas bajo análisis o, por qué no, declararlas inconstitucionales cuando así corresponda.

Perspectiva del Derecho Penal

Parte Especial

COLOQUIOS PREPARATORIOS PARA EL XIX CONGRESO INTERNACIONAL DE DERECHO PENAL: "SOCIEDAD DE LA INFORMACIÓN Y DERECHO PENAL" (1)

Sección 2

Documento de reflexión y cuestionario de la AIDP
Relator General: **EMILIO VIANO**

Respuestas del Grupo Nacional Argentino:
JAVIER A. DE LUCA, MARCELO RIQUERT, CHRISTIAN C. SUEIRO, MARÍA ÁNGELES RAMOS y **FRANCISCO FIGUEROA**

(A) Objeto del cuestionario

Las preguntas de esta Sección tratan generalmente del "ciberdelito". Este término se entiende en el sentido de dar cobertura a las conductas criminales que afectan a intereses asociados con el uso de la tecnología de la información y comunicación (TIC), como el funcionamiento adecuado de los sistemas informáticos y de internet, la intimidad y la integridad de los datos almacenados o transferidos a o a través de las TIC o la identidad virtual de los usuarios de internet. El denominador común y rasgo característico de todas las figuras de ciberdelitos y de la investigación sobre ciberdelitos puede hallarse en su relación con sistemas, redes y datos informáticos, de un lado, y con los sistemas, redes y datos cibernéticos, del otro. El ciberdelito cubre delitos que tienen que ver con los ordenadores en sentido tradicional y también con la nube del ciberespacio y las bases datos cibernéticas.

Si se precisa cualquier aclaración, por favor, contactar con el Relator General, Emilio C. Viano por email: emilio.viano@gmail.com

(B) Prácticas legislativas y conceptos jurídicos

(1) ¿Cómo se encuentran reguladas las normas penales relativas a los ciberdelitos en su país? ¿Se recogen en un título unificado o código,

(1) AIDP, Río de Janeiro, Brasil, 31 de agosto al 6 de septiembre de 2014.

o se encuentran en códigos o títulos diversos? (Aportar, por favor, las referencias adecuadas).

Partiendo de un análisis político–criminal de la ley 26.388 de reforma en materia de criminalidad informática del Código Penal de la República Argentina (en adelante, CP) puede verificarse en primer orden que, desde una perspectiva de la técnica legislativa empleada, el legislador ha acudido a la instrumentación de una ley de reforma integral, armónica y concordante con dicho cuerpo legal.

Sin embargo, desde que se sancionó la primera ley con disposiciones penales con referencias directas a expresiones de las TICs (ley 24.766, de 1997), se fueron sucediendo hasta 2008 una serie de reformas en leyes especiales o en el propio CP que, en forma parcial, fueron incorporando tipos penales que responderían a lo que se identifica en el cuestionario como "ciberdelitos". Por eso existen previsiones fuera y dentro del CP. Entre las primeras se cuentan, en particular, las relativas a la propiedad intelectual, los delitos contra la hacienda pública o el sistema de seguridad social y los servicios de comunicaciones móviles.

(2) ¿Cuál es el impacto de las decisiones judiciales en la formulación del derecho penal relativa a los ciberdelitos?

La ley 26.388 fue sancionada en 2008 con lo cual la jurisprudencia en materia de delitos informáticos resulta sumamente escasa hasta la fecha.

No obstante, decisiones judiciales que pusieron de manifiesto problemas de tipicidad (por ej., caso "Pinamonti" de 1991 para el "daño" informático; o el caso "Autodesk", de 1997, para la propiedad intelectual) operaron de disparadores para la adopción de reformas legislativas con mayor o menor celeridad.

(3) Para hacer frente a las necesidades y circunstancias cambiantes y para alcanzar nuevos objetivos, algunas leyes sufren frecuentes reformas. Normalmente, tales reformas adoptan la forma de nuevas leyes. En algunos casos esas nuevas leyes, en lugar de modificar simplemente las partes de la ley que precisan ser cambiadas, incluyen las reformas requeridas en un texto consolidado junto con las anteriores modificaciones. Esta técnica se llama refundición (recasting). ¿Es así como las leyes sobre ciberdelitos son actualizadas y adaptadas a las realidades cambiantes en su país? Aportar, por favor, las referencias y citas adecuadas.

En general las reformas en materia penal en el área de cibercriminalidad resultan muy escasas y distanciadas en el tiempo. En su mayoría, han sido

incorporadas al CP para dotarlas de sistematicidad con las disposiciones de delitos tradicionales.

(C) Las infracciones específicas en materia de ciberdelitos

(1) ¿En lo relativo a la mens rea, deben las infracciones en material de ciberdelitos ser dolosas? ¿Se requiere un dolo específico?

La reforma de la ley 26.388 al CP se ha caracterizado por abarcar la modificación, en su mayoría, de tipos penales dolosos, sin el empleo de tipos penales culposos, a excepción del delito de "alteración, sustracción, ocultación, destrucción e inutilización de medios de prueba" (art. 255 CP), con lo cual respeta la tradición jurídico-normativa de nuestra legislación penal en cuanto a mantener a los tipos culposos como *numerus clausus*.

En el mismo orden de ideas, la ley 26.388 no ha incorporado ningún tipo omisivo, ni doloso, ni culposo, lo cual evita ampliaciones del ámbito de punibilidad.[2]

En referencia a la existencia de un dolo específico, la reforma no ha incorporado en ninguna figura el empleo de un dolo específico o ultraintención.

(2) ¿Hay también delitos imprudentes en este ámbito?

La legislación argentina prevé, como tipo culposo o imprudente, el tipo de alteración, sustracción, ocultación, destrucción e inutilización de medios de prueba.

> "Será reprimido con prisión de un (1) mes a cuatro (4) años, el que sustrajere, alterare, ocultare, destruyere o inutilizare en todo o en parte objetos destinados a servir de prueba ante la autoridad competente, registros o documentos confiados a la custodia de un funcionario público o de otra persona en el interés del servicio público. Si el autor fuere el mismo depositario, sufrirá además inhabilitación especial por doble tiempo.
>
> Si el hecho se cometiere por imprudencia o negligencia del depositario, éste será reprimido con multa de pesos setecientos cincuenta ($750) a pesos doce mil quinientos ($12.500)". (art. 255 CP)

(2) Fillia Leonardo C., Monteleone Romina, Nager Horacio S., Rosende Eduardo E., Sueiro Carlos C., "Análisis a la reforma en materia de Criminalidad Informática al Código Penal de la Nación (ley 26.388)", Suplemento de Derecho Penal y Procesal Penal, *La Ley*, 2008, pp. 15/41.

(3) En caso afirmativo, por favor, aportar una lista de tales delitos

(a) Integridad y funcionalidad del sistema TI

1. Acceso ilegal e interceptación de una transmisión.

La interceptación de comunicaciones prevista en el artículo 197 CP.

a. Objeto – ¿sistema o datos?
¿Califica su derecho penal como infracción penal la obstaculización grave, ilegítima, del funcionamiento de un ordenador y/o sistema electrónico, mediante la introducción, transmisión, daño, borrado, deterioro, alteración o supresión de información o datos de un programa, software o sistema informático?

Lo hace a través del tipo de daño del art. 183 CP.

Se prevé la alteración dolosa de registros fiscales (art. 12, ley 24769) y la alteración de controladores fiscales (art. 12 *bis*, misma ley).

b. ¿Exigencia de infracción de medidas de seguridad?
¿Es un requisito de su derecho penal que el *hacker* lleve a cabo su conducta de acceso del sistema informático usando uno o más softwares necesarios para saltar las medidas de seguridad y lograr nivel de entrada o un nivel más elevado de acceso?

No es necesario, basta con el mero acceso.

2. Interferencias con datos y sistemas

a. Objeto – ¿protección del sistema/hardware/datos?
¿Define su derecho penal el concepto de "datos electrónicos y/o informáticos"? ¿Incluye esta definición los programas, el software o codificaciones similares? Si tiene una definición, apórtela por favor, así como la referencia a los correspondientes artículos/párrafos de su código.

La reforma 26.388 contempló la introducción de terminología específica al Código Penal de la Nación. En particular, a través de la reforma al artículo 77 del CP, se incorporaron los términos documento, firma, suscripción, e instrumento privado en su modalidad digital según los siguientes párrafos:

> "... El término 'documento' comprende toda representación de actos o hechos, con independencia del soporte utilizado para su fijación, almacenamiento, archivo o transmisión.
>
> Los términos 'firma' y 'suscripción' comprenden la firma digital, la creación de una firma digital o firmar digitalmente.
>
> Los términos 'instrumento privado' y 'certificado' comprenden el documento digital firmado digitalmente..." (art. 77 CP).

b. Acto – ¿destrucción/alteración/hacer inaccesible?

El art. 183 CP castiga a quien "alterare, destruyere o inutilizare datos, documentos, programas o sistemas informáticos; o vendiere, distribuyere, hiciere circular o introdujere en un sistema informático, cualquier programa destinado a causar daños".

i. ¿Penaliza su derecho penal el borrado, alteración, conversión en inaccesible, adquisición u otra interferencia similar no autorizada con información o datos de un sistema o programa informático o electrónico?

Sí, específicamente a través de la afectación de bienes intangibles contemplados en el tipo penal de daño simple y agravado (arts. 183 y 184 CP).

ii. ¿Penaliza su derecho penal la interceptación no autorizada de cualquier forma o modo de transmisión de información o datos informáticos o electrónicos?

Sí, a través de los tipos penales de violación de secretos y privacidad.

3. Falsificación de datos

a. Objeto – ¿autenticidad?
¿Define su derecho penal como una infracción penal la introducción, alteración, borrado o supresión no autorizados de datos electrónicos o informáticos que produzca la inautenticidad de los datos con el fin de proteger la autenticidad de los datos susceptible de ser usados o aportados con fines jurídicos? Si dispone de una definición, apórtela por favor con la referencia a los correspondientes artículos/párrafos de su código y/o legislación especial.

El art. 157 *bis*, inc. 3 CP, castiga la conducta de quien "ilegítimamente insertare o hiciere insertar datos en un archivo de datos personales".

b. Acto – ¿alteración/borrado?
¿Penaliza su derecho penal como infracción penal la introducción, alteración, borrado o supresión no autorizadas de datos/información electrónica o informática que produzca la inautenticidad de los datos/información con el fin de que sea considerados o aportados a efectos jurídicos como si fueran auténticos? En caso afirmativo, aporte por favor la referencia a los artículos/párrafos correspondientes de su código.

Sí, específicamente a través de la afectación de bienes intangibles contemplados en el tipo penal de daño simple y agravado (art. 183 y 184 CP).

4. Uso abusivo de dispositivos

a. Objeto – ¿tipo de dispositivos?
¿Penaliza su derecho penal el desarrollo de un "kit de herramientas" de *hacker* en todo o en parte (e. g. capturadores de contraseñas —*password grabbers*— y

gestores de registro de claves —*key loggers*—, programas para realización de llamadas gratuitas —*blue boxing programs*—, programas de llamadas automáticas para encontrar vías de acceso a ordenadores y/o internet —*war-dialers*—, software de encriptado —*encryption* software—, programas de descifrado de contraseñas —*program password crackers*—, escáneres de vulnerabilidades de seguridad —*security vulnerability scanners*—, rastreadores de paquetes —*packet sniffers*— etc.) para el acceso no autorizado a sistemas o transmisiones electrónicas o informáticas?

No penaliza el desarrollo de herramientas, aplicaciones, ni programas, pero sí su empleo mediante la captación de datos personales.

b. Acto – ¿distribución/transferencia pública a otra persona?
i. ¿Penaliza su derecho penal el uso no autorizado de cualquiera de las herramientas de *hacker* recogidas en el epígrafe i?

Penaliza el acceso a la información sin importar la herramienta empleada.

ii. ¿Penaliza su derecho penal la distribución pública y/o transferencia a otras partes de la información electrónica hackeada?

Si mediante los tipos penales de: Publicación abusiva de correspondencia (art. 155 del CP), Revelación de secretos (art. 157 del CP), Delitos relacionados con la protección de datos personales (art. 157 *bis* del CP),

c. ¿Posesión?
¿Penaliza su derecho penal la posesión de un "kit de herramientas" de *hacker* en todo o en parte (e. g. capturadores de contraseñas —*password grabbers*— y gestores de registro de claves —*key loggers*—, programas para realización de llamadas gratuitas —*blue boxing programs*—, programas de llamadas automáticas para encontrar vías de acceso a ordenadores y/o internet —*war-dialers*—, software de encriptado —*encryption* software—, programas de descifrado de contraseñas —*program password crackers*—, escáneres de vulnerabilidades de seguridad —*security vulnerability scanners*—, rastreadores de paquetes —*packet sniffers*— etc.) para el acceso no autorizado a transmisiones o sistemas electrónicos o informáticos?

Nuestro derecho penal no contiene una figura que reprima la tenencia de programas destinados al acceso ilegitimo.

(b) Intimidad

1. Violación del carácter secreto de datos privados

a. Objeto – ¿tipos de datos privados?
(Datos privados son los datos que pertenecen a la vida privada de la gente pero que no identifican o hacen posible la identificación de una persona, e. g., estado civil, orientación sexual, estado de salud, hábitos o preferencias de compra).

i. ¿Requiere la legislación de su país que los recolectores de datos revelen sus prácticas de información con carácter previo a la recogida de información privada de los consumidores como, por ejemplo, qué información es usada, cómo se recoge y con qué fines, si se compartirá con otros o si los consumidores tendrán control sobre la revelación de sus datos privados?

ii. ¿Requiere la legislación de su país a las empresas y entidades que desarrollen sus negocios en internet que informen a los consumidores sobre la identidad de quien recoge los datos, si el suministro de los datos requeridos es voluntario u obligatorio y los pasos dados por los colectores de los datos para asegurar la confidencialidad, la integridad y la calidad de los datos?

iii. ¿Requiere la legislación de su país a las *websites* que publiquen su política de privacidad y expliquen cómo usarán la información personal antes de que los consumidores entren en el proceso de compra o en cualquier otra transacción para la que deban suministrar información sensible?

iv. ¿Penaliza el derecho penal de su país el hecho de no suministrar las garantías relativas a la revelación mencionadas más arriba (a.i; a.ii and a.iii)?

No existe un tipo penal específico que reprima la ausencia de garantías relativas a la protección de datos suministrados.

Puede haber regulación administrativa de algunos aspectos.

b. Acto – ¿uso y transferencia/distribución ilegal?
i. ¿Define el derecho penal de su país la transferencia y distribución ilegales de datos privados?

El art. 157 *bis* CP pune en su inc. 2 a quien "ilegítimamente proporcionare o revelare a otro información registrada en un archivo o en un banco de datos personales cuyo secreto estuviere obligado a preservar por disposición de la ley".

ii. ¿Penaliza el derecho penal de su país el uso, transferencia y/o distribución ilegales de datos privados?

Sí.

c. ¿Justificación?
i. ¿En qué condiciones permite la legislación de su país la recogida, procesamiento, transferencia y distribución de datos privados?

Es tema regulado por la ley 25.286 de Protección de Datos Personales del año 2000, entendida por gran parte de la doctrina como reglamentaria de la garantía constitucional del art. 43 de la Constitución Nacional (*habeas data*).

ii. ¿Qué nivel de necesidad se requiere para una recogida y/o distribución autorizadas (apremiante, importante, razonable, conveniente)? 2. Violación de la confidencialidad profesional.

a. Objeto – ¿tipo de datos privados?
i. ¿Requiere la legislación de su país que los profesionales revelen:

– Sus prácticas de recogida y gestión de la información con anterioridad a la recogida de información personal de sus pacientes o clientes:

– Sus prácticas de revelación;

– Sus obligaciones éticas profesionales;

– Y si sus pacientes o clientes tienen control sobre la revelación de sus datos personales?

ii. ¿Qué datos se encuentran, en su caso, protegidos de la manera específica? ¿Autoriza o, incluso requiere, el derecho penal de su país al personal sanitario, abogados, sacerdotes, etc. violar la confidencialidad en ciertas situaciones o por ciertas razones legalmente establecidas? ¿En qué condiciones debería hacerse? (e. g. causa razonable que permita ver o creer que hay abuso contra una víctima niño, mujer, persona de edad)?

Nuestra legislación no autoriza a los profesionales a revelar información confidencial, salvo en casos específicos (por ej. una epidemia), o por "justa causa", expresión cuyo contenido ha quedado reservado a la jurisprudencia. En algunos códigos procesales se menciona la obligación de denunciar los delitos contra la vida que determinados profesionales conozcan en el ejercicio de sus funciones, pero ello choca con otros principios como el deber de guardar el secreto profesional. La jurisprudencia se ha encargado de resolver cada caso de conflicto normativo.

b. Sujeto – ¿Tipo de autores?
¿Identifica el derecho penal de su país las categorías de profesionales sometidos a reglas de confidencialidad específicas?

c. Acto – ¿uso y transferencia/distribución ilegales?
¿Qué actos (e. g. recogida ilegal, uso, transferencia y distribución) son específicamente penalizados por la legislación penal de su país?

3. Procesamiento ilegal de los datos personales y privados

a. ¿Objeto?
¿Penaliza su derecho penal la adquisición, procesamiento, almacenamiento, análisis, manipulación, uso, venta, transferencia, etc. no autorizados e ilegales de datos privados y personales?

b. ¿Sujeto?
¿Identifica su derecho penal de manera específica las categorías de personas y entidades incluidas en esta prohibición y sanciones penales?

c. ¿Acto?
i. ¿Penaliza su derecho penal actos específicos que constituyen el todo o una parte del procesamiento ilegal de datos personales y privados? Responder, para cada categoría recogida a continuación, citando el derecho y disposiciones, en su caso, relevantes:

1. Recogida ilegal
2. Uso ilícito
3. Retención ilegal
4. Transferencia ilícita

ii. ¿Supone una diferencia el que esos datos personales y privados sean usados, transferidos etc. con fines policiales o de *law enforcement*?

d. ¿Justificación?
i. ¿En qué condiciones permite la legislación de su país la recogida, procesamiento, transferencia y distribución autorizados de datos personales y privados?

ii. ¿Qué nivel de necesidad se requiere para la recogida y/o distribución autorizadas de datos privados y personales (apremiante, importante, razonable, conveniente)?

4. Robo de identidad
(El robo o usurpación de identidad se produce cuando alguien se apropia de la información personal de otro sin su conocimiento con el fin de cometer un delito de apropiación o de defraudación. El robo de identidad es un medio para la perpetración de esquemas de fraude. Típicamente, se lleva a la víctima a la creencia de que están divulgando información personal sensible para un negocio o entidad legítima, en ocasiones como respuesta a una solicitud por *email* de actualización de información de facturación o condición de miembro, o como solicitud para un puesto de trabajo o préstamo fraudulento por internet).

Existe un proyecto de tipificación de robo de identidad de reciente trámite parlamentario, proponiendo un nuevo art. 138 *bis* al Código Penal.

a. Objeto
i. ¿Penaliza su derecho penal el robo de identidad? Cite, por favor, el derecho relevante.

No todavía.

ii. ¿Proscribe su derecho penal formas específicas de robo de identidad como, por ejemplo, el *phishing*? Se considera el *phishing* como una forma de robo de identidad *online* que utiliza *emails* con identidad suplantada destinados para atraer a los receptores a *websites* fraudulentas que tratan de engañarlos para que divulguen datos financieros personales como los números de tarjetas de crédito, nombres de usuarios y *passwords* de cuentas, números de la seguridad social, etc.

No. Lo hace por vía indirecta a través de las figuras de generales de estafa y defraudación previstas en el art. 172 CP.

b. Sujeto
¿Conoce su derecho penal responsabilidad penal ligada a una personalidad digital de una persona o a su Avatar, o a su rol digital en un juego simulado por internet (ej. *Cityville*, *Farmville*, etc.)? Cite por favor las fuentes jurídicas relevantes.

No.

(c) Protección contra contenido ilegal relacionado con las TIC

1.Objeto

a. Pornografía infantil - ¿imágenes de niños reales o virtuales?

i. ¿Penaliza su derecho penal el uso de internet con objeto de almacenar, acceder y diseminar pornografía infantil? En caso afirmativo, citar las fuentes jurídicas relevantes.

ii. En particular, ¿su derecho penal:

- Crea un nuevo delito que apunta a los delincuentes que usan internet para engañar y explotar niños con fines sexuales? Convierte en delito:

    1. transmitir?

    Sí.

    2. hacer disponible?

    Sí.

    3. exportar?

    Sí.

    4. e intencionalmente accede a pornografía infantil en Internet?

    Sí.

- Permite a los jueces ordenar el borrado de la pornografía infantil colocada en sistemas informáticos en su país;
- Permite que un juez ordene el embargo de todo material o equipo utilizado en la comisión de un delito de pornografía infantil;

El tipo penal de ofrecimiento y distribución de imágenes relacionadas con pornografía infantil:

> "Será reprimido con prisión de seis (6) meses a cuatro (4) años el que produjere, financiare, ofreciere, comerciare, publicare, facilitare, divulgare o distribuyere, por cualquier medio, toda representación de un menor de dieciocho (18) años dedicado a actividades sexuales explícitas o toda representación de sus

partes genitales con finales predominantemente sexuales, al igual que el que organizare espectáculos en vivo de representaciones sexuales explícitas en que participaren dichos menores.

Será reprimido con prisión de cuatro (4) meses a dos (2) años el que tuviere en su poder representaciones de las descriptas en el párrafo anterior con fines inequívocos de distribución o comercialización.

Será reprimido con prisión de un (1) mes a tres (3) años el que facilitare el acceso a espectáculos pornográficos o suministrare material pornográfico a menores de catorce (14) años" (art. 128 CP).

- Penaliza:

  1. El acceso a sabiendas a pornografía infantil por internet

  Sí.

  2. La transmisión de pornografía infantil por internet

  Sí

  3. Exportar pornografía infantil en internet

  Sí

  4. Poseer pornografía infantil en internet con el fin de, ej., transmitirla, exportarla.

iii. ¿Penaliza su derecho penal la oferta *online* de niños con fines sexuales vía *websites* de redes sociales o *chats*?

Sí.

iv. ¿Es la definición de pornografía infantil de su código penal similar a la recogida en los instrumentos Internacionales (e. g. Directivas UE)?

Sí.

v. ¿Se previene la victimización secundaria de las víctimas de pornografía infantil en su derecho penal? En Estados en los que la prostitución o la aparición en pornografía es un a acto castigado por el derecho penal nacional, debería ser posible la no persecución o no imposición de penas por ellas si el menor afectado ha cometido esos actos como resultado de su condición de víctima de explotación sexual o si el menor fue obligado a participar en la pornografía infantil. ¿Es esto lo que su derecho penal contempla?

No. En la Argentina no se reprime la prostitución ni la pornografía en sí mismas, sino su explotación cuando se trata de menores de edad o cuando existen medios violentos o fraudulentos en caso de mayores.

vi. ¿Penaliza su derecho penal la pornografía "infantil virtual"? La pornografía "infantil virtual" no usa niños reales o imágenes de niños reales identificables. ¿Si

la imagen no es la de un niño real, sino una combinación de millones de pixeles informáticos realizada por un artista, puede el gobierno de su país prohibir esta creación que se alega es sin víctimas? Citar, por favor, el derecho y/o decisiones judiciales aplicables.

No se reprime, se requiere que se trate de menores reales. No puede tratarse de imágenes creadas por computadoras o fotomontajes.

vii. *Mens rea*: Para ser responsable la persona debería tanto tratar de entrar en un sitio donde la pornografía infantil se encuentra disponible como saber que esas imágenes pueden encontrarse ahí. No debería aplicarse penas a personas que sin advertirlo acceden a sitios que contienen pornografía infantil. ¿Son éstas las exigencias de su derecho penal?

La acción descripta por el tipo penal es dolosa con lo cual se requiere necesariamente que conozca y quiera acceder a un sitio de pornografía infantil para la aplicación de la figura.

b. Cualquier otro objeto si la incriminación depende del uso de Tecnologías de la Información y Comunicación (TIC)

¿Penaliza su derecho penal las conductas siguientes? Cite, por favor, el derecho relevante.

1. ¿Creación y uso de verdadero anonimato en el envío y/o recepción de material por las TIC?

No se encuentra prevista ninguna figura.

2. ¿*cyber-bullying*?

Tampoco se encuentra contemplada una figura específica.

3. ¿*cyber-*stalk*ing*?

No posee una figura en particular.

4. ¿*cyber-grooming*?

Tampoco se contempla esta conducta como tipo penal específico

2. Acto – creación/acceso/posesión/transferencia/distribución pública por las TIC (dar ejemplos)

Citar las leyes específicas que incriminan la creación (incluso aun cuando no se use nunca), el acceso, la posesión (hasta si es sólo privada), la transferencia y la distribución pública por internet y otros medios electrónicos de otros materiales diferentes a los ya mencionados, especialmente debido al uso de la tecnología electrónica o de internet.

(d) Violaciones de la propiedad, incluida la propiedad intelectual, relacionadas con las TIC

¿Proscribe y penaliza específicamente su derecho penal las conductas siguientes perpetradas por medio del uso de las TIC? Citar, por favor, el derecho relevante.

1. Defraudación

Sí, a través del tipo penal del art. 173, inc. 16 CP.

2. Infracción de los derechos de la propiedad intelectual

Sí, por medio de la ley 11.723.

3. Espionaje industrial

Sí, mediante todos los tipos penales transcriptos.

(e) Criminalización de actos cometidos en el mundo virtual

¿Penaliza su derecho penal la comisión de delitos cometidos en el mundo virtual como, por ejemplo, la pornografía infantil virtual, la violencia virtual, los grafiti virtuales, la ciberdifamación, acoso sexual, acoso laboral, sin afectación de personas reales, sólo mediante representaciones virtuales? Citar por favor el derecho relevante y aportar detalles.

No contempla la existencia de tipos penales que repriman delitos virtuales.

(f) Delitos de Non-compliance

¿Penaliza su derecho penal la no cooperación con las agencias policiales y/o de persecución en el campo del ciberdelito? Los deberes de cooperar pueden consistir en deberes de retener y almacenar información, producir/entregar información solicitada por una orden específica, dar acceso a los sistemas informáticos para la instalación de filtros o dispositivos, etc. ¿Es la infracción del deber de cooperar también susceptible de generar sanciones administrativas? Citar el derecho relevante y aportar detalles.

(D) Información complementaria opcional relativa a la práctica de aplicación de la ley (incluidas estadísticas)

(1) ¿Se encuentran los ciberdelitos incluidos como tales en la recogida de datos sobre crimen en su país?

No.

(2) ¿Hay una website en su país que suministre datos e información acerca de la frecuencia, gravedad, coste, impacto etc. de los ciberdelitos en su país? En caso "afirmativo", aporte la dirección electrónica de la website.

No que sea de nuestro conocimiento.

(3) ¿Las encuestas de victimización de su país incluyen preguntas sobre ciberdelitos?

Generalmente, no.

(4) ¿Qué tipos de delito informático / fraude informático son los más frecuentemente denunciados en su país?

(5) ¿Tiene la policía y la fiscalía de su país una unidad de delitos informáticos? En caso afirmativo, ¿cuántos policías/fiscales las integran?

(6) ¿Su Facultad u otra Facultad de su país ofrece cursos sobre ciberdelito? Aporte por favor la dirección de la web.

La Facultad de Derecho de la Universidad de Buenos Aires brinda dos cursos de ciberdelitos en la carrera de Especialización de Derecho Penal.

La Facultad de Derecho de la Universidad Nacional de Mar del Plata, en su posgrado sobre "Criminalidad Económica", en conjunto con al Universidad Castilla La Mancha (España), tiene un módulo sobre "Delincuencia Informática".

La carrera de posgrado "Especialista en Derecho Penal Económico" de la Universidad Blas Pascal (Córdoba), tiene un módulo de "Delitos Informáticos". Etc.

(7) ¿Es el tema del ciberdelito objeto de la formación inicial y/o continua de jueces, fiscales y policía?

No es objeto de capacitación obligatoria. Sin embargo, en la actualidad se están incrementando los cursos de capacitación y formación en materia de criminalidad informática.

Panel 2

Aspectos problemáticos de la eventual adhesión de Argentina al Convenio sobre la Ciberdelincuencia

HORACIO J. AZZOLIN[1]

1. Introducción

Desde hace varios años, la doctrina y jurisprudencia nacional (la primera, con más intensidad que la segunda) vienen encargándose de la temática vinculada a los delitos informáticos, seguramente motivadas en la cada vez mayor utilización de la tecnología para la comisión de diversos delitos.

En el marco de este fenómeno se ha discutido acerca del alcance que debe dársele al concepto de delitos informáticos: si los mismos protegen o no un bien jurídico específico y, emparentado con ello, de qué manera deben introducirse en los códigos penales. También se trabaja sobre los aspectos procesales, en especial en lo relativo a la obtención y conserva-

(1) Abogado (UCA). Posgrado en Derecho Penal (Universidad de Palermo). Auxiliar docente (UBA). Profesor invitado en la Universidad Nacional de Río Cuarto. Fiscal a cargo de una fiscalía de juicio del fuero federal y una fiscalía de instrucción. Interviene, además, como fiscal en investigaciones por crímenes de lesa humanidad en diversas jurisdicciones del país. Designado por la Procuradora General de la Nación como punto de contacto operativo en materia de delitos informáticos en el Sistema Seguro de Comunicación Iber@ de la Red Iberoamericana de Cooperación Jurídica Internacional (IberRed).

ción de la evidencia digital, y sobre lo atinente a la cooperación internacional, que es imprescindible en esta materia ya que gran parte de estas conductas se realizan a distancia o la información necesaria para detectar a sus autores se encuentra alojada en otros países.

Todas estas cuestiones exceden el marco del presente.

La intención no es hacer un análisis integral de la reforma al Código Penal introducida por la ley 26.388, en la que se incluyeron muchas figuras vinculadas con esta temática.

El objetivo es, simplemente, comparar algunas de las disposiciones incorporadas al Código de fondo con el articulado del Convenio sobre la Ciberdelincuencia, para evaluar las consecuencias prácticas de adherir al mismo.

2. El Convenio

El Convenio sobre la Ciberdelincuencia,[2] también conocido como Convenio de Budapest, fue suscripto en Budapest, Hungría, el 23 de noviembre de 2001, entre los Estados miembros del Consejo de Europa y demás Estados invitados —Canadá, Japón, Sudáfrica, Estados Unidos de América—.

La mayoría de los Estados miembros del Consejo de Europa lo han suscripto y luego ratificado. Entre los Estados no miembros del Consejo, fue ratificado por Australia, República Dominicana, Japón y Estados Unidos de América; Canadá y Sudáfrica lo firmaron sin ratificarlo.[3]

Entró en vigor el 1 de julio de 2004 y en el trascurso del año 2010 nuestro país solicitó ser invitado a acceder al mismo.[4]

El Convenio aborda la temática vinculada con los delitos cometidos a través del uso de nuevas tecnologías de la información y las comunicaciones. Tiene tres secciones principales:

a. Derecho Penal: sección en la que los Estados parte se comprometen a ajustar su legislación interna para sancionar como delitos determinadas conductas que se mencionan.

(2) En inglés —uno de los idiomas oficiales—, *Convention on Cybercrime*.

(3) Conforme información oficial consultada en la página web del Consejo de Europa (versión en inglés), [en línea] http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=8&DF=28/10/2013&CL=ENG

(4) Ver Resolución conjunta 866/2011 y 1500/2011 de la Jefatura de Gabinete de Ministros y del Ministerio de Justicia y Derechos Humanos de la Nación.

b. Derecho Procesal Penal: en ella, los Estados parte se comprometen a ajustar su ley procesal para permitir la realización de diversas diligencias de prueba. En términos muy generales, se tiende a poder preservar e interceptar determinados datos contenidos en sistemas informáticos (datos de tráfico, datos de contenido, entre otros).

c. Cooperación Internacional: en esta sección se establecen diversos mecanismos de cooperación internacional entre los Estados parte para compartir y obtener información mediante las vías formales, aunque se establecen canales para que el intercambio de información pueda hacerse rápidamente de ser necesario.

Específicamente en materia de derecho penal de fondo, el Convenio describe determinadas conductas que son discriminadas en "Delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos" (capítulo II, sección 1, título 1, arts. 2° a 6°); "Delitos informáticos" (capítulo II, sección 1, título 2, arts. 7° y 8°); "Delitos relacionados con el contenido" (capítulo II, sección 1, título 3, art. 9°); y "Delitos relacionados con infracciones de la propiedad intelectual y de los derechos afines" (capítulo II, sección 1, título 4, arts. 10 a 13).

Concretamente, se conviene la tipificación como delito en cada derecho interno de los siguientes actos:

a. Acceso deliberado e ilegítimo a un sistema informático (art. 2°).

b. Interceptación deliberada e ilegítima de datos informáticos en transmisiones no públicas (art. 3°).

c. Ataques a la integridad de los datos, conducta definida como todo acto deliberado e ilegítimo que borre, deteriore, altere o suprima datos informáticos (art. 4°).

d. Ataques a la integridad de un sistema informático, definidos como la obstaculización grave, deliberada e ilegítima del funcionamiento de un sistema informático mediante la transmisión, daño, borrado, deterioro, alteración o supresión de datos informáticos (art. 5°).

e. Abuso de dispositivos. Contempla como supuestos:

    - La producción, venta, obtención para su uso, importación, difusión y otras formas de puesta a disposición de cualquier dispositivo —incluidos los programas— concebido para la comisión de las conductas descriptas anteriormente o de contraseñas, códigos de acceso o datos informáticos similares que permitan acceder a un sistema informático, siendo exigencia que exista la intención sea utilizarlos para cometer esas conductas (art. 6.1. a y la aclaración sobre la intención exigida en el art. 6.2.); y

- La mera posesión de alguno de esos elementos con intención de ser utilizados para cometer esos ilícitos (art. 6.1. b).

f. Falsificación informática, definida como la introducción, alteración, borrado o supresión de datos informáticos que genere datos no auténticos con la intención que sean tomados o utilizados a los efectos legales como auténticos (art. 7°).

g. Fraude informático, consistente en la realización de actos deliberados que causen perjuicio patrimonial mediante la introducción, borrado o supresión de datos informáticos o cualquier interferencia en el funcionamiento de un sistema informático (art. 8°)

h. Pornografía infantil. El art. 9° del Convenio describe varias conductas relacionadas con este tópico:

- La producción de pornografía infantil con intención de difundirla a través de un sistema informático.
- La oferta o puesta a disposición, la difusión o transmisión y la adquisición de la misma a través de un sistema informático.
- La posesión de pornografía infantil en un sistema informático o en un dispositivo de almacenamiento de datos informáticos (art. 9.1).

El mismo artículo define pornografía infantil (art. 9.2) como todo material pornográfico que contenga:

- la representación visual de un menor, o de una persona que parezca serlo, adoptando un comportamiento sexualmente explícito; e
- imágenes realistas que representen a un menor adoptando un comportamiento sexualmente explícito.

A los efectos de la Convención, debe tratarse de un menor de 18 años, aunque las partes pueden elegir un límite de edad inferior que debe ser como mínimo de 16 años (art. 9.3).

i. Delitos relacionados con la propiedad intelectual. Se establece la obligación de sancionar la comisión deliberada, a escala comercial y por medio de un sistema informático, de las infracciones de propiedad intelectual establecidas en las legislaciones internas en función de las obligaciones contraídas en aplicación:

- Del Convenio de Berna para la protección de las obras literarias y artísticas, del Tratado de la Organización Mundial de la Propiedad Intelectual (OMPI) sobre Derechos de Autor[5] y del Acuerdo sobre los aspectos de los derechos de propiedad intelectual relacionados con el comercio[6] (art. 10.1),

(5) Nuestro país aprobó estos instrumentos por ley 25.140, de 1999.

(6) Nuestro país lo ratificó por ley 24.425, de 1994.

- de la Convención Internacional sobre la Protección de los Artistas, Intérpretes o Ejecutantes, los Productores de Fonogramas y los Organismos de Radiodifusión[7] y del Tratado de la OMPI sobre Interpretación o Ejecución y Fonogramas[8] (art. 10.2).

j. Tentativa y complicidad. Se establece la obligación de sancionar cualquier complicidad deliberada con vistas a la comisión de alguno de los delitos descriptos más arriba (art. 11.1) y toda tentativa deliberada de cometer las conductas denominadas como interceptación ilícita (art. 3), ataques a la integridad de los datos (art. 4), ataques a la integridad del sistema (art. 5), falsificación informática (art. 7), fraude informático (art. 8), producción de pornografía infantil con intención de difusión por un sistema informático (art. 9.1.a) y su difusión (art. 9.1.c).

k. Responsabilidad de las personas jurídicas. Se establece adecuar la legislación para que pueda exigirse responsabilidad a las personas jurídicas por los delitos previstos en aplicación del Convenio en la medida en que los mismos fueran cometidos por cuenta de las mismas por parte de persona física —a título individual o como miembro de alguno de sus órganos— (art. 12.1).

   Además, los Estados deben garantizar que pueda responsabilizarse a una persona jurídica cuando la ausencia de vigilancia o de control por parte de una persona física haya permitido la comisión de un delito previsto en aplicación del Convenio por parte de una persona física que actúa por cuenta de la persona jurídica y bajo su autoridad (art. 12.2).

   La misma norma dispone que, en base a los principios jurídicos de cada parte, la responsabilidad puede ser penal, civil o administrativa (art. 12.3) y que dicha responsabilidad debe entenderse sin perjuicio de la responsabilidad penal de las personas físicas que cometieron el hecho (art. 12.4).

3. Situación en nuestro país

Como se adelantó, nuestro país no es Estado parte del Convenio, aunque se habrían generado los mecanismos necesarios para obtener una invitación a adherir a él.

Pese a ello, durante el año 2008 se sancionó la ley 26.388 que introdujo en el Código Penal (en adelante, CP) un conjunto de delitos vinculados con la criminalidad informática, tipificando algunas de las figuras delictivas contempladas en el Convenio de Budapest, si bien con algunas diferencias.

(7) Ratificada en Argentina por ley 23.921, de 1991.

(8) Ratificada por ley 25.140, de 1999.

Concretamente se produjeron las siguientes reformas:

a. Se incorporaron, como últimos párrafos del art. 77 CP, definiciones para los términos "documento", "firma", "suscripción", "instrumento privado" y "certificado" (art. 1, ley 26.388).

b. Se sustituyó el art. 128 CP por el siguiente:

> "Será reprimido con prisión de seis (6) meses a cuatro (4) años el que produjere, financiare, ofreciere, comerciare, publicare, facilitare, divulgare o distribuyere, por cualquier medio, toda representación de un menor de dieciocho (18) años dedicado a actividades sexuales explícitas o toda representación de sus partes genitales con fines predominantemente sexuales, al igual que el que organizare espectáculos en vivo de representaciones sexuales explícitas en que participaren dichos menores.
>
> Será reprimido con prisión de cuatro (4) meses a dos (2) años el que tuviere en su poder representaciones de las descriptas en el párrafo anterior con fines inequívocos de distribución o comercialización.
>
> Será reprimido con prisión de un (1) mes a tres (3) años el que facilitare el acceso a espectáculos pornográficos o suministrare material pornográfico a menores de catorce (14) años" (art. 2 ley 26.388, en consonancia —aunque no idéntico— con lo descripto en el art. 9 del Convenio de Budapest).

c. Se sustituyó el epígrafe del Capítulo III, del Título V, del Libro II del Código Penal, por el siguiente: "Violación de Secretos y de la Privacidad" (art. 3, ley 26.388; el título es similar al Título 1, de la Sección del Capítulo II del Convenio de Budapest).

d. Se sustituyó el art. 153 CP por el siguiente:

> "Será reprimido con prisión de quince (15) días a seis (6) meses el que abriere o accediere indebidamente a una comunicación electrónica, una carta, un pliego cerrado, un despacho telegráfico, telefónico o de otra naturaleza, que no le esté dirigido; o se apoderare indebidamente de una comunicación electrónica, una carta, un pliego, un despacho u otro papel privado, aunque no esté cerrado; o indebidamente suprimiere o desviare de su destino una correspondencia o una comunicación electrónica que no le esté dirigida.
>
> En la misma pena incurrirá el que indebidamente interceptare o captare comunicaciones electrónicas o telecomunicaciones provenientes de cualquier sistema de carácter privado o de acceso restringido.
>
> La pena será de prisión de un (1) mes a un (1) año, si el autor además comunicare a otro o publicare el contenido de la carta, escrito, despacho o comunicación electrónica.

Si el hecho lo cometiere un funcionario público que abusare de sus funciones, sufrirá además, inhabilitación especial por el doble del tiempo de la condena" (art. 4 ley 26.388, en consonancia con el art. 3 del Convenio de Budapest).

e. Se incorporó como artículo 153 *bis* CP, el siguiente:

"Será reprimido con prisión de quince (15) días a seis (6) meses, si no resultare un delito más severamente penado, el que a sabiendas accediere por cualquier medio, sin la debida autorización o excediendo la que posea, a un sistema o dato informático de acceso restringido.

La pena será de un (1) mes a un (1) año de prisión cuando el acceso fuese en perjuicio de un sistema o dato informático de un organismo público estatal o de un proveedor de servicios públicos o de servicios financieros" (art. 5, ley 26.388, en base al art. 2 del Convenio de Budapest).

f. Se sustituyó el art. 155 CP, por el siguiente:

"Será reprimido con multa de pesos un mil quinientos ($ 1.500) a pesos cien mil ($ 100.000), el que hallándose en posesión de una correspondencia, una comunicación electrónica, un pliego cerrado, un despacho telegráfico, telefónico o de otra naturaleza, no destinados a la publicidad, los hiciere publicar indebidamente, si el hecho causare o pudiere causar perjuicios a terceros.

Está exento de responsabilidad penal el que hubiere obrado con el propósito inequívoco de proteger un interés público" (art. 6 ley 26.388, se condice con el espíritu de las conductas comprendidas en el Título 1, Sección 1, Capítulo II del Convenio de Budapest "Delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos").

g. Se sustituyó el art. 157 CP por el siguiente:

"Será reprimido con prisión de un (1) mes a dos (2) años e inhabilitación especial de un (1) a cuatro (4) años, el funcionario público que revelare hechos, actuaciones, documentos o datos, que por ley deben ser secretos" (art. 7 ley 26.388, en base al espíritu de los injustos comprendidos en el Título 1, Sección 1, Capítulo II del Convenio de Budapest "Delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos").

h. Se sustituyó el artículo 157 *bis* CP por el siguiente:

"Será reprimido con la pena de prisión de un (1) mes a dos (2) años el que:

1. A sabiendas e ilegítimamente, o violando sistemas de confidencialidad y seguridad de datos, accediere, de cualquier forma, a un banco de datos personales;

2. Ilegítimamente proporcionare o revelare a otro información registrada en un archivo o en un banco de datos personales cuyo secreto estuviere obligado a preservar por disposición de la ley.

3. Ilegítimamente insertare o hiciere insertar datos en un archivo de datos personales.

Cuando el autor sea funcionario público sufrirá, además, pena de inhabilitación especial de un (1) a cuatro (4) años" (art. 8, ley 26.388, basándose en lo dispuesto en los arts. 2 y 4 del Convenio de Budapest).

i. Se incorporó como inciso 16 del art. 173 CP (que trata las defraudaciones especiales), el siguiente:

"El que defraudare a otro mediante cualquier técnica de manipulación informática que altere el normal funcionamiento de un sistema informático o la transmisión de datos" (art. 9 ley 26.388, conforme el art. 8 de Budapest).

j. Se incorporó como segundo párrafo del art. 183 CP (que regula el delito de daño), el siguiente:

"En la misma pena incurrirá el que alterare, destruyere o inutilizare datos, documentos, programas o sistemas informáticos; o vendiere, distribuyere, hiciere circular o introdujere en un sistema informático, cualquier programa destinado a causar daños" (art. 10 ley 26.388, conforme los arts. 4 y 5 del Convenio de Budapest).

k. Se sustituyó el art. 184 CP (que sanciona el daño agravado), por el siguiente:

"La pena será de tres (3) meses a cuatro (4) años de prisión, si mediare cualquiera de las circunstancias siguientes:

1. Ejecutar el hecho con el fin de impedir el libre ejercicio de la autoridad o en venganza de sus determinaciones;

2. Producir infección o contagio en aves u otros animales domésticos;

3. Emplear substancias venenosas o corrosivas;

4. Cometer el delito en despoblado y en banda;

5. Ejecutarlo en archivos, registros, bibliotecas, museos o en puentes, caminos, paseos u otros bienes de uso público; o en tumbas, signos conmemorativos, monumentos, estatuas, cuadros u otros objetos de arte colocados en edificios o lugares públicos; o en datos, documentos, programas o sistemas informáticos públicos;

6. Ejecutarlo en sistemas informáticos destinados a la prestación de servicios de salud, de comunicaciones, de provisión o transporte de energía, de medios de transporte u otro servicio público" (art. 11 ley 26.388, conforme también los arts. 4 y 5 del Convenio de Budapest).

l. Se sustituyó el art. 197 CP por el siguiente:

> "Será reprimido con prisión de seis (6) meses a dos (2) años, el que interrumpiere o entorpeciere la comunicación telegráfica, telefónica o de otra naturaleza o resistiere violentamente el restablecimiento de la comunicación interrumpida" (art. 12 ley 26.388, conforme el espíritu del art. 3 del Convenio de Budapest).

m. Se sustituyó el artículo 255 CP, por el siguiente:

> "Será reprimido con prisión de un (1) mes a cuatro (4) años, el que sustrajere, alterare, ocultare, destruyere o inutilizare en todo o en parte objetos destinados a servir de prueba ante la autoridad competente, registros o documentos confiados a la custodia de un funcionario público o de otra persona en el interés del servicio público. Si el autor fuere el mismo depositario, sufrirá además inhabilitación especial por doble tiempo.
>
> Si el hecho se cometiere por imprudencia o negligencia del depositario, éste será reprimido con multa de pesos setecientos cincuenta ($ 750) a pesos doce mil quinientos ($ 12.500)" (art. 13 ley 26.388).

4. Problemas de adecuación

Como puede advertirse, nuestro país ha incorporado a su legislación interna muchas de las conductas que se consideraron delitos en el Convenio de Budapest.

Pese a que los tipos no son idénticos, aparecen siguiendo los lineamientos trazados en el instrumento internacional, muy en especial en lo relativo al acceso ilícito a un sistema informático, la interceptación ilícita de datos informáticos, los ataques a la integridad de los datos y del sistema, la falsificación y el fraude informáticos, y los delitos relacionados con la pornografía infantil.

De hecho, la sanción de la ley 26.388 fue presentada como muestra del cumplimiento suficiente del requisito de la adecuación de la ley de fondo a los parámetros de ese instrumento internacional.[9]

Pero si nuestro país decide adherir al Convenio, necesariamente deberá discutirse acerca de si es posible incorporar a nuestra legislación algunos aspectos del convenio que no fueron tratados en la reforma de 2008. Recordemos al respecto que los Estados partes tienen la obligación de sancionar como delito las conductas descriptas en la Convención; la adhesión a Budapest implicaría en principio respetar esa manda.

(9) Ver Resolución conjunta 866/2011 y 1500/2011 de la Jefatura de Gabinete de Ministros y del Ministerio de Justicia y Derechos Humanos de la Nación.

Algunos aspectos podrían ser obviados ya que el Convenio prevé la posibilidad de efectuar reservas. Aunque, conforme su art. 42, solo pueden realizarse algunas específicamente previstas (en los arts. 4.2, 6.3, 9.4, 10.3, 11.3, 14.3, 22.2, 29.4 y 41.1) y no puede formularse ninguna otra.[10]

En definitiva, adherir a Budapest implica la obligación de incorporar a nuestro ordenamiento interno interna una serie de disposiciones (en materia penal, procesal penal y de cooperación internacional) que, en algunos pocos casos, no parecen compatibles con nuestra actual legislación o al menos generarán situaciones que deben tenerse en cuenta.

Dejando de lado, para otra ocasión, algunos aspectos de la parte procesal y de cooperación internacional de la Convención que deben analizarse, se advierten algunos inconvenientes en los siguientes tópicos:

4.1. La regulación de lo que denomina "abuso de los dispositivos" (art. 6)

El Convenio, en su artículo 6, regula lo que denomina "abuso de los dispositivos", describiendo los siguientes actos:

a. La producción, venta, obtención para su utilización, importación, difusión u otra puesta a disposición de una contraseña, código de acceso o datos informáticos similares que permitan acceder en todo o en parte de un sistema informático y de cualquier dispositivo (incluyendo un programa informático) concebido o adaptado principalmente para la comisión de cualquiera de los siguientes delitos: accesos ilícitos a sistemas informáticos (art. 2); intercepción de transmisiones dirigidas a un sistema informático (art. 3); supresión o alteración de daños informáticos (—ataques a la integridad de los datos— art. 4) y obstrucción ilegítima del funcionamiento de un sistema informático (—ataques a la integridad del sistema— art. 5) —art. 6.1.a—.

b. La posesión de algunos elementos mencionados más arriba con la intención de cometer los delitos allí mencionados. Las partes pueden exigir en su derecho interno que la posesión sea de un número determinado de dichos elementos para que se considere que existe responsabilidad penal —art. 6.1.b—.

En nuestro país, en la ley citada solo se dispuso sancionar a quien "vendiere, distribuyere, hiciere circular o introdujere en un sistema informático cualquier programa destinado a causar daños" (art. 10 ley 26.338, que modifica el art. 183 CP).

(10) En lo que interesa, la Convención de Viena sobre el Derecho de los Tratados (aprobada por ley 19.865) establece que un Estado puede formular reservas en el momento de firmar, ratificar, aceptar o aprobar un tratado o de adherirse al mismo salvo, que estén prohibidas en el Tratado, o que sólo puedan hacerse determinadas reservas entre las cuales no está la que se pretende formular o que sean incompatibles con su objeto y fin (art. 19).

Puede observarse que han quedado fuera de reproche penal, por un lado, acciones tales como la producción, obtención e importación. Por el otro, las acciones solo pueden recaer sobre programas y no sobre otros dispositivos, contraseñas, códigos de acceso y datos informáticos similares para acceder a un sistema informático. Tampoco se ha sancionado la tenencia de estos elementos.

La adhesión al Convenio implicaría incorporar como delito la mayoría de las conductas omitidas, al menos que formulemos una reserva, que solo podría ser formulada con relación a la norma que contempla como ilícito la tenencia, producción e importación, sin afectar las conductas de vender, distribuir o poner a disposición contraseñas, códigos de acceso o datos informáticos que permitan acceder a un sistema (art. 6.3).

La reserva podría motivarse en que la conducta descripta implica un adelantamiento de la pena a actos que pueden considerarse meramente preparatorios y que, y esto es fundamental, no se condicen con los principios de un derecho penal liberal que parecería exigir concretas afectaciones a bienes jurídicos(11) y que cuestiona severamente la expansión de los delitos de peligro abstracto. El Convenio parece hacerse cargo, en cierta medida, de dicha realidad cuando exige que la tenencia tenga un fin específico (cometer alguno de los delitos previstos en sus arts. 2 a 5) y faculta a los Estados a determinar a partir de qué número de dispositivos hallados en poder de una persona puede responsabilizársela penalmente.

Esto, sin perjuicio de destacar que nuestro Código Penal mantiene vigentes normas similares que colisionan con esta visión. Por ejemplo, reprime al que fabricare introdujere en el país o conservare en su poder, materias o instrumentos conocidamente destinados a cometer alguna de las falsificaciones previstas en el Código (art. 299) y la portación de armas de fuego, con una pena atenuada cuando resultare evidente la falta de intención de utilizar las armas portadas con fines ilícitos (art. 189 *bis,* inc. 2, primero, segundo, tercero, cuarto y sexto párrafo).

Sin embargo, la reserva dejaría vigente la obligación del Estado de modificar el Código Penal para incluir como objeto de las conductas típicas del art. 183 CP no sólo los programas sino también otros dispositivos similares (hay una relación de género y especie entre los dispositivos y los progra-

(11) Donna, Edgardo, "¿Es posible un derecho penal liberal?" en *Revista de Derecho Penal,* Rubinzal-Culzoni, Año 2003-1.

mas) y las contraseñas, códigos de acceso o datos informáticos similares que permitan acceder a un sistema informático. En ese sentido, la reforma parecería necesaria para ampliar la protección penal del bien jurídico.

Restaría discutir finalmente si la conducta de vender alguno de estos elementos (contemplada en Budapest y en nuestra legislación) puede considerarse o no un acto preparatorio. Esta cuestión —importante, por cierto—, excede el marco del presente en la medida en que esa conducta ya está sancionada por nuestro ordenamiento interno y no depende de la adhesión a Budapest.

4.2. La regulación de lo que denomina "delitos relacionados con la pornografía infantil" (art. 9)

El Convenio regula, en su art. 9, lo que denomina "delitos relacionados con la pornografía infantil", describiendo los siguientes actos:

a. La producción de pornografía infantil con intención de difundirla a través de un sistema informático.
b. La oferta o puesta a disposición de la misma a través de un sistema informático.
c. Su difusión o transmisión a través de un sistema informático.
d. La adquisición, para si o para terceros, de pornografía a través de un sistema informático.
e. La posesión de la misma en un sistema informático o en un dispositivo de almacenamiento de datos informáticos (art. 9.1.).

Define, además, que por pornografía infantil se entiende a todo material pornográfico que contenga la representación visual de:

a. Un menor (en principio de 18 años) adoptando un comportamiento sexualmente explícito.
b. Una persona que parezca un menor adoptando ese mismo comportamiento.
c. Imágenes realistas que representen a un menor adoptando ese tipo de comportamiento (art. 9.2).

En Argentina, la reforma al Código ha decidido sancionar a quien

> "produjere, financiare, ofreciere, comerciare, publicare, facilitare, divulgare o distribuyere por cualquier medio, toda representación de un menor de dieciocho años dedicado a actividades sexuales explícitas o toda representación de sus partes genitales con fines predominantemente sexuales" [y a quien] "tuviere en su poder representaciones de las descriptas (…) con fines inequívocos de distribución o comercialización" (art. 2 de la ley 26.388, que modifica el art. 128 del Código Penal).

Como se advierte, en nuestra legislación no se sancionó la adquisición de pornografía. Además, la tenencia de material pornográfico debe tener un fin específico e inequívoco, a diferencia de lo establecido en el Convenio.[12]

Finalmente, el concepto de pornografía se restringió a la representación de un menor de 18 años, excluyendo los casos de un adulto que se hace pasar por un menor y las imágenes realistas —que implican que no hay un menor involucrado sino que solo se lo representa—.

La adhesión a Budapest implicaría, entonces, sancionar la adquisición de pornografía, retirar el dolo específico de la tenencia del material pornográfico y ampliar el concepto de pornografía infantil a otros supuestos que no involucran a menores.

Sin embargo, según el Convenio (art. 9.4) podría —y considero que debería— hacerse una reserva con relación a la norma que sanciona la adquisición de pornografía. Si bien esta acción aparece como el último eslabón de la cadena de tráfico (en ese sentido, es similar a lo que sucede, por ejemplo, con el tráfico de sustancias estupefacientes) su punición aparece inconveniente desde un punto de vista político-criminal. Sancionar al cliente, si bien puede parecer atractivo desde el discurso, puede generar que las agencias de persecución estatal centren sus esfuerzos en esa parte de la cadena sin avanzar en quienes se encargan de su producción y distribución a gran escala (algo similar ocurre con los estupefacientes y su tenencia, y ha sido objeto de tratamiento a lo largo de estos años por la jurisprudencia de la Corte Suprema).

El Convenio también permite hacer una reserva sobre la norma que sanciona la tenencia del material pornográfico. En el caso argentino, esa acción fue sancionada como delito, con lo cual la reserva no sería necesaria. Más allá de las objeciones que podamos tener con relación a la tipificación de esta conducta —similares a las mencionadas anteriormente respecto de la adquisición—, no se tratará el tema por exceder el objeto del presente. Lo que sí hay que tener en claro es que la adhesión implicará analizar si el dolo específico de tenencia consagrado en nuestra norma (que, al menos, delimita el universo de supuestos punibles evitando así la penalización del tenedor involuntario del material) puede mantenerse o no, en la medida en que Budapest no lo contempla.

(12) En ese sentido, nuestra norma respeta el criterio sentado en el art. 3 del Protocolo Relativo a la Venta de Niños, la Prostitución Infantil y la Utilización de los Niños en la Pornografía, que complementa la Convención de las Naciones Unidas sobre los Derechos del Niño (ley 25.763).

Finalmente, el Convenio permite formular una reserva en relación a lo que debe entenderse por pornografía infantil. Concretamente, en relación a los supuestos en los que un adulto simule ser un menor y en los que se represente una situación en la que un menor no esté involucrado. La reserva, en este caso, es necesaria para que pueda ser compatibilizada con nuestra legislación, teniendo en cuenta el bien jurídico que se pretende proteger, que siempre debe involucrar a menores de edad.[13]

4.3. La sanción de lo que denomina "complicidad" (art. 11.1.)

Otro aspecto problemático de Budapest es la sanción, en su art. 11.1, de lo que denomina "complicidad" y define como "cualquier complicidad deliberada con vistas a la comisión de alguno de los delitos previstos", ya que sobre este aspecto no puede formularse reserva (art. 42).

La adhesión implicaría la consagración de esta norma, que puede ser discutida porque implicaría penar actos preparatorios. Sin embargo, debe mencionarse que en nuestra Ley de Estupefacientes existe una norma similar (art. 29 *bis,* ley 23.773) cuyos presupuestos —en especial, el momento a partir del cual la conspiración puede ser punible—[14] deberían ser tomados como parámetros en una futura eventual reforma.

4.4. El tratamiento de lo relativo a la responsabilidad de las personas jurídicas (art. 12)

Finalmente, el art. 12 trata lo relativo a la responsabilidad de las personas jurídicas en los siguientes términos:

> "1. Las Partes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias para permitir que las personas jurídicas puedan ser tenidas por responsables de las infracciones establecidas en el presente Convenio, cuando éstas sean cometidas por una persona física, actuando ya sea a título individual, ya sea como miembro de un órgano de la persona jurídica, que ejerce un poder de dirección en su seno, cuyo origen se encuentre en:
>
> a. un poder de representación de la persona jurídica;
>
> b. una autorización para tomar decisiones en nombre de la persona jurídica;

(13) Palazzi, Pablo, *Los delitos informáticos en el Código Penal. Análisis de la ley 26.388*, Bs. As., Abeledo-Perrot, 2009, p. 45.

(14) Ver, al respecto, Falcone, Roberto y Capparelli, Facundo, *Tráfico de estupefacientes y derecho penal,* Bs. As., Ad-Hoc, 2002, p. 345 y ss.

c. una autorización para ejercer control en el seno de la persona jurídica.

2. Fuera de los casos previstos en el párrafo 1, las Partes adoptarán las medidas necesarias para asegurar que una persona jurídica puede ser tenida por responsable cuando la ausencia de vigilancia o de control por parte de cualquier persona física mencionada en el párrafo 1 haya permitido la comisión de las infracciones descritas en el párrafo 1 a través de una persona física que actúa bajo autorización de la persona jurídica.

3. La responsabilidad de la persona jurídica podrá resolverse en sede penal, civil o administrativa, dependiendo de los principios jurídicos propios del Estado.

4. Esta responsabilidad se establecerá sin perjuicio de la responsabilidad penal de las personas físicas que hayan cometido la infracción…".

Sobre este aspecto tampoco pueden formularse reservas, de forma tal que, en un escenario de adhesión al Convenio, nuestro país deberá establecer qué esquema de responsabilidad le otorgará a las personas jurídicas más allá de la responsabilidad penal de las personas físicas que la integran. Lo que se encare al respecto deberá necesariamente replicarse en otros aspectos, como la criminalidad económica.

5. Conclusiones

Se han puntualizado tanto aquellos aspectos —desde la óptica del derecho penal— que aparecen como problemáticos en el caso de que nuestro país decida adherir al Convenio sobre la Ciberdelincuencia como algunas de las soluciones posibles. Queda pendiente hacer este mismo análisis —porque hay problemas similares— desde otros aspectos relacionados con las normas relativas al proceso penal y a la cooperación internacional, también consagradas en ese instrumento.

Si el presente sirve para generar una discusión sobre estos tópicos, habrá cumplido su cometido.

La criminalidad informática en el Anteproyecto de Código Penal de la Nación

CARLOS CHRISTIAN SUEIRO[1]

1. Introducción

El siguiente trabajo tiene por finalidad realizar un análisis de la legislación nacional en materia de criminalidad informática, adentrándose en el estudio del reciente Anteproyecto de Ley de Reforma, Actualización e Integración del Código Penal de la Nación (decreto 678/2012), a efectos de poder establecer qué reformas y actualizaciones resultan indispensables para lograr una política criminal eficiente en torno al tratamiento de los delitos de alta tecnología o perpetrados mediante dispositivos digitales.

Para poder abordar esta temática, dividiremos el trabajo en cuatro etapas o ejes analíticos.

El primero de ellos denominado "La sociedad del siglo XXI, la sociedad de la información", tendrá por finalidad exhibir cómo las tecnologías de la informática y de la comunicación han modificado todas nuestras actividades

(1) Abogado, especialista en Derecho Penal (UBA). Realizó estudios en Göttingen, Alemania (2011); Salzburg, Austria (2012); y Siracusa, Italia (2013). Jefe de Trabajos Prácticos de las cátedras de los Dres. Alagia y Niño (UBA). Secretario Letrado de la Defensoría Oficial ante la CSJN.

culturales tales como la política, la economía, la sociología, la medicina, la biónica, la genética, el derecho, las relaciones exteriores, las comunicaciones, la educación, la pedagogía, los servicios de transporte, la música o el arte.

El segundo punto centrará su análisis en los "Antecedentes nacionales y las leyes de reforma en materia de criminalidad informática al Código Penal de la Nación (leyes 26.388, 26.685 y 26.904)", a los fines de conocer con qué dispositivos normativos se cuenta en la actualidad en nuestro país para afrontar la criminalidad de alta tecnología.

Luego de abordar nuestras disposiciones legales vigentes en materia de criminalidad informática, daremos paso, en un tercer apartado, al estudio y análisis de "La criminalidad informática en el Anteproyecto de Ley de Reforma, Actualización e Integración al Código Penal de la Nación (decreto 678/2012)", a fin de conocer qué actualizaciones y reformas se han propuesto en materia de delitos cometidos a través de medios informáticos o dispositivos digitales.

En una cuarta y última etapa, realizaremos nuestras "Recomendaciones y sugerencias en torno a la actualización de la ley penal y procesal penal en materia de criminalidad informática", conforme el estado actual de la legislación nacional y la infraestructura disponible por la administración de justicia a los efectos de poder afrontar este cambio paradigmático, que implica el traspaso de una sociedad analógica propia de finales del siglo XX a una sociedad digital propia del siglo XXI.

Finalmente, se presentarán las conclusiones.

2. La sociedad del siglo XXI, la sociedad de la información

Sin lugar a dudas, la sociedad del siglo XXI se encuentra definida y caracterizada por el avance de las tecnologías de la información y comunicación (TIC), y cómo ellas han modificado cada una de las actividades culturales que la comunidad realiza y despliega diariamente, influyendo así en la política, la economía, la sociología, la medicina, la biónica, la genética, el derecho, las relaciones exteriores, las comunicaciones, la educación, la pedagogía o los servicios de transporte, entre muchas otras.

En virtud del impacto e influencia que la informática ha tenido en la sociedad de fines del siglo XX y de la primera década del siglo XXI es que a la sociedad actual se la conoce o define como la "sociedad de la información".

Sería inimaginable en nuestros días pensar una sociedad sin Internet ni el empleo de motores de búsqueda tales como Google[2] o Yahoo ni el uso de correos electrónicos (*emails*), mensajes de texto (*sms*), mensajería instantánea (*mms*), micromensajería (*Twitter*), chats (*Messenger, Messenger* Yahoo*, BlackBerry Messenger,* Google Talk*,* Whatsapp*, Line, Viber*), blogs, fotologs, redes sociales (Facebook,[3] Myspace, Sonico, Hi5, Orkut, Haboo Hotel, Linkedln), o programas de geolocalización como *Foursquare*.

Es más, estos medios de comunicación electrónicos a los cuales acudimos diariamente, hoy no solo se encuentran disponibles en computadoras de escritorio o portátiles como *notebooks*, *netbooks*, *ultrabooks* o *tablets*, sino también en teléfonos celulares inteligentes (*smartphones*) y más recientemente hasta en relojes inteligentes (*SmartWatch*)[4] y anteojos inteligentes (Google *Glass Proyect*). Tan indispensables se nos han convertido estas nuevas tecnologías de la informática y la comunicación en todas nuestras labores cotidianas que incluso han generado que a raíz de su empleo constante y habitual haya surgido la necesidad de trasladar las reglas de cortesía básica a las comunicaciones realizadas a través de dispositivos electrónicos debido a la habitualidad de su empleo y al desplazamiento y desuso de los medios tradicionales de comunicación, como por ejemplo, el correo postal.

Por ello,

> "con el avance de la tecnología, las reglas de cortesía, que constituían las normas básicas de la conversación o la correspondencia, se han trasladado desde el lenguaje oral y el género epistolar a la red, a tal punto que, según los expertos, todo navegante educado deberá observar un buen número de normas de *netiqueta*; este neologismo es una castellanización del inglés *netiquette*".[5]

---

(2) Sobre la evolución de Google como motor de búsqueda, ver Reischl, Gerald, *El engaño* Google. *Una potencia mundial sin control en Internet*, (trads. Héctor Piquer y Cristina Sánchez), 1ª ed., Bs. As., Sudamericana, 2009; y Cassin, Barbara, *Googléame. La segunda misión de los Estados Unidos,* 1ª ed., Bs. As., FCE, 2008.

(3) Sobre la irrupción de Facebook, ver Faerman, Juan, *Faceboom. El nuevo fenómeno de masas* Facebook, Bs. As., Ediciones B, 2009.

(4) Es el caso de los recientes modelos lanzados por las firmas *Sony (SmartWatch), Apple (iPhone Wrist & iWatch), Samsung (Samsumg Galaxy Gear) y Motorola (Moto Actv).*

(5) De Gavaldá y Castro, Rubén A., *Ceremonial. Un arte para comprender la vida*, Bs. As., Paidós, 2010, p. 85.

El surgimiento de reglas de cortesía mínima o normas básicas de conversación en el ambiente digital no constituye una cuestión menor, sino que todo lo contrario; como refiere el filólogo e historiador francés Milad Doueihi, el desarrollo de la informática y las tecnologías de la comunicación han influido tan profundamente en estas últimas décadas en nuestro desarrollo como civilización que una prueba cabal de ello lo constituye sin lugar a dudas el advenimiento de la *netiqueta*.[6]

Es más, tal ha sido el impacto de la informática a nivel sociológico que no solo ha llevado al advenimiento de la *netiqueta*, sino que ha generado también el surgimiento de grupos de identidad basados tanto en el contacto social directo como a través de sitios virtuales como blogs, fotologs o redes sociales, como es el caso de denominados los *floggers*.

Pero el irrefrenable avance de las telecomunicaciones y la informática ha generado cambios sociales más radicales que el nacimiento de la *netiqueta* o el surgimiento de grupos de identidad virtual como los *floggers*, pues también ha dado lugar, incluso, a distinguir generaciones en períodos más breves de tiempo y en relación directa a la edad del sujeto con la evolución de la informática y las tecnologías digitales al momento de desarrollo de su adolescencia o inicios de su vida adulta.

Es así como en la actualidad se habla de la convivencia de tres generaciones: una "X",[7] otra "Y"[8] y una más, la "Z".[9] Este inusitado avance de la tecnología y el impacto que ella ha generado en la sociedad en pocos años es lo que llevó a que en 2001 Marc Prensky acuñara el término **nativos digitales**

---

(6) Doueihi, Milad, *La gran conversión digital*, (trad. Julia Bucci), Bs. As., FCE, 2010, p. 21.

(7) La generación "X" está integrada por personas nacidas entre finales de los años 60 y la década de los 70, más precisamente entre 1970 y 1981, y que es la generación que desarrolló su adolescencia entre los años 80 y 90, viviendo los primeros pasos e inicios de la era digital y adaptándose a ella.

(8) La generación "Y" está constituida por personas nacidas entre 1982 y 1992, que desarrollaron su adolescencia en la década de los 90 y la primera década del siglo XXI, teniendo una gran familiaridad con los desarrollos tecnológicos tales como las *PC*, *notebook*, *CD*, *CDROM*, video juegos, radios digitales, y los primeros celulares.

(9) La generación "Z", que está comprendida por las personas nacidas entre 1993 y 2004, que viven actualmente su adolescencia, son quienes no han conocido una sociedad sin computadoras de escritorio, *notebook*, *netbook*, teléfonos celulares, *Internet*, correos electrónicos (*e-mails*), mensajes de texto (*sms*), mensajería instantánea (*mms*), micromensajería (*Twitter*), motores de búsqueda como Google o Yahoo, redes sociales (Facebook, Myspace, Sonico, Hi5, Orkut, o Habbo Hotel), blogs, fotologs, etc.

> "para definir a quienes nacieron en un mundo constituido por y alrededor de tecnologías digitales, una tecnología diferente y distante de las que enmarcaron la vida de los adultos de la generación anterior. Para Prensky, esta circunstancia ha generado una brecha entre una y otra generación, los 'nativos' (que nacieron en su entorno) y los 'inmigrantes', adultos para quienes esta tecnología les adviene en sus vidas".(10)

Como puede apreciarse, las tecnologías de la informática y las comunicaciones han impactado contundentemente en nuestro desarrollo como sociedad. Sin embargo, el impacto de estas nuevas tecnologías se extienden incluso más allá, pues han generado grandes cambios a nivel sociológico, filológico, comunicacional, generacional, y también han abarcado otras áreas tales como la medicina, la biónica, la genética, la neurológica, la pedagogía, entre tantas otras. Para el neurocientífico Gary Small y su colaboradora Gigi Vorgan:

> "la actual eclosión de la tecnología digital no solo está cambiando nuestra forma de vivir y comunicarnos, sino que está alterando, rápida y profundamente, nuestro cerebro,(11) (...) seamos nativos o inmigrantes digitales, la alteración de nuestras redes neuronales y conexiones sinápticas mediante actividades como el correo electrónico, los videojuegos, (...) u otras experiencias tecnológicas agudizan, sin duda, ciertas habilidades cognitivas. Podemos aprender a reaccionar más deprisa a los estímulos visuales, y mejorar muchas formas de atención, en particular la capacidad de observar las imágenes de nuestra visión periférica. Desarrollamos una mejor destreza para tamizar rápidamente gran cantidad de información y decidir qué es importante y qué no lo es...".(12)

En definitiva, "la tecnología digital, además de influir en como pensamos, nos está cambiando la forma de sentir y comportarnos, y el modo de funcionar de nuestro cerebro".(13)

---

(10) Balardini, Sergio, "Hacia un entendimiento de la interacción de los adolescentes con los dispositivos de la Web 2.0. El caso de Facebook", en Barindelli y Gregorio (comps.), *Datos personales y libertad de expresión en las redes sociales digitales. Memorándum de Montevideo*, Bs. As., Ad-Hoc, 2010, p. 85.

(11) Small, Gary y Vorgan, Gigi, *El cerebro digital. Cómo las nuevas tecnologías están cambiando nuestra mente*", (trad. Roc Filella Escolá), Barcelona, Urano, 2009, p. 15.

(12) Small y Vorgan, *ibid*., p. 36.

(13) *Ibid.*, p. 16.

Tal es así que estas nuevas tecnologías nos están dotando, como especie, de nuevas capacidades como aprender y reaccionar más deprisa a estímulos visuales y a procesar gran cantidad de información con mayor facilidad.

Sin embargo, también es menester mencionar que han traído nuevas afecciones o enfermedades como consecuencia de la excesiva exposición del usuario, tales como los trastornos de déficit de atención (ADD, *Attention Deficit Disorder*) o el trastorno de déficit de atención con hiperactividad (ADHD, *Attention Déficit Hiperactivity Disorder*).(14)

Además de los datos y estudios que la neurociencia nos reporta que las tecnologías digitales están efectuando en nuestro aparato psíquico, la evolución de la informática y de las TIC ha comenzado a generar grandes cambios en otras áreas del desarrollo humano.

En medicina, la informática y las nuevas tecnologías digitales han influido fuerte y significativamente, en un primer momento a través de la digitalización e informatización del instrumental médico.

Así es como en la actualidad "la empresa 3M vende estetoscopios que digitalizan los sonidos..." y "los cardiodesfibriladores son ahora minúsculos chips que se implantan en el pecho de los pacientes y van 'dictando' vía internet cada dato que recogen".(15)

No obstante, las nuevas tecnologías de la información y comunicación no solo han permitido la digitalización del instrumental médico, sino que han otorgado un nuevo horizonte a la biónica.

La biónica, como rama de la medicina dedicada a la integración de circuitos electrónicos en el cuerpo humano a modo de prótesis e implantes conectados al organismo para restaurar funciones damnificadas, genera grandes expectativas en la actualidad debido al acelerado avance de la informática y en particular a la miniaturización de los componentes electrónicos biocompatibles.

En la actualidad "existe un software que permite mover el cursor de una pantalla solo con el movimiento de la cabeza o de los ojos, depositarlo sobre una letra y transformar lo que 'lee' en frases con sonido. Este sistema

(14) *Ibid.*, pp. 84/85.

(15) Ivoskus, Daniel, *Obsesión digital. Usos y abusos en la red,* Bs. As., Norma, 2010, p. 19.

permite a un usuario imposibilitado físicamente navegar por internet, abrir su casilla de *email* y mandar SMS a celulares".(16)

Aún más sorprendentes son los desarrollos efectuados en investigación por la compañía Cyberkinectics, la cual "ya está efectuando pruebas clínicas de un implante cerebral que permite a pacientes paralíticos el uso de computadoras mediante controles puramente mentales". De esta manera, "un paciente inmovilizado del cuello para abajo pudo manejar objetos a distancia gracias a un microchip instalado en su cerebro...".(17)

Pero además de los avances en medicina y biónica como consecuencia del impacto de la informática y las nuevas tecnologías digitales, más sorprendente resulta la fusión de avances con otras áreas. La informática, teleinformática, telecomunicaciones, genética, biónica, biotecnología, nanomedicina, han dado lugar a que en la actualidad se haya comenzado a investigar la transmisión de información entre organismos vivos y circuito electrónicos.

Esto que parece digno del guión de una película de ciencia ficción o producto de una mente muy imaginativa o creativa resulta factible hoy en día.

Es así como en el presente ha llegado a sugerirse la bioprogramación como mecanismo válido de superación de la pedagogía tradicional como medio de obtención de información. El autor Ray Kurzweil sostiene que

> "el cerebro dejará de tener un límite establecido por la naturaleza (...) Más allá de los implantes de memoria artificial, el científico destaca la posibilidad de introducir datos en el cerebro a través de canales neurales directos. Por lo tanto, sería posible aumentar la capacidad de almacenar información a velocidades inusitadas, dejando obsoletos los arduos métodos de aprendizaje tradicionales".(18)

Como puede apreciarse en este primer apartado, tal ha sido el impacto e influencia de la informática y las tecnologías digitales de la comunicación: la *netiqueta*, el advenimiento de grupos de identidad basados en sitios

(16) Ivoskus, *ibid.*, p. 19.

(17) Sibilia, Paula, *El hombre postorgánico. Cuerpo, subjetividad y tecnologías digitales*, 2ª ed., Bs. As., FCE, 2009, p. 128.

(18) Sibilia, Paula, *ibid.*, p. 123.

blogs o fotologs (*floggers)*, la distinción de generaciones en períodos de tiempo más breves y acotados ("nativos digitales" o "inmigrantes digitales" o generaciones "X", "Y" o "Z"), la adquisición de nuevas capacidades cognitivas como consecuencia de la exposición a estas nuevas tecnologías y el surgimiento de afecciones tales como trastornos de déficit de atención a raíz de una excesiva exposicióna ellas.

También constituyen prueba cabal de su profunda influencia la digitalización del instrumental médico, los avances en biónica mediante la introducción de implantes o prótesis con circuitos electrónicos biocompatibles destinados a restaurar funciones damnificadas o el empleo de la bioprogramación para la transmisión directa de información al cerebro humano a través de la compatibilidad o integración de organismos biológicos con organismos cibernéticos.

Frente a una sociedad cada vez más dependiente de la informática y las tecnologías digitales de la comunicación, la comunidad jurídica argentina se cuestionó hace más de dos décadas el dictado y sanción de una ley que previera la posible comisión de conductas típicas a través del empleo de medios informáticos o dispositivos electrónicos, como así también la protección jurídica de bienes intangibles.

Fue así como hace solo cinco años se produjo la sanción de la ley 26.388 de reforma en materia de criminalidad informática al Código Penal de la Nación, a lo cual se le sumaría la promulgación de las leyes 26.685 y 26.904.

3. Antecedentes nacionales y leyes de reforma en materia de criminalidad informática al Código Penal de la Nación (leyes 26.388, 26.685 y 26.904)

La comunidad jurídica argentina se interrogó tempranamente por el dictado y sanción de una ley que previera la protección de bienes intangibles y la posible comisión de conductas típicas a través del empleo de medios informáticos o tecnologías digitales.

Fue así como desde el año 1996 hasta el año 2008 se presentaron numerosos proyectos de ley destinados a reformar el Código Penal de la Nación mediante una ley integral y concordada para adaptar cada tipo penal a esta nueva modalidad comisiva o bien a través de la sanción de una ley complementaria con idénticas finalidades.

Así podemos mencionar los siguientes proyectos de ley presentados durante el período 1996-2008:

1. Proyecto de Ley de Leonor Esther Tolomeo de 1996;
2. Proyecto de Ley de Carlos "Chacho" Álvarez (1996);
3. Proyecto de Ley José A. Romero Feris (1996);
4. Proyecto de Ley de Antonio Tomás Berhongaray (1997);
5. Proyecto de Ley de Anteproyecto de Ley de 2001;
6. Proyecto de Ley Marta Osorio (1225-D-05);
7. Proyecto de Ley de Silvia Virginia Martínez (1798-D-05);
8. Proyecto de Ley Andrés L. Sotos (985-D-05);
9. Delia Beatriz Bisutti (2032-D-06);
10. Dante Omar Canevarolo (3001-D-06);
11. Diana Conti y Agustín Rossi (2291-D-06);
12. Proyecto de Ley de Reforma y Actualización Integral del Código Penal de la Nación (resoluciones MJyDH 303/2004 y 136/2005) hasta culminar en el Proyecto de Ley (CD-109/06; S-1751-1875 y 4417/06 y expediente 5864-D-2006) que dio origen a la presente ley 26.388.

Este último surgió del tratamiento de un gran número de expedientes legislativos y se presenta como una versión por demás mejorada y refinada de todos los anteriores proyectos de ley desde 1996 hasta 2008.

Finalmente, la ley 26.388 fue sancionada el 04/06/2008, promulgada el 24/06/2008 y publicada en el Boletín Oficial de la República Argentina el 25/06/2008.

La ley 26.388 partió de una ley de reforma integral y concordada al Código Penal de la Nación, basándose en el modelo de Proyecto de Ley de la Diputada, Leonor Esther Tolomeo (1996) y llevó adelante la modificación de tipos penales tradicionales que la doctrina venía debatiendo durante más de dos décadas (1996-2008) y que se hacían presentes en cada uno de los proyectos de ley antes enunciados.

Es así como la ley 26.388 ha alcanzado con su reforma un número muy limitado y específico de tipos penales como lo son:

1. El ofrecimiento y distribución de imágenes relacionadas con pornografía infantil (art. 128 CP),
2. Violación de correspondencia electrónica (art. 153 CP),

3. Acceso ilegítimo a un sistema informático (art. 153 *bis* CP);
4. Publicación abusiva de correspondencia (art. 155 CP);
5. Revelación de secretos (art. 157 CP);
6. Delitos relacionados con la protección de datos personales (art. 157 *bis* CP);
7. Defraudación informática (art. 173, inc. 16 CP);
8. Daño (arts. 183 y 184 CP);
9. Interrupción o entorpecimiento de las comunicaciones (art. 197 CP);
10. El tipo penal de alteración, sustracción, ocultación, destrucción e inutilización de medios de prueba (art. 255 CP), a lo cual debe agregarse las modificaciones terminológicas realizadas en el art. 77 CP.

Es así como contamos con una reforma que ha llevado doce (12) años de elaboración y que ha tomado como sustento otros trece (13) proyectos legislativos, modificando y adaptando tipos penales tradicionales para que puedan ser perpetrados o realizados a través de medios informáticos o dispositivos electrónicos.

Asimismo, debe destacarse que el dictado de la ley 26.388 de reforma al Código Penal de la Nación en materia de criminalidad informática cobra mayor significado y relevancia tras la sanción en el año 2011 de la ley que buscaba la despapelización y la digitalización de la Administración de Justicia; nos referimos más precisamente a la ley 26.685.

El jueves 7 de julio de 2011 se publicó la ley 26.685[19] que otorga a los "expedientes electrónicos, documentos electrónicos, firmas digitales y electrónicas, comunicaciones electrónicas, y domicilios constituidos [la misma] eficacia jurídica y valor probatorio" que en el soporte papel.

Como bien alude Horacio R. Granero, la ley 26.685 es producto del "Plan Estratégico de Modernización de la Justicia que ha encarado la Corte Suprema de Justicia de la Nación que es, sin dudas, una proyección ambiciosa, pero a la vez realista, encaminada a transformar en los próximos años el servicio público de Justicia".[20]

La ley 26.685 que introduce el domicilio electrónico y el expediente digital cuenta con dos (2) artículos de fondo y uno de forma.

---

(19) BO, 07/07/2011.

(20) Granero, Horacio R., "La sanción de la Ley 26.685 de Expedientes Digitales. El principio de equivalencia funcional y la firma digital", [en línea] *elDial.com*, CC2736.

El art. 1 de la ley 26.685 dispone: "Autorízase la utilización de expedientes electrónicos, documentos electrónicos, firmas electrónicas, firmas digitales, comunicaciones electrónicas y domicilios electrónicos constituidos, en todos los procesos judiciales y administrativos que se tramitan ante el Poder Judicial de la Nación, con idéntica eficacia jurídica y valor probatorio que sus equivalentes convencionales".

Mientras que el art. 2 establece que "La Corte Suprema de Justicia de la Nación y el Consejo de la Magistratura de la Nación, de manera conjunta, reglamentarán su utilización y dispondrán su gradual implementación".

Es así como la Corte Suprema de Justicia de la Nación desde la sanción de la ley 26.685, ha profundizado sus esfuerzos a fin de materializar la aplicación del expediente digital y que este no se transforme en una mera declaración de buenas intenciones por parte de la ley.

Pueden destacarse como actos tendientes por parte de la Corte Suprema de Justicia de la Nación, orientados a la concreción y materialización del empleo del expediente digital:

1. La creación de la "Biblioteca Jurídica Digital de la CSJN, Dr. Rodolfo G. Valenzuela", el 31/10/2011.[21]
2. La reglamentación, desde el 13/12/2011, del "Sistema de Notificación Electrónica (SNE)".[22]
3. La puesta en funcionamiento del "Sistema de Notificación Electrónica (SNE)", de aplicación obligatoria desde el 07/05/2012, para la interposición de recursos de queja por denegación de recurso extraordinario federal.[23]
4. El establecimiento, a partir del 01/06/2012, del "Libro de Asistencia de Letrados (Libro de Notas) dentro del programa informático" de seguimiento de causas de la CSJN, que actualmente se realiza de en soporte papel.[24]
5. La extensión de la aplicación obligatoria del Sistema de Notificación Electrónica a todos los fueros y en diversas materias.[25]

(21) CSJN, Acordada 28/2011, [en línea] www.csjn.gov.ar

(22) CSJN, Acordada 31/2011, [en línea] www.csjn.gov.ar.

(23) CSJN, Acordada 3/2012, [en línea] www.csjn.gov.ar.

(24) CSJN, Acordada 8/2012, [en línea] www.csjn.gov.ar.

(25) CSJN, Acordada 29/2012, "Aplicación obligatoria del Sistema de Notificación Electrónica para los Tribunales Provinciales en los que se tramite un Recurso Extraordinario Federal o un Recurso de Queja por Extraordinario denegado". CSJN, Acordada 14/2013, "Se dispone la aplicación obligatoria del Sistema Informático de Gestión Judicial (SGJ) para todos los fueros". CSJN, Acordada 35/2013, "Ampliación del Sistema de Notificación Electrónica a las presentaciones por retardo de justicia y presentaciones varias ante la CSJN".

La Corte Suprema de Justicia de la Nación no ha sido la única que ha dado grandes avances en materia de digitalización del servicio brindado por la administración de justicia, como bien menciona Gisela Candarle, "la Justicia de la Ciudad de Buenos Aires ha dado pasos significativos en la formulación de sistemas de gestión bajo soporte digital".[26]

Además de la sanción de la ley 26.388 de reforma al Código Penal de la Nación en materia de criminalidad informática y de la ley 26.685 de implementación del expediente digital y la notificación electrónica, en el último año se ha realizado una reforma específica y puntual que amplía el catálogo de delitos por medio de la ley 26.904.

Le ley 26.904[27] introduce la figura del *grooming* al Código Penal de la Nación a través de la nueva redacción del art. 131, el cual establece que "será penado con prisión de seis (6) meses a cuatro (4) años el que, por medio de comunicaciones electrónicas, telecomunicaciones o cualquier otra tecnología de transmisión de datos, contactare a una persona menor de edad, con el propósito de cometer cualquier delito contra la integridad sexual de la misma".

Como refiere Hugo Vaninetti, el *grooming* "engloba básicamente la realización de actos preparatorios a través de las modernas tecnologías de la comunicación e información para perpetrar posteriormente delitos contra la integridad sexual. Importaría decir que es una etapa virtual previa al abuso sexual en el mundo real".[28]

Con esta última ley 26.904 tenemos una visión panorámica del marco de la legislativo de la República Argentina en materia de criminalidad informática, conformada así por la ley 26.388 de reforma en materia de criminalidad

---

CSJN, Acordada 36/2013, "Ampliación del Sistema de Notificación Electrónica a las presentaciones efectuadas en causas originarias ante la CSJN". CSJN, Acordada 38/2013, "Ampliación del Sistema de Notificación Electrónica a todos los fueros, implementándose a través de las Cámaras Nacionales y Federales". CSJN, Acordada 43/2013, "Ampliación del SNE a todos los Superiores Tribunales de Provincia y a la Ciudad Autónoma de Buenos Aires", [en línea] www.csjn.gov.ar.

(26) Candarle, Gisela, "Hacia la justicia digital en la Ciudad de Buenos Aires", [en línea] *elDial.com*, DC167D.

(27) BO 11/12/2013.

(28) Vaninetti, Hugo A., "Inclusión del '*grooming*' en el Código Penal", Bs. As., La Ley, 2013, AR/DOC/4628/2013. También sobre *grooming* se sugiere ver Vaninetti, Hugo A., "Media sanción del Senado al proyecto de '*grooming*'", publicado en el Suplemento de Actualidad de la Ley, Bs. As., 26/04/2012. Lo Giudice, María Eugenia, "Con motivo de la sanción de la ley que introduce el 'delito de *grooming*' en el Código Penal (año 2013)", en *elDial.com*, DC1C0B.

informática al Código Penal de la Nación, la ley 26.685 de implementación del expediente digital y la notificación electrónica y la reciente ley 26.904 que incorpora la figura del *grooming* al catálogo de delitos ya preestablecido por la ley 26.388 al Código Penal de la Nación.

Habiendo dejado en claro las disposiciones legales vigentes en materia de criminalidad informática en el sistema legislativo nacional procederemos a verificar qué reformas propone el Anteproyecto de Ley de Reforma, Actualización e Integración al Código Penal de la Nación.

4. La criminalidad informática en el Anteproyecto de Código Penal de la Nación

Desde inicios de la primera década de este siglo XXI, la República Argentina se ha propuesto la recodificación de su legislación penal, buscando la supresión de las leyes complementarias y llevando a cabo un proceso de reforma y actualización integral del Código Penal de la Nación.

Una prueba cabal de ello fue el Anteproyecto de Ley de Reforma y Actualización integral del Código Penal de la Nación de 2006 (MJyDH, resoluciones 303/2004 y 136/2005),[29] elaborado por una Comisión de los más destacados juristas nacionales que había sido convocada por el Ministerio de Justicia y Derechos Humanos bajo la coordinación de la Secretaría de Política Criminal y Asuntos Penitenciarios. Anteproyecto este que no resultó tratado en el Honorable Congreso de la Nación por razones de índole netamente política.

No obstante, a partir del año 2012 fue puesto en marcha un nuevo proceso de recodificación de la legislación penal por medio de la creación de una Comisión para la Elaboración del Anteproyecto de Ley de Reforma, Actualización e Integración del Código Penal de la Nación,[30] conformada por el Sr. Profesor Emérito de la Universidad de Buenos Aires, Dr. Eugenio Raúl Zaffaroni, los diputados Ricardo Gil Lavedra de Unión Cívica Radical y Federico Pinedo de la Alianza Propuesta Republicana y los abogados María Elena Barbagelata del Partido Socialista/Frente de Acción Progresista y León Carlos Arslanián por el Partido Justicialista, lo que exhibe la pluralidad partidaria al momento de conformar la comisión elaboradora y redactora del Proyecto.

(29) Ver Anteproyecto de Ley de Reforma y Actualización Integral del Código Penal de la Nación (MJyDH, resoluciones 303/2004 y 136/2005).

(30) Decreto 678/2012, BO 08/05/2012.

Como bien nos expresa el Sr. Profesor Dr. Daniel Pastor,

> "la reforma iniciada tiene la finalidad explícita de integrar en un solo cuerpo normativo toda la legislación penal hoy dispersa y desarmonizada por una descodificación que ha alterado el equilibrio y la proporcionalidad que deben tener las disposiciones represivas, con lo cual se ha afectado la sistematicidad normativa, aspecto de la legislación penal que no es un adorno intelectual, sino garantía de efectividad de los principios de legalidad y culpabilidad (seguridad y previsibilidad), que son el corazón del derecho penal liberal".[31]

Es así como el jueves 13 de febrero de 2014 la Comisión encargada de la elaboración del Anteproyecto de Reforma presentó al Poder Ejecutivo de la Nación el Anteproyecto de Ley de Reforma, Actualización e Integración del Código Penal de la Nación.

A continuación, analizaremos desde la óptica de la criminalidad informática el Anteproyecto de Ley de Reforma, Actualización e Integración del Código Penal de la Nación, a los fines de relevar y dilucidar qué reformas y actualizaciones propone para los delitos perpetrados mediante el empleo de las nuevas tecnologías y dispositivos digitales.

4.1. Parte general. Terminología y definiciones

El actual Código Penal de la Nación, tras la reforma de la ley 26.388, estableció en el art. 77 la conceptualización de los términos "documento", "firma", "suscripción" e "instrumento privado".

Es así como el art. 77 CP reza:

> "... El término 'documento' comprende toda representación de actos o hechos, con independencia del soporte utilizado para su fijación, almacenamiento, archivo o transmisión.
>
> Los términos 'firma' y 'suscripción' comprenden la firma digital, la creación de una firma digital o firmar digitalmente.
>
> Los términos 'instrumento privado' y 'certificado' comprenden el documento digital firmado digitalmente...".

(31) Pastor, Daniel, "La recodificación penal en marcha. Una iniciativa ideal para la racionalización legislativa", en *Pensar en Derecho*, Bs. As., Eudeba/Facultad de Derecho (UBA), 2012, p. 38.

El Anteproyecto de Ley de Reforma, Actualización e Integración del Código Penal de la Nación, en la Parte General, ha dedicado dentro del Título XIV destinado a la "Significación de conceptos empleados en el Código", un artículo más, específicamente el art. 69, para otorgar las definiciones de: "reglamento", "ordenanzas", "funcionario público", "mercadería", "capitán", "tripulación", "estupefaciente", "establecimiento rural", "violencia", y así también la definición de "firma digital", "documento", etc.

Es así que en en el primer borrador de trabajo, el art. 69 del Proyecto de Ley de Reforma, Actualización e Integración del Código Penal de la Nación, disponía en lo referente a los términos "documento", "firma", "suscripción" e "instrumento privado", lo siguiente:

> "k) Los términos 'firma' y 'suscripción' comprenden la firma digital, la creación de una firma digital o firmar digitalmente. Los términos 'documento', 'instrumento privado' y 'certificado' comprenden al documento digital firmado digitalmente".
>
> l) Se considerará 'documento' a la representación de actos o hechos, con independencia del soporte utilizado para su fijación, almacenamiento o archivo que contenga datos".

Como puede apreciarse a simple vista, la Comisión Redactora del Anteproyecto de Ley de Reforma, Actualización e Integración del Código Penal de la Nación había decidido conservar, pese al orden otorgado, la redacción original de la ley 26.388.

No obstante, en su versión final y definitiva del Anteproyecto del Proyecto de Ley de Reforma, Actualización e Integración del Código Penal de la Nación se dispone la teminología y conceptualización en el art. 63, incs. s) y t), el cual dispone:

> "s) Por 'sistema informático' se entiende todo dispositivo aislado o conjunto de dispositivos interconectados o relacionados entre sí, cuya función, o la de alguno de sus elementos, sea el tratamiento automatizado de datos en ejecución de un programa.
>
> t) 'Dato informático' es toda representación de hechos, información o conceptos expresados de cualquier forma, que se preste a tratamiento informático, incluidos los programas diseñados para que un sistema informático ejecute una función. El término comprende, además, los datos relativos al tráfico, entendiendo como tales todos los relativos a una comunicación realizada por

> medio de un sistema informático, generados por este último en tanto que elemento de la cadena de comunicación, y que indican el origen, el destino, la ruta, la hora, la fecha, el tamaño y la duración de la comunicación o el tipo de servicio subyacente".

Se presenta una versión mejorada respecto a la actual redacción del Código Penal de la Nación y al primer borrador de trabajo utilizado por la Comisión, en relación a la conceptualización y teminología, esta nueva redacción y técnica legislativa resulta ser mucho más adecuada, actualizada y versátil a la dinámica de la materia de la criminalidad informática.

4.2. Parte especial. El tipo penal de ofrecimiento y distribución de imágenes relacionadas con pornografía infantil

El tipo penal de ofrecimiento y distribución de imágenes relacionadas con pornografía infantil se encuentra contemplado en el art. 128 CP, el cual dispone que:

> "Será reprimido con prisión de seis (6) meses a cuatro (4) años el que produjere, financiare, ofreciere, comerciare, publicare, facilitare, divulgare o distribuyere, por cualquier medio, toda representación de un menor de dieciocho (18) años dedicado a actividades sexuales explícitas o toda representación de sus partes genitales con finales predominantemente sexuales, al igual que el que organizare espectáculos en vivo de representaciones sexuales explícitas en que participaren dichos menores.
>
> Será reprimido con prisión de cuatro (4) meses a dos (2) años el que tuviere en su poder representaciones de las descriptas en el párrafo anterior con fines inequívocos de distribución o comercialización.
>
> Será reprimido con prisión de un (1) mes a tres (3) años el que facilitare el acceso a espectáculos pornográficos o suministrare material pornográfico a menores de catorce (14) años".

Por su parte, la Comisión de Reforma, Actualización e Integración del Código Penal de la Nación trabajó sobre un borrador para este tipo penal que establecía que:

> "Será reprimido con prisión de seis (6) meses a tres (3) años, el que produjere o publicare imágenes pornográficas en que se exhibieran menores de dieciocho (18) años, al igual que el que

> organizare espectáculos en vivo con escenas pornográficas en que participaren dichos menores".
>
> En la misma pena incurrirá el que distribuyere imágenes pornográficas cuyas características externas hicieren manifiestas que en ellas se ha grabado o fotografiado la exhibición de menores de dieciocho (18) años de edad al momento de la creación de la imagen".
>
> Será reprimido con prisión de quince (15) días a dos (2) años quien facilitare el acceso a espectáculos pornográficos o suministrare material pornográfico a menores de catorce (14) años".

Como puede apreciarse el primer borrador disminuía el máximo de la pena en un año, pasando de una pena máxima de cuatro (4) años a una máxima de tres (3).

En su redacción puede constatarse que suprimía los ocho verbos típicos empleados por la redacción original ("produjere, financiare, ofreciere, comerciare, publicare, facilitare, divulgare o distribuyere") y los sustituía únicamente por los verbos "producir" y "publicar". Se mantenía en el segundo párrafo la punición de la tenencia de material pornográfico que exhiba a menores de edad, siempre que sea con fines de distribución, dejando como atípico la mera tenencia de material pornográfico, tal como lo previó la ley 26.388.

En lo pertinente al tercer párrafo, también se mantenía el texto original instaurado por la ley 26.388. En su versión final y definitiva, el Anteproyecto optó por la siguiente redacción del tipo penal en su art. 131:

> "1. Será reprimido con prisión de UNO (1) a SEIS (6) años, el que produjere o por cualquier medio publicare, comerciare o divulgare imágenes de actividades sexuales explícitas de menores.
>
> 2. La misma pena se impondrá a quien organizare espectácu-los en vivo con escenas pornográficas en que participaren menores.
>
> 3. Si los delitos de los incisos precedentes se cometiesen contra menores de trece años, la pena de prisión será de TRES (3) a DIEZ (10) años.
>
> 4. El que facilitare el acceso a espectáculos pornográficos o suministrare material pornográfico a menores de trece años, será penado con prisión de UNO (1) a SEIS (6) años".

Como puede apreciarse, en la redacción definitiva realizada por el Anteproyecto respecto a éste tipo penal, se ha mantenido la redacción de la ley 26.388 en gran medida, pero se ha incrementado su escala punitiva.

Su mínimo se ha incrementado en seis (6) meses y su máximo se ha incrementado en dos (2) años, pasando, de seis (6) meses a un (1) año en el caso del mínimo, y para el máximo de los originales cuatro (4) años a seis (6) años de prisión.

Respecto a la facilitación al acceso a espectáculos pornográficos o el suministro de material pornográfico a un menor de trece años, la reforma en su versión final, se ha tornado más represiva.

En primer lugar, ha disminuido la edad del sujeto pasivo de 14 a 13 años, y en segundo orden, ha incrementado la pena en tres (3) años, pasando de un máximo de tres (3) años a un máximo de seis (6) años de prisión.

También ha generado un incremento de la escala original cuando la producción, publicación, comercialización o divulgación de imágenes de menores con actividades sexuales explicitas fueran de un menor de 13 años, incrementando la escala hasta un máximo de 10 años.

Claramente resulta más represivo que el tipo penal vigente cuyo máximo era cuatro (4) años de prisión, y ahora se incrementa en seis (6) años la formula agravada, ascendiendo la escala en seis (6) años más de prisión.

4.3. Los tipos penales de violación de secreto y privacidad

Una de los puntos más relevantes y significativos de la reforma de la ley 26.388 ha sido la ampliación y redefinición del bien jurídico protegido. Dicha ley ha sustituido en el Título V —"Delitos contra la libertad"— el contenido de su Capítulo III de "Violación de Secretos" por "Violación de Secretos y de la Privacidad" en el Libro II del Código Penal de la Nación.

4.3.1. Violación de correspondencia electrónica

Entre los tipos penales que fueron alcanzados por la ley 26.388 encontramos el tipo penal de violación de correspondencia, el cual reza, en su art. 153:

> "Será reprimido con prisión de quince (15) días a seis (6) meses el que abriere o accediere indebidamente a una comunicación electrónica, una carta, un pliego cerrado, un despacho telegráfico, telefónico o de otra naturaleza, que no le esté dirigido; o se apoderare indebidamente de una comunicación electrónica,

> una carta, un pliego, un despacho u otro papel privado, aunque no esté cerrado; o indebidamente suprimiere o desviare de su destino una correspondencia o una comunicación electrónica que no le esté dirigida.
>
> En la misma pena incurrirá el que indebidamente interceptare o captare comunicaciones electrónicas o telecomunicaciones provenientes de cualquier sistema de carácter privado o de acceso restringido.
>
> La pena será de prisión de un (1) mes a un (1) año, si el autor además comunicare a otro o publicare el contenido de la carta, escrito, despacho o comunicación electrónica.
>
> Si el hecho lo cometiere un funcionario público que abusare de sus funciones, sufrirá además, inhabilitación especial por el doble del tiempo de la condena".

El Proyecto de Ley de Reforma, Actualización e Integración del Código Penal de la Nación preveía en el primer borrador de trabajo respecto a este tipo penal que:

> "Será reprimido con prisión de quince (15) días a seis (6) meses o de diez (10) a doscientos (200) días multa, el que abriere indebidamente una carta, un pliego cerrado o un despacho telegráfico, telefónico, mensaje de correo electrónico o de otra naturaleza que no le esté dirigido; o se apoderare indebidamente de una carta, de un pliego, de un mensaje de correo electrónico, de un despacho o de otro papel privado, aunque no esté cerrado; o suprimiere o desviare de su destino una correspondencia o mensaje de correo electrónico que no le esté dirigida.
>
> Se le aplicará prisión de un (1) mes a un (1) año o de diez (10) a trescientos (300) días multa, si el culpable comunicare a otro o publicare el contenido de la carta, escrito, mensaje de correo electrónico o despacho".

En dicho borrador se mantenía, en su primer párrafo, la redacción original del art. 153 CP conforme la ley 26.388. Es así como se consideraban como típicas las conductas de:

1. Apertura o acceso a correspondencia.
2. Apoderamiento de una comunicación electrónica.

3. Supresión y desvío de comunicaciones electrónicas.
4. Interceptación y captación de comunicaciones electrónicas.
5. Comunicación o publicación ilegítima.

No se contempla en esta nueva redacción la agravación de la pena con inhabilitación especial por el doble del tiempo de la pena si la conducta fuera realizada por un funcionario público en la redacción de este artículo.

Por cuestiones de sistematización y ordenamiento concordado del proyecto de reforma, en lugar de incluirlo en el mismo artículo, se lo contemplaba en un artículo por separado que decía que "Cuando en alguno de los artículos de este capítulo hubiese intervenido un funcionario público en desempeño o ejercicio del cargo, se le aplicará además la pena de inhabilitación especial por el doble de tiempo de la condena".

Sin embargo, en su versión final y definitiva, el Anteproyecto de Ley de Reforma, Actualización e Integración del Código Penal de la Nación previó esta figura en el art. 119 con la siguiente redacción:

> "Será reprimido con prisión de SEIS (6) meses a DOS (2) años y multa de DIEZ (10) a CIENTO CINCUENTA (150) días, el que:
>
> a. Abriere o accediere indebidamente una comunicación electrónica, telefónica, una carta, un pliego cerrado, un papel privado, un despacho telegráfico o telefónico o de otra naturaleza, que no le estuviere dirigido.
>
> b. Se apoderare indebidamente de alguno de ellos, aunque no estuviere cerrado.
>
> c. Lo suprimiere o desviare de su destino, cuando no le estuviere dirigido.
>
> d. Interceptare o captare comunicaciones electrónicas o telecomunicaciones provenientes de cualquier sistema de carácter privado o de acceso restringido".

En la redacción final y definitiva del Anteproyecto se mantiene casi textual el texto vigente del art. 153 CP establecido por la ley 26.388.

No obstante debe destacarse el incremento de la escala penal. Respecto al mínimo de la escala pasa de 15 días a seis (6) meses de prisión y en su máximo de seis (6) meses, se eleva a dos (2) años de prisión.

4.3.2. Acceso ilegítimo a un sistema informático

La ley 26.388 contempló la incorporación de la acción de acceso ilegítimo a un sistema informático a través del art. 153 *bis*, el cual reza:

> "Será reprimido con prisión de quince (15) días a seis (6) meses, si no resultare un delito más severamente penado, el que a sabiendas accediere por cualquier medio, sin la debida autorización o excediendo la que posea, a un sistema o dato informático de acceso restringido.
>
> La pena será de un (1) mes a un (1) año de prisión cuando el acceso fuese en perjuicio de un sistema o dato informático de un organismo público estatal o de un proveedor de servicios públicos o de servicios financieros".

El borrador original sobre el que trabajo la Comisión de Reforma disponía, en los arts. 140, 141 y 142, que:

> "Será reprimido con prisión de seis (6) meses a dos (2) años el que, para vulnerar la privacidad de otro, utilice artificios de escucha, transmisión, grabación o reproducción del sonido o imagen" (art. 140, que introducía la figura penal de captaciones de imágenes y sonidos la cual había sido descartada al momento de la sanción de la ley 26.388);
>
> "Se impondrá pena de prisión de seis (6) meses a dos (2) años si se difundieran, revelaran o cedieran a terceros los datos o hechos descubiertos o las imágenes captadas a que se refiere el artículo anterior"(art. 141 del borrador de trabajo, que preveía la difusión o revelación de las imágenes captadas);
>
> "Será reprimido con prisión de seis (6) meses a dos (2) años el que indebidamente interceptare, captare o desviare comunicaciones telefónicas, postales, de telégrafo o facsímil o cualquier otro sistema de envío de objetos o transmisión de imágenes, voces o paquetes de datos, así como cualquier otro tipo de información, archivo, registros y/o documentos privados o de entrada o lectura no autorizada o no accesible al público que no le estuvieren dirigidos.
>
> La pena será de uno (1) a cinco (5) años si el autor fuere funcionario público o integrante de las fuerzas armadas o de seguridad" (este artículo realizaba una ampliación de las conductas

previstas para el acceso ilegítimo a un sistema informático, contemplado también la interceptación, captación y desvío, además del mero acceso ilegítimo a un sistema informático que no sea de índole público).

Sin embargo, en la redacción final y definitiva del Anteproyecto de Ley de Reforma, Actualización e Integración del Código Penal de la Nación, previó contener esta figura en el art. 123 con la siguiente redacción.

"1. Será reprimido con multa de DIEZ (10) a CIEN (100) días, el que a sabiendas accediere por cualquier medio, sin autorización o excediendo la que poseyere, a un sistema o dato informático de acceso restringido.

2. La pena será de SEIS (6) meses a DOS (2) años de prisión cuando el acceso fuere en perjuicio de un sistema o dato informático de un organismo público estatal o de un proveedor de servicios públicos, de salud o financieros. Si el hecho se cometiere con el fin de obtener información sensible a la defensa nacional, el máximo de la pena de prisión se elevará a CUATRO (4) años.

3. Será penado con prisión de SEIS (6) meses a DOS (2) años el que:

a. A sabiendas y violando sistemas de confidencialidad y seguridad de datos, accediere, de cualquier forma, a un banco de datos personales.

b. Proporcionare o revelare a otro información registrada en un archivo o en un banco de datos personales cuyo secreto estuviere obligado a preservar por disposición legal.

c. Insertare o hiciere insertar ilegítimamente datos en un archivo de datos personales.

d. Mediante cualquier ardid o engaño determinare a otro a proveer datos personales, financieros o confidenciales.

e. Tuviere, desarrollare o comerciare artificios técnicos inequívocamente destinados a la indebida obtención de datos personales, financieros o confidenciales.

f. Utilizare la identidad de una persona física o jurídica que no le perteneciere, a través de cualquier medio electrónico, con el propósito de causar perjuicio.

4. Cuando el agente fuere funcionario público sufrirá, además, inhabilitación de UNO (1) a CINCO (5) años".

En la redacción final el Anteproyecto en lugar de mantener la figura de acceso Ilegítimo a un sistema informático en forma disgregada en tres artículos, se decidió unirlos en un único artículo con cuatro puntos.

Asimismo, cuando la acción se desplegara en "perjuicio de un sistema o dato informático de un organismo público estatal o de un proveedor de servicios públicos, de salud o financieros", como modificación se previó un incremento de la pena que supera la escala original prevista por el art. 153 *bis* CP, pasando de un (1) mes a un (1) año de prisión a seis (6) meses y dos (2) años de prisión.

También es dable destacar que en esta versión final, la escala se incrementa aún más, "Si el hecho se cometiere con el fin de obtener información sensible a la defensa nacional", llegando a elevar el máximo de la pena en cuatro años de prisión.

Por último debe resaltarse que la figura definitiva contemplada por el Anteproyecto en este art. 123 posibilita la introducción de una nueva figura punible: en su apartado 3, inciso f, prevé la incorporación de la figura de usurpación de identidad a través de medios electrónicos ya sea que se trate de una persona física o jurídica.

4.3.3. Publicación abusiva de correspondencia

La ley 26.388 contempló en el art. 155 CP la publicación abusiva de correspondencia con la siguiente redacción:

> "Será reprimido con multa de pesos un mil quinientos ($ 1500) a pesos cien mil ($ 100.000), el que hallándose en posesión de una correspondencia, una comunicación electrónica, un pliego cerrado, un despacho telegráfico, telefónico o de otra naturaleza, no destinados a la publicidad, los hiciere publicar indebidamente, si el hecho causare o pudiere causar perjuicios a terceros.
>
> Está exento de responsabilidad penal el que hubiere obrado con el propósito inequívoco de proteger un interés público".

El borrador sobre el que trabajó originalmente la Comisión de Reforma, Actualización e Integración del Código Penal de la Nación, conservaba esta figura típica tal como podrá apreciarse a continuación:

> "Será reprimido con multa de diez (10) a ciento cincuenta (150) días-multa el que, hallándose en posesión de una correspondencia o mensaje de correo electrónico no destinado a la publicidad,

> lo hiciere publicar indebidamente, aunque haya sido dirigida a él, si el hecho causare o pudiere causar perjuicios a terceros".

La principal modificación que puede observarse es la sustitución de la pena de multa por días-multa, como así también el reemplazo de la expresión amplia de "comunicación electrónica", establecida por la ley 26.388, por "mensaje de correo electrónico", lo que podría reducir ampliamente la punición de la conducta.

Afirmamos ello toda vez que la expresión comunicación electrónica abarca: correos electrónicos (*emails*) mensajería instantánea (sms), micromensajería (Twitter), chats (Messenger, Messenger Yahoo, Google Talk, Whatsapp), blogs, fotolog, y redes sociales (Facebook, Myspace, Sonico, Hi5, Orkut, Haboo Hotel, LinkedIn); mientras que la opción de mensajes de correo electrónico resulta mucho más acotada, ya que por conforme el principio de legalidad, es su faz de ley estricta, y quedaría solo acotado a los correos electrónicos, siendo ampliamente debatible si se encuentra incluida la mensajería instantánea, micromensajería, los chats, blogs y redes sociales.

Tampoco contemplaba en esa redacción la exención de responsabilidad penal si la publicación tuviere por objeto proteger el interés público.

Sin embargo, en su versión final y definitiva, el Anteproyecto de Ley de Reforma, Actualización e Integración del Código Penal de la Nación previó esta figura en el art. 121 con la siguiente redacción.

> "1. Será reprimido con prisión de SEIS (6) meses a TRES (3) años, multa de DIEZ (10) a CIENTO CINCUENTA (150) días e inhabilitación de UNO (1) a CUATRO (4) años el que, hallándose en posesión de un instrumento, registro o contenidos a que se refieren los dos artículos precedentes, lo comunicare, publicare o lo hiciere publicar, indebidamente.
>
> 2. La misma pena se impondrá a quien los hiciere publicar, cuando le hubieren sido dirigidos, siempre que no estuvieren destinados a la publicidad, si el hecho causare o pudiere causar perjuicios.
>
> 3. Estará exento de responsabilidad penal quien hubiere obrado con el propósito inequívoco de proteger un interés público actual".

En su versión final y definitiva la redacción del Anteproyecto mantiene la redacción original del art. 155 CP conforme la ley 26.388, modificando únicamente su escala punitiva, pasando de una pena de multa de la $1500 a 100.000, a un mecanismo de pena conjunta que implica, pena de prisión, multa e inhabilitación, consistiendo de SEIS (6) meses a TRES (3) años, multa de DIEZ (10) a CIENTO CINCUENTA (150) días e inhabilitación de UNO (1) a CUATRO (4) años.

4.3.4. Revelación de secretos

La ley 26.388 previó como otro delito contra la violación de secretos y la privacidad, la violación de secretos, en el art. 157, el cual dispone que:

> "Será reprimido con prisión de un (1) mes a dos (2) años e inhabilitación especial de un (1) a cuatro (4) años, el funcionario público que revelare hechos, actuaciones, documentos o datos, que por ley deben ser secretos".

En el primer borrador de trabajo utilizado por la Comisión de Reforma, Actualización e Integración del Código Penal de la Nación, se mantenía la misma redacción modificando únicamente la escala punitiva, como puede chequearse a continuación.

> "Será reprimido con prisión de seis (6) meses a dos (2) años el funcionario público que revelare hechos, actuaciones o documentos que por la ley deben quedar secretos" (art. 145).

No obstante, en su redacción final y definitiva, el Anteproyecto de Ley de Reforma, Actualización e Integración del Código Penal de la Nación, tiene la siguiente descripción típica (art. 122):

> "1. Será reprimido con prisión de SEIS (6) meses a DOS (2) años o multa de DIEZ (10) a CIEN (100) días e inhabilitación por doble tiempo del de la condena, el que teniendo noticias, por razón de su estado, oficio, empleo, profesión o arte, de un secreto cuya divulgación pueda causar daño, lo revelare sin justa causa.
>
> 2. La misma pena se impondrá al funcionario público que revelare hechos, datos, actuaciones o documentos que por ley debieren quedar secretos".

La redacción final y definitiva del Anteproyecto de Reforma y Actualización del Código Penal mantuvo en gran medida la redacción original del art. 157 del CP conforme ley 26.388.

La principal variante que se puede apreciar una vez más en la redacción de este tipo penal se vislumbra en su la escala de la pena.

Se incrementó en cinco (5) meses el mínimo para el caso de la pena de prisión, pasando de ser de un (1) mes a ser de 6 (seis) meses. Asimismo, se impuso una nueva pena, la multa, la que no estaba contemplada en el tipo original, y se elevó la pena de inhabilitación por el doble del tiempo de la condena.

4.3.5. Delitos relacionados con la protección de datos personales

La ley 26.388 procuró también proteger los datos personales contenidos en bases de datos digitalizadas; fue así que se sancionó el art. 157 *bis* CP, el cual dispone que:

> "Será reprimido con la pena de prisión de un (1) mes a dos (2) años el que:
>
> 1. A sabiendas e ilegítimamente, o violando sistemas de confidencialidad y seguridad de datos, accediere, de cualquier forma, a un banco de datos personales;
> 2. Ilegítimamente proporcionare o revelare a otra información registrada en un archivo o en un banco de datos personales cuyo secreto estuviere obligado a preservar por disposición de la ley.
> 3. Ilegítimamente insertare o hiciere insertar datos en un archivo de datos personales.
>
> Cuando el autor sea funcionario público sufrirá, además, pena de inhabilitación especial de un (1) a cuatro (4) años".

El borrador que sirvió de base al trabajo de la Comisión mantenía la misma redacción modificando únicamente la escala punitiva, incrementando el mínimo de la escala penal de un (1) mes a seis (6) meses de pena de prisión, como puede observarse a continuación.

> "Será reprimido con la pena de prisión de seis (6) meses a dos (2) años el que ilegítimamente accediere, de cualquier forma, a un banco de datos personales.
>
> La misma pena se aplicará al que insertare o hiciere insertar datos falsos en un archivo de datos personales o proporcionare a un tercero información falsa contenida en un archivo de datos personales o revelare a otro información registrada en un banco

> de datos personales cuyo secreto estuviere obligado a preservar por disposición de una ley" (art. 146).

En su redacción final y definitiva el Anteproyecto fundió el art. 157 *bis* CP conforme ley 26.388, en el actual tipo penal del art. 123, punto 3, inc. a), b), c), d) y e), fusionando así este tipo penal de "Protección de Datos Personales" (art. 157 *bis*) con el de "Acceso Ilegítimo a un sistema informático" (art.153 *bis*) y con la nueva figura de usurpación de identidad por medios informáticos, y dice:

> "1. Será reprimido con multa de DIEZ (10) a CIEN (100) días, el que a sabiendas accediere por cualquier medio, sin autorización o excediendo la que poseyere, a un sistema o dato informático de acceso restringido.
>
> 2. La pena será de SEIS (6) meses a DOS (2) años de prisión cuando el acceso fuere en perjuicio de un sistema o dato informático de un organismo público estatal o de un proveedor de servicios públicos, de salud o financieros. Si el hecho se cometiere con el fin de obtener información sensible a la defensa nacional, el máximo de la pena de prisión se elevará a CUATRO (4) años.
>
> 3. Será penado con prisión de SEIS (6) meses a DOS (2) años el que:
>
> a. A sabiendas y violando sistemas de confidencialidad y seguridad de datos, accediere, de cualquier forma, a un banco de datos personales.
>
> b. Proporcionare o revelare a otro información registrada en un archivo o en un banco de datos personales cuyo secreto estuviere obligado a preservar por disposición legal.
>
> c. Insertare o hiciere insertar ilegítimamente datos en un archivo de datos personales.
>
> d. Mediante cualquier ardid o engaño determinare a otro a proveer datos personales, financieros o confidenciales.
>
> e. Tuviere, desarrollare o comerciare artificios técnicos inequívocamente destinados a la indebida obtención de datos personales, financieros o confidenciales.
>
> f. Utilizare la identidad de una persona física o jurídica que no le perteneciere, a través de cualquier medio electrónico, con el propósito de causar perjuicio.

4. Cuando el agente fuere funcionario público sufrirá, además, inhabilitación de UNO (1) a CINCO (5) años".

4.3.6. Violación de privacidad o captación de imágenes y sonidos

Se incorpora un nuevo tipo penal no contemplado por el Código Penal de la Nación, conforme la ley 26.388, que es la violación a la privacidad, este tipo penal había sido tratado al momento de la sanción de la ley 26.388 como el tipo penal de Captación de imágenes y sonido, el cual finalmente en el año 2008 no había sido aprobado y en la actualidad se lo incorpora por vía de esta reforma integral.

"1. Será reprimido con prisión de SEIS (6) meses a DOS (2) años y multa de DIEZ a CIENTO CINCUENTA días, el que vulnerare la privacidad de otro, mediante la utilización de artificios técnicos de escucha, transmisión, grabación o reproducción del sonido o imagen, o se hiciere de registros no destinados a la publicidad.

2. El que incurriere en cualquiera de los delitos del presente artículo o del anterior, abusando de su oficio o profesión, o de su condición de funcionario público, será reprimido con prisión de UNO (1) a CUATRO (4) años".

4.4. El tipo penal de defraudación informática

La ley 26.388 incorporó la por demás cuestionada defraudación informática al Código Penal de la Nación, más precisamente por la redacción que se le otorgó al tipo penal que se trascribe a continuación, en el art. 173, inc. 16 CP:

"El que defraudare a otro mediante cualquier técnica de manipulación informática que altere el normal funcionamiento de un sistema informático o la transmisión de datos".

El borrador de trabajo suprimía esta por demás compleja y cuestionada figura de la defraudación informática, dejando subsistente únicamente la figura de la defraudación automatizada prevista en el art. 173, inc. 15 CP.

Finalmente en su versión final y definitiva el Anteproyecto de Ley de Reforma, Actualización e Integración del Código Penal de la Nación, mantuvo la Defraudación Informática con la redacción original de la ley 26.388 en el art. 144, inc. o):

> "El que defraudare a otro mediante cualquier técnica de manipulación informática que altere el normal funcionamiento de un sistema informático o de la transmisión de datos".

4.5. El tipo penal de daño

La reforma de la ley 26.388 introdujo un segundo párrafo al delito de daño, contemplando lo que se conoce como daño a bienes inmateriales o intangibles, el cual dispone en el art. 183, 2° párrafo que:

> "En la misma pena incurrirá el que alterare, destruyere o inutilizare datos, documentos, programas o sistemas informáticos; o vendiere, distribuyere, hiciere circular o introdujere en un sistema informático, cualquier programa destinado a causar daños".

El borrador sobre el que trabajó la Comisión de Reforma mantenía la redacción original de la ley 26.388 y contemplaba el daño a bienes intangibles o inmateriales en el art. 187:

> "Será reprimido con prisión de quince (15) días a un (1) año, el que por cualquier medio, destruya en todo o en parte, borre, altere en forma temporal o permanente, o de cualquier manera impida la utilización de datos o programas contenidos en soportes magnéticos, electrónicos o informáticos de cualquier tipo o durante un proceso de transmisión de datos.
>
> La misma pena se aplicará a quien venda, distribuya, o de cualquier manera haga circular o introduzca en un sistema informático, cualquier programa destinado a causar daños de los prescriptos en el párrafo anterior, en los datos o programas contenidos en una computadora, una base de datos o en cualquier tipo de sistema informático".

Luego de la lectura de ambos artículos puede apreciarse que se seguían empleando los tres verbos típicos "destruir", "alterar" e "inutilizar", aunque agregaba en su nueva redacción el verbo "borrar".

Al igual que la figura original, se penaba en el segundo párrafo la venta, distribución, circulación o introducción de programas destinados a causar daño, tales como virus o códigos maliciosos; y se mantenía atípica la conducta de diseño o creación de programas destinados a causar daños, virus o códigos maliciosos, siempre y cuando ellos no sean puestos en circulación, distribuidos, vendidos o introducidos en un sistema informático.

Finalmente, la versión definitiva del Anteproyecto de Ley de Reforma, Actualización e Integración del Código Penal de la Nación establece como figura de daño el texto previsto en el art. 161:

> "1. Será reprimido con prisión de SEIS (6) meses a UN (1) año o multa de DIEZ (10) a CIEN (100) días, el que destruyere, inutilizare, hiciere desaparecer o de cualquier modo dañare una cosa mueble o inmueble o un animal, total o parcialmente ajenos.
>
> 2. La misma pena se impondrá al que vendiere, distribuyere, hiciere circular o introdujere en un sistema informático, cualquier programa destinado a causar daños.
>
> 3. El máximo de la pena de prisión será de CUATRO (4) años cuando el daño:
>
> a. Fuere ejecutado con violencia en las personas, o se emplearen sustancias venenosas o corrosivas.
>
> b. Fuere ejecutado en cosas de valor científico, artístico, cultural, militar o religioso, o cuando, por el lugar en que se encontraren, se hallaren libradas a la confianza pública o destinadas al servicio o a la utilidad de un número indeterminado de personas.
>
> c. Recayere sobre medios o vías de comunicación o de tránsito, sobre obras hechas en cursos de agua, o sobre instalaciones destinadas al servicio público.
>
> d. Se ejecutare en sistemas informáticos destinados a la prestación de servicios de salud, de comunicaciones, de provisión o transporte de energía, u otros servicios públicos.
>
> e. Se ejecutare en archivos, registros, puentes, caminos u otros bienes de uso público, tumbas, signos o símbolos conmemorativos.
>
> f. Produjere infecciones o contagios en aves o en otros animales domésticos o ganado.
>
> g. Se cometiere sobre yacimientos arqueológicos o paleontológicos, sobre bienes provenientes de éstos, o sobre cualquier otro perteneciente al patrimonio cultural de la Nación.
>
> 4. El máximo de la pena de prisión será de CINCO (5) años cuando el daño:
>
> a. Pusiere en peligro la vida, la integridad física o la salud de una o más personas.
>
> b. Consistiere en la violación o destrucción de tumbas, con o sin esparcimiento de cadáveres, motivada en razones discriminatorias.

> 5. Se impondrá la pena de prisión de SEIS (6) meses a UN (1) año o multa de DIEZ (10) a CIEN (100) días, al que indebidamente realizare u ordenare realizar tareas de prospección, remoción o excavación en yacimientos arqueológicos y paleontológicos, cuando no resultare daño".

Esta versión final suprime el párrafo segundo del actual art. 183, en cuanto refiere a que se considera daño a bienes intangibles descripto a través de datos, documentos, programas y sistemas, como refería en su redacción "En la misma pena incurrirá el que alterare, destruyere o inutilizare datos, documentos, programas o sistemas informáticos".

No obstante, si mantiene como figura típica de venta distribución, puesta en circulación o introducción en un sistema informático, cualquier programa destinado a causar daños.

4.6. El tipo penal de interrupción o entorpecimiento de las comunicaciones

La reforma de la ley 26.388 previó la interrupción o entorpecimiento de las comunicaciones como una de las conductas que podían realizarse a través de medios informáticos o dispositivos digitales. Así fue como la reforma introdujo al texto original de este tipo penal la expresión "comunicación (…) de otra naturaleza", a fin de abarcar las comunicaciones electrónicas en general.

De esta manera, el art. 197 modificado por la ley 26.388 dispone que:

> "Será reprimido con prisión de seis (6) meses a dos (2) años, el que interrumpiere o entorpeciere la comunicación telegráfica, telefónica o de otra naturaleza o resistiere violentamente el restablecimiento de la comunicación interrumpida".

La Comisión de Reforma, Actualización e Integración del Código Penal de la Nación había efectuado una pequeña modificación terminológica a la conducta típica descripta, sustituyendo la expresión "comunicación (…) de otra naturaleza", por "toda comunicación transmitida por cualquier medio alámbrico o inalámbrico", lo cual resultaba más extensivo y preciso.

Sin embargo, la versión final y definitiva del Anteproyecto de Ley de Reforma, Actualización e Integración del Código Penal de la Nación deja redactado, en el art. 190, el tipo penal de interrupción de comunicaciones de la siguiente manera:

> "1. El que, sin crear una situación de peligro común, impidiere o interrumpiere el normal funcionamiento de los transportes por tierra, agua o aire, los servicios públicos de comunicación telefónica, radiofónica, satelital o electrónica, de provisión de agua, de electricidad o de sustancias energéticas, o resistiere con violencia su restablecimiento, será reprimido con prisión de SEIS (6) meses a DOS (2) años.
>
> 2. En caso de impedimento o interrupción de servicios de transporte por tierra, agua o aire, el delito solo se configurará mediante desobediencia a la pertinente intimación judicial".

La redacción definitiva del tipo abandona la descripción original de la conducta típica pero contempla la interrupción "telefónica, radiofónica, satelital o electrónica", sustituyendo así la expresión comunicación (...) de otra naturaleza".

La escala pena no es alterada, manteniéndose la pena de seis (6) meses a dos (2) años de prisión.

4.7. El tipo penal de alteración, sustracción, ocultación, destrucción e inutilización de medios de prueba

La ley 26.388 previó también como tipo penal que pudiera ser realizado por medios informáticos la alteración, sustracción, ocultamiento, destrucción e inutilización de los medios de prueba, en el art. 255 CP:

> "Será reprimido con prisión de un (1) mes a cuatro (4) años, el que sustrajere, alterare, ocultare, destruyere o inutilizare en todo o en parte objetos destinados a servir de prueba ante la autoridad competente, registros o documentos confiados a la custodia de un funcionario público o de otra persona en el interés del servicio público. Si el autor fuere el mismo depositario, sufrirá además inhabilitación especial por doble tiempo.
>
> Si el hecho se cometiere por imprudencia o negligencia del depositario, este será reprimido con multa de pesos setecientos cincuenta ($ 750) a pesos doce mil quinientos ($ 12.500)".

En el primer borrador de trabajo se había mantenido la redacción original de la ley 26.388 alterando únicamente, para el caso de la conducta negligente o culposa, la pena por días multa en el caso de tope máximo de la escala prevista para el delito imprudente, lo que puede verificarse en el texto transcripto a continuación.

> "Será reprimido con prisión de un (1) mes a cuatro (4) años, el que sustrajere, ocultare, destruyere o inutilizare objetos destinados a servir de prueba ante la autoridad competente, registros o documentos confiados a la custodia de un funcionario o de otra persona en el interés del servicio público.
>
> Si el culpable fuere el mismo depositario, sufrirá además inhabilitación especial por el doble del tiempo de la condena.
>
> Si el hecho se cometiere por imprudencia o negligencia del depositario, este será reprimido con multa de sesenta (60) a trescientos sesenta (360) días-multa".

Sin embargo, en su versión final y definitiva, la figura ha quedado contemplada en el art. 260, con la siguiente redacción:

> "1. Será reprimido con prisión de SEIS (6) meses a CUATRO (4) años, el que sustrajere, ocultare, alterare, destruyere o inutilizare objetos destinados a servir de prueba ante la autoridad competente, registros o documentos confiados a la custodia de un funcionario o de otra persona en el interés del servicio público.
>
> 2. Si el culpable fuere el mismo depositario, sufrirá además inhabilitación por el doble de tiempo de la condena.
>
> 3. Si el hecho se cometiere por imprudencia o negligencia del depositario, éste será reprimido con multa de TREINTA (30) a CIENTO OCHENTA (180) días".

En la versión final y definitiva del Anteproyecto se mantiene la redacción original del tipo penal de alteración, sustracción, ocultamiento, destrucción e inutilización de medios de prueba.

Solo se incrementa el mínimo de la pena de un mes a seis (6) meses para el tipo penal doloso. En cuanto al tipo culposo, se estable días multas en lugar una suma pecuniaria.

5. Recomendaciones y sugerencias

Hace tan solo dos años atrás, en junio del año 2011 más precisamente, nos referimos puntualmente a las ventajas y limitaciones político-criminales de la Reforma al Código Penal de la Nación en materia de criminalidad infor-

mática establecida por la ley 26.388.[32] En esta oportunidad es menester profundizar este análisis debido a la incorporación de las recientes leyes 26.685, 26.904 y al actual Anteproyecto de Ley de Reforma, Actualización e Integración del Código Penal de la Nación (decreto 678/2012).

Como expresáramos oportunamente, "la ley 26.388 de ciberdelitos constituye un gran avance legislativo, sobre todo por su ambición de reformar integralmente y actualizar el Código Penal..."[33] y, desde una perspectiva de la técnica legislativa empleada, el legislador ha acudido a la instrumentación de una ley de reforma integral, armónica y concordada al Código Penal de la Nación.

Ella no implicó la creación nuevas figuras delictivas o tipos penales, sino que se modificaron ciertos aspectos de los tipos penales ya contemplados por nuestro ordenamiento jurídico con el objeto de receptar y captar las nuevas tecnologías como medios comisivos para su ejecución, afirmando así que las TIC solo constituyen nuevos medios comisivos para realizar las acciones ya descriptas por los tipos penales previstos por nuestro Código Penal.

Así, con esta reforma se incorporaron los tipos penales de:

1. Ofrecimiento y distribución de imágenes relacionadas con pornografía infantil (art. 128 CP).
2. Violación de correspondencia electrónica (art. 153 CP).
3. Acceso ilegítimo a un sistema informático (art. 153 *bis* CP).
4. Publicación abusiva de correspondencia (art. 155 CP).
5. Revelación de secretos (art. 157 CP).
6. Delitos relacionados con la protección de datos personales (art. 157 *bis* CP).
7. Defraudación informática (art. 173, inc. 16 CP).
8. Daño (arts. 183 y 184 CP).
9. Interrupción o entorpecimiento de las comunicaciones (art. 197 CP).
10. El tipo penal de alteración, sustracción, ocultación, destrucción e inutilización de medios de prueba (art. 255 CP).

Debe destacarse, como menciona Riquert, que "la ley 26.388 ha significado un sustancial avance sobre temas cuya consideración venía siendo re-

(32) Sueiro, Carlos C., "La eficiencia de la reforma en materia de criminalidad informática", ponencia presentada y galardonada con el Segundo lugar en el XI Encuentro de la Asociación Argentina de Profesores de Derecho Penal, Facultad de Derecho de la Universidad Nacional de Rosario, Provincia de Santa Fe, 1°, 2° y 3° de junio de 2011, en *La Ley*, Suplemento de Penal y Procesal Penal, 2011, pp. 11/22.

(33) Reggiani, Carlos, *Delitos Informáticos*, Bs. As., *La Ley*, 2008-D, p. 1090.

clamada desde mucho tiempo atrás, poniendo fin a antiguas discusiones jurisprudenciales y doctrinarias".(34)

Asimismo, la ley 26.388 también ha seguido los lineamientos establecidos por el "Convenio sobre la Ciberdelincuencia de Budapest",(35) incorporando las definiciones terminológicas en el art. 77 CP, teniendo en consideración las definiciones suministradas por el Convenio arriba citado en su art. 1° destinado a "Definiciones", perteneciente al Capítulo I, dedicado a la "Terminología".

Otra ventaja desde una perspectiva criminológica de la ley 26.388 es que no ha recurrido en tal sentido a una clasificación biotipológica o en este caso puntual, cibertipológica de autores. En este sentido, la presente ley 26.388 en ninguno de los tipos penales contemplados ha recurrido al empleo de una biotipología de autores de la criminalidad informática o cibertipología como puede ser las designaciones de: 1) *hacker*; 2) *cracker*; 3) *preaker* o *phreaker*; 4) *phisher*; 5) *sniffer*; 6) *virucker*; 7) propagandista informático, 8) pirata informático, o 9) *cyberbullying* o ciber-acosador.

Asimismo, a nivel dogmático, también debe elogiarse que la mayoría de los tipos penales que han sido modificados son tipos penales dolosos, no presentando el empleo de tipos penales culposos a excepción del tipo penal de alteración, sustracción, ocultación, destrucción e inutilización de medios de prueba (art. 255 CP) y, no habiéndose incorporado ningún tipo omisivo, ni doloso, ni culposo, lo cual debe destacarse en un Estado de derecho, y respetuoso del principio de reserva de los ciudadanos.

No obstante, nuestro actual sistema normativo en materia de criminalidad informática presenta múltiples limitaciones en materia penal, procesal penal, infraestructura y capacitación de la administración de justicia, y cooperación internacional.

5.1. La actualización normativa en materia de criminalidad informática

Nuestro actual sistema normativo en materia de criminalidad informática, si bien presenta todas las ventajas que hemos referido previamente, también exhibe limitaciones y deficiencias en diversas materias.

---

(34) Riquert, Marcelo A., *Delincuencia Informática en Argentina y el Mercosur*, Bs. As., Ediar, 2009, p. 217.

(35) Ver Convenio sobre la Ciberdelincuencia, Budapest, 23/11/2001, [en línea] http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Convention%20and%20protocol/ETS_185_spanish.PDF

5.5.1. Recomendaciones y sugerencias de actualización en materia de derecho penal

En primer lugar, debemos referir que pese a que ley 26.388 constituyó una ley de reforma integral y concordada al Código Penal de la Nación y que implicó la modificación de varios de los tipos penales tradicionales, desgraciadamente esta reforma no abarcó o comprendió todas las figuras delictivas que pueden perpetrarse a través de medios informáticos o dispositivos electrónicos. Se sugiere, sin renunciar a una política criminal reductora del poder punitivo, la incorporación de los siguientes tipos penales.

5.5.1.1. Tipos penales propuestos por otros proyectos de ley previos, no incorporados por las leyes 26.388, 26.904, ni por el Anteproyecto (decreto 678/2012)

a. El tipo penal de hurto (art. 162 CP).[36]

b. El tipo penal de revelación de secretos de Estado y ultraje a los símbolos patrios (art. 222 CP).[37]

c. El tipo de penal de incendios y otros estragos (art. 186 CP).[38]

d. Los tipos penales de falsificación de documento público y privado (art. 292 CP) y uso de documento falso o adulterado (art. 296 CP).[39]

5.5.1.2. Tipos penales previstos en leyes complementarias y no incorporados por las leyes 26.388, 26.904, ni por el Anteproyecto (PEN, decreto 678)

a. El Régimen Penal Tributario (leyes 24.769 y 26.735).

---

(36) Figura esta que había sido propuesta para permitir su perpetración o realización a través de medios informáticos o tecnologías digitales en tres proyectos de ley. En el año 1996 fue objeto de tratamiento de los Proyectos de ley del Diputado Carlos R. Álvarez y del Proyecto del Diputado José A. Romero Feris, este último a su vez presentado también en el año 2000 cuando Romero Feris se desempeñaba como senador bajo el número de expediente 0168-S-2000 ante la Honorable Cámara de Senadores del Congreso de la Nación, sin que el mismo lograra ser aprobado por ambas cámaras del Congreso de la Nación.

(37) El tipo penal que cobra significativa importancia luego del "caso Wikileaks". Véase Iellimo, Marcela, "El caso Wikileaks ¿un planteo de cambio para el orden jurídico internacional?", [en línea] *elDial.com*, DC1522; Domscheit-Berg, Daniel, *Dentro de WikiLeaks. Mi etapa en la web más peligrosa del mundo*, Ana Duque de Vega y Carles Andreu Saburit, Bs. As., Rocaeditorial, 2011; y O´Donnell, Santiago, *ArgenLeaks*, Bs. As., Sudamericana, 2011.

(38) Tipo penal propuesto por el Proyecto de Ley de la Diputada Leonor E. Tolomeo en 1996.

(39) En lugar de dejarlo supeditado a la interpretación extensiva, ambas figuras se encuentran alcanzadas por las modificaciones de terminología previstas en el art. 77 CP. Palazzi, Pablo A., *Los Delitos Informáticos en el Código Penal. Análisis de la ley 26.388*, Bs. As., Abeledo-Perrot, 2009, pp. 35/36.

b. El Régimen Penal Cambiario (leyes 19.359, 22.338, 23.928, 24.144 y decreto 480/1995).

c. El Derecho Penal Aduanero (ley 22.415).[40]

5.5.1.3. La incorporación de nuevos tipos penales

A criterio de autores como Riquert y Palazzi, debieron ser tratadas en forma más exhaustiva por la reforma para decidir su incorporación o exclusión los siguientes tipos penales:

a. La ciberocupación o registro impropio de nombres de dominio.[41]

b. El *spamming* o correo basura o publicidad no solicitada.[42]

c. La captación ilegal y difusión de datos, imágenes y sonidos.[43]

d. La posesión simple de material pornográfico infantil.

e. La responsabilidad de los proveedores.[44]

5.5.2. Recomendaciones y sugerencias de actualización en materia de Derecho Procesal Penal

Otra limitación es que, a la fecha, pese la sanción de las leyes 26.388, 26.685, 26.904 y la presentación del Anteproyecto de Ley de Reforma, Actualización e Integración del Código Penal de la Nación, no se cuenta con una reforma a nivel procesal penal en materia de criminalidad informática.

---

(40) "Sería importante que para evitar los perniciosos efectos de la descodificación, como la falta de coherencia, de armonía y pérdida de proporcionalidad (...) se asumiera la profundización de la técnica de la última reforma (...) al que faltaría incorporar los tipos penales que en leyes especiales han quedado aislados, mejorando así su sistematicidad y orden", en Riquert, Marcelo A., *Delincuencia Informática..., op. cit.*, p. 218.

(41) Riquert, *ibid.*, pp. 202/204.

(42) *Ibid.*, pp. 204/206.

(43) Palazzi, Pablo A., *Los Delitos Informáticos..., op cit.*, pp. 159/166, quien se inclina por su no punición y su amparo a través del derecho civil. También Riquert, Marcelo A., *Delincuencia Informática..., op. cit.*, pp. 206/207, quien considera prudente y acertado postergar su punición hasta que exista un serio debate en torno a esta figura penal.

(44) Tomeo, Fernando, *Responsabilidad penal de los administradores de sitios web. El "caso Taringa!"*, Bs. As., La Ley, 01/06/2011; Granero, Horacio R., "La naturaleza jurídica de la nube *('cloud computing')*", [en línea] *elDial.com*, DC11A9; Velazco San Martín, Cristo, "Aspectos jurisdiccionales de la computación de la nube", [en línea] *elDial.com*, DC1304; Elizalde Marín, Francisco, "La prueba en la *Cloud Computing: Cloud Computing & Service Level Agreements*. El modelo en los Estados Unidos de América y su proyección al ámbito local argentino", [en línea] *elDial.com*, DC15EE; Teijeiro, Nicolás, "La protección constitucional de la intimidad en internet con especial referencia a redes sociales", [en línea] *elDial.com*, DC15EF.

Se sugiere o recomienda la adaptación de nuestra legislación procesal penal a la Sección 2 del "Convenio sobre la Ciberdelincuencia de Budapest" destinada al derecho procesal.[45]

Así, resultaría indispensable que una legislación procesal penal en materia de criminalidad informática prevea:

1. La conservación rápida de datos informáticos almacenados (art. 16 del Convenio).
2. Conservación y revelación parcial rápidas de los datos relativos al tráfico (art. 17 del Convenio).
3. Orden de presentación (art. 18 del Convenio).
4. Registro y confiscación de datos informáticos almacenados (art. 19 del Convenio).
5. Obtención en tiempo real de datos relativos al tráfico (art. 20 del Convenio) e
6. Interceptación de datos relativos al contenido (art. 21 del Convenio).

5.5.3. Recomendaciones y sugerencias para la actualización de la infraestructura tecnológica y capacitación del personal de la administración de justicia

En directa relación con la ausencia de la sanción de una ley procesal penal en materia de criminalidad informática, debemos referir la carencia de órganos especializados dentro del sistema de administración de justicia (Poder Judicial de la Nación,[46] Ministerio Público Fiscal[47] y Ministerio

(45) "La reforma legislativa reviste una importancia central frente a la necesidad de readecuar las normas procesales (...) ante el avance del ciberdelito y la falta de previsión legislativa ante las extendidas formas delictivas (...) La necesidad de reformular las reglas procesales sobre prueba digital se torna imperiosa, ya que si bien el uso de la analogía probatoria está permitida en materia procesal, resulta evidente la inconveniencia de seguir utilizando normas destinadas a otras situaciones (por ejemplo, intervenciones telefónicas) a realidades nuevas y con distintas connotaciones (por ejemplo, intervenciones de cuentas de correo electrónico)". Sáenz, Ricardo y Ruiz, Maximiliano, "Hacia un nuevo modelo de investigación en materia de ciberdelincuencia", [en línea] *elDial.com*.

(46) El Poder Judicial de la Nación, por medio de la CSJN ha realizado profundas actualizaciones en materia de infraestructura tecnológica y capacitación del personal. Lo cierto es que en la actualidad no se cuenta con ningún Juzgado Nacional especializado en materia de criminalidad informática o área destinada específicamente a esta materia. Ver CSJN, *Justicia argentina* online, [en línea] http://www.fam.org.ar/media/img/paginas/Justicia%20Argentina%20On%20Line.pdf.

(47) Desgraciadamente, el Ministerio Público Fiscal se encuentra en una situación análoga a la del Poder Judicial de la Nación, ya que si bien cuenta con un importante número de Unidades Fiscales Temáticas o Unidades Especiales, hasta la fecha no ha creado o destinado

Público de la Defensa)[48] y sus auxiliares (Policía Federal Argentina —PFA—, Gendarmería Nacional Argentina —GNA—, Prefectura Naval Argentina —PNA—, y la Policía de Seguridad Aeroportuaria —PSA—).

Se recomienda y sugiere:

a. La creación de juzgados, fiscalías y defensorías especializadas en materia de criminalidad informática o delitos de alta tecnología.[49]

b. La capacitación del personal para afrontar el gran desafío que implica la digitalización e informatización de la administración de justicia a partir de la sanción de la ley 26.685.

c. Capacitar y concientizar sobre otro nuevo fenómeno no contemplado o previsto por las leyes 26.388, 26.685, 26.904 y por el Anteproyecto de Ley de Reforma, Actualización e Integración del Código Penal de la Nación, que ha surgido de la revolución digital y de la computación de la nube o *cloud computing*.[50]

---

recursos a instaurar una Unidad Fiscal especializada en criminalidad informática. Véase www.mpf.gov.ar.

(48) Idéntica realidad exhibe el Ministerio Público de la Defensa (MPD), quien también posee una gran cantidad de Comisiones y Programas, como así también un importante Departamento de Informática dentro del área de la Dirección General de Administración de la Defensoría General de la Nación, pero hasta el presente no dispone de ninguna comisión o programa especializado en criminalidad informática. Fuente: [en línea] www.mpd.gov.ar.

(49) Como bien refieren el Fiscal General Dr. Ricardo Sáenz y el funcionario Dr. Maximiliano Ruiz al manifestar que "el Ministerio Público Fiscal, como actor y motor principal de las investigaciones [debe] enfrentar esta problemática mediante un lineamiento estratégico político criminal". Es así como proponen trazar "dos puntos de aproximación en materia de investigaciones sobre ciberdelicuencia, a saber: 1) una amplia reforma legislativa a nivel procesal actualizadora de las normas sobre investigación en esta materia, y 2) la creación de una Fiscalía especial integral e interdisciplinaria dedicada a la investigación de los delitos informáticos", ver Sáenz, Ricardo y Ruiz, Maximiliano, "Hacia un nuevo modelo de investigación en materia de ciberdelincuencia", [en línea] *elDial.com*, DC19CB.

(50) Esta tecnología de la "computación de la nube" (*cloud computing)* presenta serios problemas de compatibilidad con la implementación del expediente digital. En primer lugar, porque la computación de la nube o *cloud computing*, "por su naturaleza distribuida [en forma de] nube informática a menudo empaña su ubicación y las medidas de seguridad asociada a los datos (...) Esta situación en particular, choca con los requisitos legales de protección de datos". En el caso puntual de la implementación del expediente digital por parte de la administración de justicia, deberá tenerse en consideración que si se desea hacer uso de la tecnología de la computación de la nube o *cloud computing*, la CSJN deberá pensar en el empleo de una "nube privada" (*private cloud*), ya que el uso de una "nube pública" (*public cloud*) o "nube híbrida" o "multi nube" (*hybrid cloud* o *multi cloud*), traerá aparejado un sin número de riesgos, tales como la pérdida de la privacidad y protección de datos personales, la pérdida del control de la información personal, el desconocimiento de la localización y ubicación de la información, problemas con la transmisión o flujo transfronterizo de datos, destrucción o alteración de datos, divulgación de datos, acceso no autorizado a datos, alto nivel de vulnerabilidad, o posible indisponibilidad de la información por falta de conectividad.

5.5.4. Recomendaciones y sugerencias
para la actualización en materia de cooperación internacional

a. Profundizar el estudio de los problemas en materia de criminalidad informática que trae aparejada para la aplicación espacial de la ley penal, sin adaptar nuestra legislación nacional a la Sección 3 del "Convenio sobre la Ciberdelincuencia de Budapest" destinada a la "Jurisdicción".

b. Contemplar la protección de un bien jurídico colectivo, macrosocial o supraindividual, como por ejemplo la hipotética protección del "ciberespacio público", "medio ambiente digital" o "espacio virtual público".(51)

6. Conclusión

El presente trabajo ha buscado exponer las disposiciones legales vigentes a nivel nacional en materia de criminalidad informática y las actualizaciones y reformas que se han propuesto a través de la presentación el Anteproyecto de Ley de Reforma, Actualización e Integración del Código Penal de la Nación.

Asimismo, hemos apreciado las exigencias y cambios significativos que se han producido en todas nuestras expresiones culturales desde los inicios de la sociedad de la información del siglo XXI y cómo ella plantea nuevos retos al momento de concebir e instrumentar normales legales, infraestructura tecnológica y capacitación eficiente para adecuar nuestra administración de justicia actual a los requerimientos de una sociedad altamente informatizada.

A lo largo del estudio y tras analizar las propuestas de actualización y reforma en materia de criminalidad informática propuestas por el Anteproyecto

(51) Muy probablemente por el hecho de desconocer que el acceso a las nuevas tecnologías de la información y comunicación (TIC) así como a Internet hoy han adquirido el estatus o nivel de derechos humanos gracias a la "Declaración Universal de los Derechos Humanos Emergentes" (DUDHE) elaborada en el "Fórum Universal de las Culturas Barcelona 2004" y aprobada en el "Fórum de las Culturas de Monterrey 2007", como así también por el informe de Naciones Unidas que pone en cabeza de todos los estados el garantizar el acceso a Internet toda vez que constituye un nuevo derecho humano indispensable para la concreción de otros derechos humanos, como la libertad de expresión. Considerar el acceso a *web* y a las nuevas tecnologías digitales como un derecho humano emergente constituye el marco jurídico sobre el cual en unos pocos años podrá sustentarse la construcción de un bien jurídico colectivo, supraindividual y macrosocial como lo puede ser el "ciberespacio público", "medio ambiente digital" o "espacio virtual público", en pos de resguardar todas las actividades sociales que dependen directa o indirectamente del correcto funcionamiento de sus sistemas informáticos públicos interconectados vía Internet y también a través de intranet. Véase Carnevale, Carlos A., "¿El acceso a internet es un Derecho Humano?", [en línea] *elDial.com*, DC1746.

de Ley de Reforma, Actualización e Integración del Código Penal de la Nación, hemos realizados recomendaciones y sugerencias en torno a la actualización de la ley penal, procesal penal, cooperación internacional e infraestructura tecnológica y capacitación del personal de la administración de justicia en materia de criminalidad informática.

Es así como sugerimos entre las reformas a instrumentarse en el área del derecho penal la incorporación de tipos penales tales como:

1. El hurto (art. 162 CP).
2. El tipo pena de revelación de secretos de Estado y ultraje a los símbolos patrios (art. 222 CP).
3. Incendios y otros estragos (art. 186 CP).
4. Los tipos penales de falsificación de documento público y privado (art. 292 CP) y uso de documento falso o adulterado (art. 296 CP).
5. El Régimen Penal Tributario (leyes 24.769 y 26.735).
6. El Régimen Penal Cambiario (leyes 19.359, 22.338, 23.928 y 24.144 y decreto 480/1995).
7. El Derecho Penal Aduanero (ley 22.415).
8. La ciberocupación o registro impropio de nombres de dominio.
9. El *spamming* o correo basura o publicidad no solicitada.
10. La captación ilegal y difusión de datos, imágenes y sonidos.
11. La responsabilidad de los proveedores.

En lo que respecta a las reformas a instrumentarse a nivel de derecho procesal penal, se sugirió la indispensable adaptación de nuestra legislación procesal penal a la Sección 2 del "Convenio sobre la Ciberdelincuencia de Budapest" destinada al "Derecho Procesal".

Acompañándose esta reforma procesal penal con actualización de la infraestructura tecnológica y capacitación del personal de la administración de justicia que impliquen la creación de juzgados, fiscalías y defensorías especializadas en materia de criminalidad informática o delitos de alta tecnología, la capacitación del personal para afrontar el gran desafío que implica la digitalización e informatización de la administración de justicia a partir de la sanción de la ley 26.685, y concientización sobre el nuevo fenómeno la computación de la nube o *cloud computing*.

Finalmente, también se sugirió, en materia de cooperación internacional, profundizar seriamente en el estudio de los problemas en materia de criminalidad informática que trae aparejado para la aplicación espacial de la ley penal, adaptando nuestra legislación nacional a la Sección 3 del "Convenio sobre la Ciberdelincuencia de Budapest" destinada a la jurisdicción; y la contemplación de una posible futura protección de un bien jurídico colectivo, macrosocial o supraindividual, como por ejemplo la hipotética protección del "ciberespacio público", "medio ambiente digital" o "espacio virtual público".

Todo ello en aras de contar con una normativa legal en materia penal, procesal penal y en el área de cooperación internacional acordes a los desafíos que plantea el traspaso a una sociedad altamente tecnificada.

Perspectiva del Derecho Procesal Penal

COLOQUIOS PREPARATORIOS PARA EL XIX CONGRESO INTERNACIONAL DE DERECHO PENAL: "SOCIEDAD DE LA INFORMACIÓN Y DERECHO PENAL" (1)

Sección 3

Documento de reflexión y cuestionario de la AIDP
Relator General: **JOHANNES F. NIJBOER**

Respuestas del Grupo Nacional Argentino:
JAVIER A. DE LUCA, MARCELO RIQUERT, CHRISTIAN C. SUEIRO, MARÍA ÁNGELES RAMOS y **FRANCISCO FIGUEROA**

(A) Objeto del cuestionario

Las preguntas de esta Sección tratan generalmente del "ciberdelito". Este término se entiende en el sentido de dar cobertura a las conductas criminales que afectan a intereses asociados con el uso de la tecnología de la información y comunicación (TIC), como el funcionamiento adecuado de los sistemas de ordenadores y de internet, la intimidad y la integridad de los datos almacenados o transferidos a o a través de las TIC o la identidad virtual de los usuarios de internet. El denominador común y rasgo característico de todas las figuras de ciberdelitos y de la investigación sobre la materia, puede hallarse en su relación con los sistemas, redes y datos de ordenadores, de un lado, y con los sistemas, redes y datos cibernéticos, del otro. El ciberdelito cubre delitos que tienen que ver con los ordenadores en sentido tradicional y también con la nube del ciberespacio y las bases de datos cibernéticas.

Si se precisa cualquier aclaración, por favor, contactar con el Relator General, Prof. Dr. Johannes F. Nijboer, por email: J.F.Nijboer@law.leidenuniv.nl

(B) Cuestiones Generales

(1) ¿Existen definiciones (jurídicas o socio-jurídicas) para la aplicación de las TI y de las TIC en el contexto del procedimiento penal (incluida la práctica forense)? ¿Cómo están reflejadas estas definiciones

(1) AIDP, Río de Janeiro, Brasil, 31 de agosto al 6 de septiembre de 2014.

conceptuales en la doctrina científica, la legislación, las decisiones judiciales y las prácticas pertinentes en el contexto del proceso penal?

Una de las principales dificultades que presenta la legislación argentina es que no se ha llevado a cabo una reforma procesal penal con respecto a la criminalidad informática que se adapte al Convenio de Cibercriminalidad de Budapest.

Se encuentra pendiente la sanción de una ley procesal que regule la obtención, almacenamiento y conservación de prueba digital.

(2) ¿Existen instituciones específicas y/o grupos de trabajo involucrados en la aplicación de las TIC en el sistema penal?

Sí, el Ministerio Público Fiscal tiene creada una comisión.

(3) ¿Existen organizaciones (empresas) privadas (comerciales) que ofrecen servicios relacionados con las TIC en el sistema penal? Si es así, ¿puede dar ejemplos? ¿Qué límites tienen que ser observados?

No.

(C) Información e inteligencia: construyendo posiciones de información (*information positions*) para la aplicación de la ley

La construcción de posiciones de información es parte de la denominada actuación policial basada en la inteligencia. Se puede definir la actuación policial basada en la inteligencia como un marco conceptual de llevar a cabo la actividad policial como un proceso de organización de la información que se permite a las agencias de aplicación de la ley en sus tareas preventivas y represivas.

(1) ¿Qué técnicas relacionadas con las TIC se utilizan para la construcción de posiciones de información por las agencias de aplicación de la ley?

La principal técnica que se está empleando es la geolocalización de equipos celulares, mediante la activación remota de GPS o empleo de detección de antenas utilizadas por el dispositivo.

(2) ¿A qué tipo de bases de datos públicas (por ejemplo, bases de datos de ADN) y privadas (por ejemplo, el Registro de Nombre de Pasajero o los datos financieros como los datos de SWIFT) tienen acceso las agencias de la aplicación de la ley?

Las agencias de aplicación de la ley tienen acceso a las bases de datos de la Administración Federal de Ingresos Públicos (AFIP), de la Administración

Nacional de la Seguridad Social (ANSES), de la Dirección General de Aduanas (DGA), de la Dirección Nacional de Migraciones (DNM) y del Banco Central de la República Argentina (BCRA).

(3) ¿Pueden aplicarse las técnicas consideradas como minería de datos y comparación de datos? Si es así, ¿pueden utilizarse estas técnicas para crear perfiles de posibles autores o grupos de riesgo? Si es así, ¿se han desarrollado herramientas especiales para las agencias de aplicación de la ley?

No se pueden aplicar las técnicas mencionadas.

(4) ¿Pueden utilizarse medidas coercitivas (por ejemplo, la interceptación de las telecomunicaciones) para la construcción de posiciones de información?

Sí, bajo el régimen general reglado en los códigos procesales, mediante autorización judicial fundada.

La interceptación de telecomunicaciones móviles se encuentra prevista.

También existe el acceso a cuentas de correo electrónico, chat, o mensajería instantánea móvil, aunque no se haya implementado.

En particular, la mensajería instantánea móvil instalada en los celulares inteligentes (*Smarthphone*), presenta serias dificultades para su posible investigación por parte de agencias judiciales y policiales debido a que este tipo de mensajería instantánea (*BlackBerry Messenger*, Whatsapp), se encuentra encriptada.

(5) ¿Qué actores privados (por ejemplo, proveedores de internet o empresas de telecomunicaciones) conservan o están obligados a conservar información para las agencias de aplicación de la ley?

Las empresas privadas no se encuentran obligadas por ley a la conservación de información y datos.

(6) ¿Qué actores privados pueden proporcionar o están obligados a proporcionar información a las agencias de aplicación de la ley?

Ante el requerimiento judicial, proporcionan información los proveedores de internet (Speedy, Fibertel), los servidores de correos electrónicos (Hotmail, Yahoo, Gmail), los motores de búsqueda (Google, Yahoo), las Redes Sociales (Facebook, Myspace, Hi5, Orkut, Sonico, etc.).

(7) ¿Existe control judicial de la construcción de posiciones de información?

No existen hasta la fecha organismos especializados en la construcción de información digital.

(D) Las TIC en la investigación penal

(1) ¿Pueden las agencias de aplicación de la ley llevar a cabo intervenciones en tiempo real a) de datos sobre el tráfico, b) sobre el contenido de los datos?

La ley 26.388 tuvo en consideración el Convenio sobre la Ciberdelincuencia de Budapest del 23 de noviembre de 2001. Sin embargo, se limitó a seguir solo sus lineamientos parcialmente. Es decir, nuestra legislación nacional se adaptó únicamente respecto al derecho penal sustantivo, previsto en el Capítulo II —"Medidas que deberán adoptarse a nivel nacional"—, Sección 1 —"Derecho penal sustantivo"—, sin adaptar nuestra legislación a la Sección 2 de este instrumento internacional, dedicada al "Derecho Procesal".

Así que no se adoptaron medidas legislativas que permitan establecer procedimientos penales específicos para la obtención de prueba electrónica de cualquier delito cometido por medio de un sistema informático (art. 14 del Convenio sobre la Ciberdelincuencia de Budapest).

Tampoco se dio cumplimiento a la sanción de una legislación que prevea la "conservación rápida de datos informáticos almacenados", conforme lo requerido por el mencionado convenio en su Sección 2, Título 2.

Por tanto, no existe una legislación nacional que prevea: 1) La conservación rápida de datos informáticos almacenados (art. 16 del Convenio sobre la Ciberdelincuencia de Budapest); 2) la conservación y revelación parcial rápida de los datos relativos al tráfico (art. 17 del Convenio sobre la Ciberdelincuencia de Budapest); 3) El orden de presentación (art. 18 del Convenio sobre la Ciberdelincuencia de Budapest); 4) El registro y confiscación de datos informáticos almacenados (art. 19 del Convenio sobre la Ciberdelincuencia de Budapest); 5) La obtención en tiempo real de datos relativos al tráfico (art. 20 del Convenio sobre la Ciberdelincuencia de Budapest); y 6) La interceptación de datos relativos al contenido (art. 21 del Convenio sobre la Ciberdelincuencia de Budapest).

(2) ¿Pueden las agencias de aplicación de la ley tener acceso/ congelar/ investigar/secuestrar los sistemas de información sobre: a) datos sobre el tráfico, b) el contenido de los datos?

El Poder Judicial de la Nación, por medio de la Corte Suprema de Justicia de la Nación, realizó profundas actualizaciones en materia de infraestructura tecnológica y capacitación del personal,[2] sin embargo en la actualidad no se cuenta con tribunales especializados en materia de criminalidad informática o área destinada específicamente a esta materia.

El Ministerio Público Fiscal (MPF) se encuentra en una situación análoga a la del Poder Judicial de la Nación, ya que si bien cuenta con un importante número de Unidades Fiscales temáticas o Unidades Especiales,[3] hasta la fecha no ha creado o destinado recursos para instaurar una Unidad Fiscal especializada en criminalidad informática, y se debe valer de los cuerpos periciales dependientes del Poder Judicial.

Idéntica realidad exhibe el Ministerio Público de la Defensa (MPD), quien también posee una gran cantidad de Comisiones y Programas,[4] como así también un importante Departamento de Informática dentro del área de la Dirección General de Administración de la Defensoría General de la Nación, pero hasta el presente no se dispone de ninguna comisión o programa especializado en criminalidad informática.

---

(2) Ver CSJN, *Justicia argentina online. La creación de la Agencia de Noticias del Poder Judicial (Argentine Justicie online. The Creation of the News Agency of the Judiciary),* Editorial Altura Impresores, 2010.

(3) Entre sus Unidades Especiales pueden mencionarse: 1) UF AMIA (UFIA); 2) UF de Asistencia en Secuestros Extorsivos y Trata de Personas (UFASE); 3) UF de Investigación de Delitos de Tributarios y Contrabando (UFITCO); 4) UF para la Investigación de Delitos relativos a la Seguridad Social (UFISS); 5) UF para los delitos cometidos en el ámbito del PAMI (UFIPAMI); 6) U.F. para los delitos cometidos en el ámbito del Registro Nacional de Armas (UFIRENAR); 7) U.F. para la Investigación de Delitos contra la Integridad Sexual y Prostitución Infantil; 8) U.F. para la Investigación de delitos contra el Medio Ambiente; 9) UF de Investigación de Lavado de Dinero y Financiamiento del Terrorismo; 10) UF de Coordinación de causas de violación de Derechos Humanos durante el Terrorismo de Estado; 11) UF para la investigación de violencia en Espectáculos Deportivos. Ver [en línea] http://www.mpf.gov.ar/index.asp?page=Organigrama/organigrama.html

(4) La Defensoría General de la Nación cuenta con los siguientes programas y comisiones: 1) Comisión de Cárceles; 2) Comisión de Seguimiento del Tratamiento Institucional de Niñas, Niños y Adolescentes; 3) Comisión para la Asistencia Integral y Protección al Refugiado y Peticionante de Refugio, 4) Comisión de Seguimiento del Tratamiento Institucional de Neuropsiquiátricos; 5) Comisión de Temática de Género; 6) Comisión del Migrante; 7) Programa de Asistencia y Patrocinio Jurídico; 8) Programa para la Aplicación de Tratados Internacionales de Derechos Humanos; 9) Programa de Atención a las Problemáticas Sociales y Relaciones con la Comunidad; 10) Programa Piloto para la Asistencia Jurídica a Mujeres Privadas de la Libertad. Ver [en línea] www.mpd.gov.ar

En cuanto a los auxiliares de la Administración de Justicia como lo son 1) la Policía Federal Argentina (PFA), 2) la Gendarmería Nacional Argentina (GNA), 3) la Prefectura Naval Argentina (PNA), 4) la Policía de Seguridad Aeroportuaria (PSA), solo los dos primeros cuentas con áreas especializadas de investigación.

(3) ¿Se puede obligar a las empresas de telecomunicaciones o proveedores de servicios a compartir los datos con las agencias de aplicación de la ley? En caso de incumplimiento, ¿hay medidas coercitivas o sanciones?

Es una situación compleja, ya que la mayoría de las empresas (Google, *Hotmail*, Yahoo, Facebook, entre otras) son transnacionales por lo tanto es difícil aplicarle medidas coercitivas o sanciones. Además, la mayoría de esas empresas se rigen por sus políticas de privacidad para determinar en qué casos brindar información.

(4) ¿Pueden las agencias de aplicación de la ley realizar videovigilancia? ¿Pueden obligar a las personas físicas o jurídicas a cooperar?

La videovigilancia resulta una herramienta tecnológica permitida en espacios públicos, no así en espacios privados, ni en domicilios. No se encuentra autorizada la escucha acústica de domicilio o el empleo de cámaras térmicas.

Algunas leyes procesales penales provinciales (la Argentina es un país federal, dividido en provincias y cada una tiene su Código Procesal Penal) regulan entre los medios de prueba a las filmaciones de sistemas de monitoreo público o privado y grabaciones de las llamadas a teléfonos del sistema de emergencias.

(5) ¿Pueden o deben aplicar las agencias de aplicación de la ley la grabación audiovisual de los interrogatorios (sospechosos, testigos)?

Pueden realizarse grabaciones de juicios, audiencias orales antes las Cámaras de apelaciones de los distintos fueros.

Hay previsiones específicas, como la filmación y grabación de declaraciones de víctimas menores de edad de abusos sexuales (Cámara Gesell), generalmente usadas como anticipo extraordinario de prueba con videofilmación u otro medio similar de registración del acto.

También para registrar audiencias orales en la etapa de la investigación penal preparatoria y de ejecución de la pena, en la que las resoluciones judiciales son oralizadas.

(E) Las TIC y la prueba (La cadena de etapas: recogida/almacenamiento/retención/producción/presentación/valoración de la prueba electrónica)

(1) ¿Existen reglas sobre la prueba específicas para la información relacionada con las TIC?

Pese a existir modificaciones al Código Procesal Penal de la Nación, no se ha realizado una reforma procesal penal en materia de criminalidad informática. Se necesita orden judicial para los requerimientos e interceptaciones y se equipara el medio a los recaudos que deben tomarse cuando se trata de correspondencia y telecomunicaciones.

(2) ¿Existen reglas sobre la integridad (por ejemplo, manipulación o procesamiento incorrecto) y seguridad (por ejemplo, hacking) de la prueba relativa a las TIC?

Ante la ausencia de ley procesal, no existen reglas de integridad o protocolos para la manipulación de prueba digital. Debe aclararse que, en la Argentina, rige el principio de libertad probatoria, de modo que para dotar a las pruebas de las pautas de seguridad necesarias (no contaminación, no pérdida de las cadenas de seguridad, inalterabilidad, etc.), se recurre a peritos oficiales como a cualquier otra prueba.

(3) ¿Existen reglas sobre la admisibilidad (incluido el principio de legalidad procesal) de las pruebas que son específicas de la información relacionada con las TIC?

No existe ese tipo de reglas.

(4) ¿Existen reglas específicas sobre el descubrimiento y revelación de la prueba relacionada con las TIC?

No existe ese tipo de reglas específicas.

(5) ¿Existen reglas especiales para la valoración (valor probatorio) de la prueba relacionada con las TIC?

No existe ese tipo de reglas específicas.

(F) Las TIC en la etapa de juicio

(1) ¿Cómo puede o debe introducirse en el juicio la prueba relacionada con las TIC?

Deben ser introducidas a pedido de parte y con el control de ellas.

(2) ¿Pueden realizarse interrogatorios a distancia (por ejemplo, conexiones vía satélite)?

Se han implementado los métodos de declaración testimonial a distancia.

(3) ¿Pueden utilizarse técnicas digitales y virtuales para la reconstrucción de los hechos (asesinatos, accidentes de tráfico)?

Sin lugar a dudas, el empleo de mapas satelitales como Google *maps* o Google *Earth*, sistemas de coordenadas, *GPS* y programas y aplicaciones de geolocalización como "*foursquare*".

(4) ¿Pueden utilizarse técnicas audiovisuales para presentar pruebas en el juicio (en su forma más simple: imágenes y sonido)?

Sí.

(5) ¿Pueden sustituirse los expedientes penales en "papel" por otros electrónicos? ¿Se ha avanzado hacia la digitalización de los documentos del juicio?

Hasta la fecha, no; gradualmente se producirá en la República Argentina, a través de la ley 26.685, la transición al expediente digital y la gradual sustitución del expediente en soporte papel.

Un significativo avance por parte del Poder Judicial de la Nación de la República Argentina es la labor encarada por la Corte Suprema de Justicia de la Nación, la que ha digitalizado todas sus sentencias y gran parte de su biblioteca. En igual sentido, ha comenzado con los cursos de capacitación para la implementación gradual de la Acordada 31/2011, tendiente a la constitución de domicilios electrónicos de notificación.

No debe perderse de vista que, en un país con estructura federal en el que los códigos procesales han quedado reservados a las provincias y, además, el Código Procesal Penal de la Nación es de los más antiguos en cuanto a su adscripción a un sistema mixto con rasgos inquisitivos, en el orden local puede haber previsiones más actuales, como las citadas de la provincia de Buenos Aires, donde hoy es común que actos centrales del proceso se documenten mediante registración de audio/video digitales, con una breve acta escrita que complementa el legajo tradicional, dejándose constancia del acto celebrado.

Panel 3

Desafíos procesales en la investigación de delitos informáticos

DANIELA DUPUY[1]

1. Introducción

La Ciudad Autónoma de Buenos Aires organizó un sistema procesal acusatorio —tal como lo establece el art.13, inc. 3 de su Constitución—, que comenzó a regir en la ciudad a partir de la sanción de la ley 2307, promulgada y publicada entre marzo y mayo de 2007.

Las diferencias con el sistema tradicional, en términos generales, consisten en que es el fiscal quien dirige la investigación y participa en ella hasta la finalización del juicio oral, mientras que el juez cumple la función de garante. A su vez, la audiencia oral es la metodología central para incorporar información y adoptar decisiones, cuya calidad dependerá de la información que suministren las partes y la recopilación desformalizada de esta información durante la investigación preparatoria.

Para que un proceso de reforma judicial sea exitoso, es fundamental que el cambio de la ley procesal vaya acompañado de una adaptación del diseño institucional a aquella. Así se hizo en el ámbito del Ministerio Público Fiscal de la CABA. Se rediseñó la organización y gestión de las unidades fiscales; se profundizó la transparencia y la eficacia poniendo el énfasis en la confianza de la comunidad, facilitando su acceso a la justicia y brindando

(1) Fiscal a cargo del Equipo Especializado en Delitos Informáticos de la CABA.

respuestas de calidad, así como también transformando el expediente tradicional en soporte papel en una gestión digital de casos.

En este marco, el 15 de noviembre de 2012, a través de la Resolución 501/2012 FG,[2] se creó, como prueba piloto y por el término de un año, el Equipo Fiscal Especializado en delitos Informáticos de la CABA, que actúa con competencia única en toda la ciudad e investiga los delitos informáticos propiamente dichos —daño informático—, y todas aquellas conductas que se cometan a través de medios informáticos y que, por su complejidad en la investigación y su dificultad en individualizar a los autores, amerite un tratamiento especial, tal es el caso de la pornografía infantil.

Luego de un año de intenso trabajo, la Fiscalía General evaluó la gestión llevada a cabo en ese período de tiempo y, en virtud del aumento de ingreso de casos informáticos y los resultados obtenidos, decidió, a través de la Resolución 444/2013,[3] convertir en definitiva la actuación del Equipo Fiscal para investigar la delincuencia informática de competencia de la justicia local.

La especialización en criminalidad informática surge como una necesidad en las prácticas habituales de las fiscalías al haberse detectado un progresivo aumento en el número de investigaciones criminales y contravencionales vinculadas a la utilización de las nuevas tecnologías, las cuales se incrementarán con la transferencia próxima de delitos de la justicia nacional ordinaria a la justicia de la Ciudad Autónoma de Buenos Aires.

Es una realidad que la generalización de aquellos instrumentos en el desarrollo de las relaciones sociales han determinado la aparición de nuevas formas de criminalidad, posibilitando también dinámicas y mecanismos hasta ahora no conocidos en la comisión de conductas ilícitas de carácter más tradicional. Asimismo, la tecnología informática ofrece hoy importantes herramientas para la investigación de delitos que requieren de especialización y una constante capacitación.

Con la finalidad de dar respuesta a esta situación es que se pensó en la necesidad de crear una Fiscalía Especializada en materia de delincuencia informática, sobre la instrumentalización del principio de unidad de actuación, con el fin de garantizar una intervención eficiente y coordinada del

(2) Véase [en línea] www.fiscalias.gov.ar/resoluciones

(3) Véase [en línea] www.fiscalias.gov.ar/resoluciones

Ministerio Público Fiscal local, de fortalecer el principio constitucional de igualdad de todos los ciudadanos ante la ley y, en definitiva, de afianzar la seguridad jurídica.

Hacerse cargo de investigar este tipo de delitos de manera eficiente no se simplifica en la mera investigación —compleja— de las conductas presumiblemente delictivas. La frecuente naturaleza internacional de la comisión de estos delitos, la facilidad para cometerlos, las dificultades para la obtención y preservación de la evidencia digital, y su volatilidad, implican la necesidad de crear ciertos objetivos para conseguir resultados eficaces en las investigaciones. Algunos de ellos son:

a. Coordinar criterios y estrategias de investigación adecuados con las unidades especiales de las distintas fuerzas de seguridad especializadas —Policía Federal Argentina, Policía Metropolitana, Gendarmería Nacional— y el Cuerpo de Investigaciones Judiciales, así como también establecer vínculos con otros organismos cuya coordinación en determinados aspectos puede ser de vital utilidad para el desarrollo de las investigaciones —Dirección Nacional de Datos Personales, Banco Central, Ministerio de Justicia de la Nación, Jefatura de Gabinete, entre otros—.

b. Elaboración de Protocolos de actuación que faciliten y unifiquen los criterios de actuación en la investigación de los hechos delictivos que requieran para su eficiente investigación de la obtención de evidencia digital, los cuales serán coordinados con la Secretaría de Política Criminal, cuya evaluación apuntará a las necesidades y realidades que impacten en la materia.

c. Promover institucionalmente Convenios de Cooperación con el sector privado a los fines del cumplimiento eficiente de los requerimientos de la justicia de los distintos proveedores de servicio (Google, Microsoft, Mercado Libre, Fibertel, etc.) y las distintas cámaras que los nuclean.

d. Coordinar con el Centro de Formación Judicial el entrenamiento del equipo fiscal asignado en relación con la investigación de los delitos cometidos a través de Internet y la realización de cursos básicos de actuación para todos los integrantes del MP.

e. Generar intercambios de capacitación y cooperación entre las diferentes provincias y la CABA en materia de delincuencia informática, con el objetivo de garantizar una actuación similar y el mantenimiento de criterios similares en la interpretación y aplicación de las normas, y facilitar una adecuada coordinación en aquellas investigaciones en las que la actividad delictiva se desarrolla y/o produce sus efectos en diversos lugares geográficos del país. En igual sentido, intercambiar experiencias entre los fiscales de las diferentes provincias, acerca de procedimientos en curso, análisis y valoración de los problemas jurídicos.

f. Promover la organización y celebración de actividades formativas con países con experiencia en la investigación especializada de criminalidad informática.

g. Elaborar anualmente y presentar ante la Fiscalía General un informe estadístico sobre los procedimientos y casos investigados por la fiscalía especializada en materia de criminalidad informática, tanto en los aspectos cuantitativos como cualitativos.

h. Celebrar acuerdos de cooperación con organizaciones no gubernamentales nacionales y extranjeras, especialmente en lo atinente a la lucha contra la pornografía infantil en Internet.

2. Desafíos para la investigación de delitos informáticos

Considero que existen, al menos, cuatro temas centrales sobre los que se requiere trabajar profundamente, y sobre los que se apoyaron los objetivos propuestos por este equipo fiscal.

En primer lugar, es fundamental **adaptar las normas de fondo** a la utilización de herramientas informáticas para cometer delitos, debiendo reconocer la velocidad de la innovación de las redes.

Desde una perspectiva nacional, la sanción de la ley 26.388 incluyó una serie de delitos informáticos en el Código Penal, actualizando nuestro sistema penal.

Es cierto, o al menos discutible, que algunas de estas modalidades delictivas quizás no requieran de la creación de un tipo penal específico para incriminarlas, y que se pueden subsumir en conductas ya contempladas en nuestro Código Penal.

Sin embargo, debemos tener en cuenta que nuestra ley penal es de la década del 20, y entonces amparaba bienes jurídicos que responden a otra era tecnológica.

Pero si partimos de la base que no existe delito sin ley previa, de acuerdo a lo establecido en el art. 18 CN, y que no es posible la interpretación penal por analogía, la realidad es que hoy, las conductas llevadas a cabo a través de medios tecnológicos, dejan obsoletas muchas normas jurídicas al punto de tener que declarar atípicas conductas que requieren de una protección penal.

Desde el ámbito internacional, hablar de delitos en Internet sin un enfoque de estas características es imposible, toda vez que las redes atraviesan el planeta y no hay fronteras.

Los países más industrializados entendieron que era necesario armonizar sus leyes y establecer medios técnicos y procedimientos de cooperación para combatir los delitos cometidos por Internet.

Esa fue la génesis de la Convención de Budapest —o Convenio de Ciberdelito— y de otros instrumentos internacionales, tales como Protocolo adicional contra la xenofobia en Internet o el Protocolo relativo a la venta de niños, que complementa la Convención de las Naciones Unidas sobre los Derechos del Niño.

Todo ello ha demostrado que la localidad del derecho debía ceder frente a la globalidad de la red, incluso en un ámbito como el derecho penal y procesal, que siempre estuvo tan ligado a la soberanía.[4]

Los Estados miembros del Consejo de Europa y los otros estados firmantes del Convenio de Budapest —redactado en el año 2001— habían tenido experiencia en casos transnacionales y cometidos a través de Internet, y coincidieron en la necesidad de llevar a cabo una política penal común destinada a prevenir la criminalidad mediante Internet a través de una legislación apropiada de cada estado.

Si bien Argentina y el resto de los países de la región no suscribieron inicialmente al Convenio por no ser parte del Consejo de Europa, nada impide que adoptemos sus ideas y sugerencias como forma de mejorar nuestras leyes.

Nuestro país recibió la invitación a participar en las Conferencias anuales sobre ciberdelito en Estrasburgo, Francia.

En segundo lugar, es fundamental **reformar las normas procesales**. No es lo mismo la recolección de la evidencia digital que el secuestro de la prueba física a la que refieren la mayoría de los códigos de procedimiento.

Si bien el uso de la analogía está permitido en materia procesal, resulta necesario reformular ciertas reglas procesales sobre prueba digital para dejar de aplicar a realidades nuevas normas destinadas a otras situaciones, como en el caso de utilizar las reglas sobre intervenciones telefónicas a las intervenciones de cuentas de correo electrónico.[5]

---

(4) Palazzi, Pablo, *Los delitos Informáticos en el Código Penal*, 2ª. edición, Bs. As., Abeledo-Perrot, 2012.

(5) Saenz, Ricardo, "Delincuencia Informática. Necesidad de adecuar normas y prácticas investigativas", [en línea] www.delitosinformáticos.fiscalias.gob.ar

Existe una serie de temas susceptibles de ser discutidos para analizar la posibilidad de introducirlos en los códigos procesales, como la inclusión del agente encubierto, la solicitud de preservación y obtención de datos, la validez de la prueba obtenida en otro país, el registro de cosas físicas versus el registro de datos, la posibilidad de aplicar un software judicial a distancia, cuestiones de competencia, y de utilización de tecnología de cifrado, entre otras.

Muchas de estas cuestiones son abordadas y discutidas cuando analizamos el alcance de investigación de los delitos informáticos, y cada una de ellas, presenta diferentes aristas que requieren ser expresamente tratadas en las leyes de forma.

En tercer lugar, es muy importante **fortalecer los mecanismos de cooperación internacional**.

El carácter transnacional de estas figuras, y en muchos casos su condición de crimen organizado internacional —una red de pedófilos—, tornan imprescindibles los mecanismos de cooperación tanto policial como judicial, para una lucha eficaz contra esta clase de criminalidad.

Cuando el delincuente no se encuentra en el mismo lugar que la víctima, la investigación requiere la cooperación entre las autoridades competentes de todos los países que resulten afectados. El principio de soberanía nacional, si embargo, no permite que un país lleve a cabo investigaciones dentro del territorio de otro país sin el expreso permiso de las autoridades locales. Por lo tanto, las investigaciones deben realizarse con el apoyo de las autoridades de todos los países implicados. En la mayoría de los casos, se dispone de un tiempo breve para que la investigación sea exitosa. Sin embargo, el clásico régimen de asistencia mutua presenta evidentes dificultades cuando se trata de investigaciones de ciberdelitos, pues los procedimientos son muy largos.

En cuarto lugar, es fundamental e**strechar lazos con los proveedores de servicio** de Internet (ISP). Ellos nos suministrarán información vital para la investigación.

El problema es que los ISP no están regidos por reglamentación alguna que los obligue a otorgar esa información al investigador, por lo menos en cuanto al plazo y condiciones de guardado de sus registros.

Sin embargo, y mientras ello ocurra, es conveniente que aquellos sepan qué información necesitamos en cada caso concreto, y el tiempo en que nos hará falta; y los ISP nos notificarán si es posible otorgarnos lo que

solicitamos y, en caso positivo, cómo debemos efectuar dichos requerimientos. Son tratativas y acuerdos que deben efectuarse con cada uno de ellos para que las investigaciones no se dilaten por cuestiones burocráticas.

3. Adaptación de las normas procesales a la Convención de Budapest

La práctica investigativa nos lleva a reflexionar seriamente sobre la necesidad de adaptar las normas de forma a este tipo de delincuencia.

Si bien es cierto que en los códigos procesales rige el principio de libertad probatoria, y la posibilidad de utilizar analógicamente ciertas disposiciones que regulan el registro y allanamientos de lugares físicos, lo cierto es que la adaptación de las reglas procesales penales a la recolección de evidencia digital en el marco de un registro o allanamientos evitaría un abuso del principio de libertad probatoria en beneficio del respeto de las garantías constitucionales, tanto las de derecho interno de cada país que forme parte del convenio como las previstas en normas internacionales.

Si bien las medidas a adoptarse para la obtención y preservación de la evidencia digital es una intromisión del Estado al ámbito de la intimidad de las personas, puede existir una gradualidad desde medidas menos invasivas, como la orden de conservación de datos de tráfico de las comunicaciones, hasta la medida extrema de intervenir las comunicaciones en tiempo real.

Teniendo en cuenta la amenaza que plantea la tecnología, dispusieron que los países miembros del Convenio, al aplicar las medidas procesales, deberán respetar las normas del Convenio Europeo de Derechos Humanos.[6]

El Convenio propone varias medidas procesales, estipuladas entre los arts. 16 a 21 de la Convención de Budapest. Haremos referencia solo a algunas de ellas, y principalmente las vincularé con la necesidad que aquellas se adapten a nuestros códigos procesales a fin de llevar a cabo investigaciones

(6) "Las partes velarán para que la instauración, puesta en funcionamiento y aplicación de los poderes y procedimientos previstos en la presente sección se sometan a las condiciones y garantías dispuestas en su derecho interno, que debe asegurar una protección adecuada de los derechos del hombre y de las libertades y, en particular de los derechos derivados de las obligaciones que haya asumido en aplicación del Convenio para la protección de los derechos humanos y libertades fundamentales del Consejo de Europa (1950) y del Pacto Internacional de derechos Civiles y políticos de Naciones Unidas (1966) o de otros instrumentos internacionales relativos a los derechos del hombre, y que debe integrar el principio de proporcionalidad…" (Convenio Europeo de Derechos Humanos, art. 15).

eficientes, en plazos razonables que posibiliten la recolección de evidencia digital, y respetuosas al máximo de las garantías procesales.

Las medidas serán, seguidamente, analizadas en detalle.

3.1. Conservación inmediata de datos informáticos

En este tipo de investigaciones es ineludible tener que requerir, a los proveedores de servicios de Internet, los datos relativos a los abonados cuyas conexiones estén involucradas en una investigación, pues es la única forma de individualizar a los eventuales autores del hecho.

El investigador forense llegará hasta la dirección de IP del posible infractor.

Se entiende por **datos relativos a los abonados** toda información que posea una proveedora de servicios de Internet en relación a sus abonados: su identidad, la dirección, el número de teléfono, datos relativos a la facturación y al pago, y toda información relativa al lugar donde se encuentran los equipos de comunicación.

Ahora bien, por otra parte, para identificar al infractor que ha cometido un ciberdelito, es fundamental analizar los datos relativos al tráfico.

Los **datos de tráfico** es la información sobre el circuito de una comunicación realizada por medio de un sistema informático que indique el origen, destino, la ruta, la hora, la fecha, el tamaño y la duración de la comunicación.

En esta línea, una de las principales dificultades para los investigadores es que los datos de tráfico se suprimen automáticamente al poco tiempo. Ello se debe a que al final de un proceso (envío de un correo electrónico, acceso a Internet) los datos de tráfico ya no son necesarios y los IPS quieren suprimir la información lo antes posible ya que almacenar los datos por más tiempo exigiría mayor capacidad de almacenamiento y ello sería más oneroso.

En consecuencia el **tiempo** es un parámetro fundamental de las investigaciones por Internet.

Entonces, dada la probabilidad de que transcurra tiempo entre la perpetración del delito, su descubrimiento, y la notificación de las autoridades competentes, es importante aplicar mecanismos que impidan la supresión de los datos durante el proceso de investigación que puede ser largo.[7]

(7) International Telecommunication Union (ITU), "*Understanding Cybercrime: Phenomena, Challenges and Legal Response*", [en línea] http://www.itu.int/ITU-D/cyb/cybersecurity/docs/Cybercrime%20legislation%20EV6.pdf

El art. 16 del Convenio de Budapest, prevé que las autoridades puedan obligar a una empresa proveedora de servicio a impedir la supresión de ciertos datos con el fin de garantizar que la prolongada investigación de un ciberdelito no fracase porque se suprimieron los datos de tráfico.

El problema que existe cuando esta petición no está legislada o reglamentada es que el proveedor no tiene la obligación de responder al requerimiento del fiscal o juez y hasta podría avisar al infractor que lo están investigando.

Entonces, el juez o el fiscal, quien se encuentre a cargo de la investigación, debería poder ordenar la conservación y protección de datos contenidos en un dispositivo de almacenamiento. La orden deberá contener los datos a preservar, y el tiempo de conservación de los mismos será de 90 días.

La conservación de datos se conoce como "*quickfreeze*", método por el que se congelan ciertos datos dispuestos por orden de la autoridad judicial fundado en la necesidad de poder contar con ellos en el transcurso de la investigación.

La obligación de conservar los datos fuerza a la IPS a salvaguardar datos de tráfico durante cierto tiempo, direcciones de IP del emisor y del receptor de la comunicación, o de visitantes de páginas *web*, fecha y hora de la conexión. El claro objeto de conservar es acceder a los datos de tráfico antes que sean borrados.

Ni en el Código Procesal Penal de la Nación, ni en el Código Procesal de la CABA, está contemplada la posibilidad de que el juez o fiscal —según quien dirija la investigación— ordene, fundadamente, la conservación de datos cuando corran peligro de ser eliminados.

Es fundamental que la orden sea precisa para no causar perjuicios a otros usuarios y el secreto de la medida, en especial para el titular de los datos, es imprescindible para el éxito de la investigación.

Hoy, en las investigaciones, estas medidas se solicitan amparados en el principio de libertad probatoria, contemplado en los arts. 93, 106 y 107 de la ley procesal local. Pero al no estar reglamentada la obligación de responder en tiempo y forma por parte de los ISP, muchas veces las respuestas a nuestros requerimientos pueden llegar a destiempo, o no llegar.

Esta disposición solo autoriza a las autoridades competentes a impedir la supresión de los datos pertinentes, pero no obliga a los proveedores a

transferir los datos. La obligación de transferir se contempla en los arts. 17 y 18 del Convenio sobre ciberdelincuencia.

La separación entre la obligación de conservar y la de revelar los datos tiene su fundamento en que, en relación a los datos de conservación, se requiere una reacción inmediata, y en ese caso quizás sea conveniente que en lugar que se emita una orden judicial, sea el fiscal o la policía quienes puedan solicitarlo. La protección de los derechos del sospechoso se puede lograr exigiendo una orden del juez para revelar los datos,[8] y ello se puede lograr con una **orden de presentación** para la revelación de datos.

Es una medida menos gravosa que permite a los jueces ordenar la presentación de elementos relacionados con el delito en lugar de ordenar su secuestro —la Convención de Budapest prevé que "cada parte adoptará las medidas legislativas para facultar a los investigadores a pedir a una empresa proveedora de servicio que comunique los datos que obren en su poder relativo a los abonados"(art. 18)—, y si bien la orden de presentación está prevista tanto en el art. 232 del CPPN como en el art. 113, párr 3 del CPPCABA, lo ideal sería la adecuación de la presentación, por parte de cualquier persona física o jurídica, de datos contenidos en un dispositivo de almacenamiento informático que esté bajo su poder o control y al que pueda acceder.

Ahora bien, uno de los problemas que suelen presentarse en una investigación es que los infractores pueden eludir la obligación de conservación de datos usando servidores de comunicación anónima, por ejemplo, redes públicas como redes inalámbricas en aeropuertos o en cibercafés. En este caso, los fiscales podremos demostrar que el infractor usó un servidor de comunicación anónima pero al no poder acceder a los datos de tráfico, no se podrá demostrar la participación del imputado en el delito.[9]

Ello llevó a pensar en la adopción de medidas adicionales para garantizar la eficacia; por ejemplo, en la obligación de registrarse antes de usar el servicio, o bien el uso de tecnologías anónimas, como ocurre en Italia y en China que restringen el acceso a Internet sin control. Por su parte, entiendo que dicha restricción generaría una clara violación a la libertad de expresión,

(8) Sáenz, Ricardo, "Delincuencia Informática", *op. cit.*

(9) International Telecommunication Union (ITU), *El Ciberdelito. Guía para los países en desarrollo*, [en línea] http://www.itu.int/dms_pub/itu-d/oth/01/0B/D010B0000073301PDFS.pdf

en razón de que ciertas personas prefieren expresar sus ideas u opiniones a través de las redes sociales en forma anónima, o bien utilizando un seudónimo, y dicha medida obligaría a una correcta registración e individualización del usuario y ello desalentaría la libertad de muchos de expresarse.

También, si el sospechoso utiliza un servicio de comunicación anónima como el software TOR, será muy difícil analizar los datos de tráfico e identificar a los participantes.

A fin de garantizar que el ISP no informe a su cliente sobre la investigación en curso, la Convención obliga a los estados a adoptar legislaciones que garanticen que los proveedores de servicios de Internet garanticen la confidencialidad de la información.

3.2. Registro

El registro, allanamiento y secuestro sigue siendo una de las medidas de investigación más importantes. Es la medida que se adopta inmediatamente después de determinar donde está ubicada la IP y a quién pertenece, destinada a secuestrar los equipos informáticos para que los peritos especializados los analicen y reúnan así pruebas para llevar al juicio oral.

El problema que se presenta es que, si bien la mayoría de las legislaciones procesales prevén el registro y secuestro, lo cierto es que la mayoría de ellas se refieren a **cosas físicas** y no a **datos**.

En esta línea, los investigadores podrían secuestrar un servidor entero pero no copiar los datos de ese servidor, lo cual plantea dificultades cuando la información está almacenada en un servidor junto con los datos de miles de usuarios, los cuales ya no estarían disponibles luego del secuestro del servidor.

Así, tanto el art. 224 CPPN como el art.108 del CPPCABA se refieren al registro de los lugares en los que pueda presumirse la existencia de cosas vinculados a la investigación de un delito; aunque el art. 113 última parte del CPPCABA determina que, cuando el secuestro fuere de equipos de computación u otro soporte informático, deberá guardarse reserva de su contenido con igual alcance que el previsto para la interceptación de correspondencia y comunicaciones.

En esta línea, y siguiendo los lineamientos del art. 19 de la Convención de Budapest, sería conveniente una reforma de los códigos procesales que prevea clara y expresamente, "el registro o, el acceso de un modo similar,

a todo sistema informático, o parte del mismo, a los datos informáticos en él almacenados, y a todo dispositivo de almacenamiento informático que permita guardar datos informáticos".

Otro problema que presenta el registro y secuestro en las investigaciones de ciberdelitos es que todas las órdenes judiciales suelen estar dirigidas a lugares determinados, por ejemplo, al hogar del sospechoso. Lo que puede ocurrir es que, cuando se registran los datos informáticos, el resultado es que el sospechoso no almacenó la información en discos duros locales, sino en un servidor externo al cual accedió por Internet. Es común que los usuarios almacenen y procesen datos en la **nube**. Este tipo de almacenamiento tiene la ventaja de poder acceder fácilmente a la información desde cualquier lugar con una conexión de Internet.

Entonces, para garantizar la eficacia de las investigaciones, es importante que las órdenes de registro tengan cierta flexibilidad, de manera que si los fiscales descubren que la información necesaria para el éxito de la investigación está almacenada en otro sistema informático, se debe poder extender el registro a ese sistema.

Lo ideal sería una reforma que habilite extender rápidamente el registro o el acceso a otro sistema cuando hubiere motivos para creer que los datos buscados se encuentran almacenados en otro sistema informático.

Otro problema es que los investigadores pueden tener dificultades para ubicar datos que están almacenados en un sistema informático en el extranjero. Aun cuando se conoce su ubicación exacta, el volumen de los datos almacenados suelen obstaculizar las investigaciones, pues al adquirir una dimensión internacional, exige una cooperación internacional.

3.3. Importancia de la evidencia digital recolectada

Es de vital importancia las etapas que deben respetarse para obtener la evidencia digital:

1. Adquisición: recolección efectiva del objeto (discos rígidos, memorias, teléfonos, celulares, dispositivos móviles). Debe ser la información correcta. Se extreman los recaudos para no contaminar la evidencia y no afectar el objeto secuestrado, de lo contrario será evidencia inadmisible.
2. Preservación: conservación del objeto. Garantiza que lo que se recolecta es lo mismo que utilizaremos en la investigación. Se lo conserva sacando una huella de la configuración actual (*hash*).

3. Obtención: análisis y búsqueda.
4. Presentación: informe de resultados.
5. Juicio: se incorpora a través del informe técnico y el testimonio del experto que intervino en su confección.

Es fundamental que en estas etapas intervengan peritos o técnicos expertos a fin de garantizar la cadena de custodia. Es el registro minucioso del movimiento de la evidencia durante el proceso probatorio que indica con exactitud las actividades realizadas, las personas responsables. Se inicia cuando se comienza a recolectar la prueba. En Argentina, el único Código Procesal que la contempla es el de Chubut en su art. 267.

3.4. Software a distancia

Algunos países europeos y EEUU planean sustituir el registro y el secuestro por la utilización de un software para acceder a la computadora del sospechoso.

La regla general para buscar pruebas en el ordenador de un sospechoso es acceder físicamente al equipo en cuestión, lo que obliga a allanar su casa; y si está enterado sobre la investigación en curso, podría cambiar su comportamiento.

Para evitarlo, se discute hoy la posibilidad de usar una herramienta que permita a las autoridades competentes acceder a datos informáticos almacenados en la computadora del imputado a distancia y buscar la información necesaria.

Consiste en la utilización de programas informáticos capaces de interceptar en tiempo real y grabar datos transmitidos o recibidos a través de diferentes medios de comunicación electrónica. Estos programas permiten también obtener datos de archivos almacenados en la memoria de los equipos informáticos investigados.

¿Qué implicancia tiene para el proceso penal el hecho de que la tecnología permita realizar búsqueda de datos en la computadora de un sospechoso sin necesidad de acceder físicamente al hardware donde están alojados?

¿La prueba obtenida en el marco de una investigación penal, con alguna de estas herramientas, sería admisible en un juicio penal con las normas procesales vigentes? y, en caso contrario, ¿es posible regular

legislativamente este medio de prueba que brinda la tecnología sin afectar garantías constitucionales?[10]

Esta posibilidad que hoy ya representa herramientas utilizadas en otros países para investigaciones cometidas a través de Internet, abre canales de profunda discusión para analizar si el uso del software a distancia representa un abuso al principio de libertad probatoria, o bien si la validez de los datos obtenidos a través su utilización depende de su incorporación expresa en las normas procesales.

4. Conclusión

Hoy es indiscutible la necesidad de adaptar los códigos procesales específicamente al desafío que implica las investigaciones de delitos que se cometen a través de Internet.

Ajustar las normas de forma, teniendo como principio rector a la Convención de Budapest, implicaría limitar el principio de libertad probatoria a lo que expresamente determina la ley para la necesidad de cada caso concreto, a favor de reafirmar el profundo respeto a las garantías constitucionales en el marco de una investigación penal.

(10) Salt, Marcos, "Registro y secuestro de datos realizados a distancia. La utilización de software especial de acceso remoto a datos", capítulo de su tesis doctoral (en preparación).

Panóptico sin fronteras

LUIS MARÍA BUNGE CAMPOS[1]

Gracias. Bueno, quiero saludar y agradecer la invitación y no puedo dejar de mencionar la satisfacción que tengo de ver algunas caras que hace tiempo no veía. Carlos, Daniel y, fundamentalmente, decir que todos estamos acá en gran medida debido al enorme esfuerzo que hizo, a lo largo de muchos años, un señor que está sentado ahí que es el doctor "Tute" Baigún. Estamos aquí porque la AIDP Argentina es, en gran medida, hija de él y quería saludarlo por ello.

Yo voy a dar una visión un poco, tal vez, discordante. Puse un título, que es el de "panóptico sin fronteras", y estoy tomando unos hechos que están sucediendo en los últimos tiempos y que me preocupan mucho.

A fines de enero se reunió en Davos el Foro Económico Mundial, el cual, ustedes saben, es probablemente el foro económico más importante a nivel mundial, donde se reúnen las personas que toman las decisiones más grandes. Allí, el día treinta y uno de enero se hizo una mesa redonda llamada "El problema del 'Gran Hermano'", tratando el tema de la privacidad en Internet. Así arranca el Foro de Davos, nada menos. En esta charla, el Secretario General de Amnesty International, Salil Shetty, dijo simplemente esto: "el problema de los derechos humanos hoy es el derecho a la privacidad. En la década del 70, y también en la década del 80, lo eran los derechos civiles, los derechos de la mujer, pero hoy es el derecho a la privacidad". Lo planteó simplemente así. En este sentido, estimo que es un buen comienzo para

(1) Juez de la Cámara Nacional de Apelaciones en lo Criminal y Correccional. Profesor Adjunto de Derecho Penal (UBA). Profesor de la Carrera de Especialización en Derecho Penal (UBA). Profesor Titular de Derecho Penal, parte especial de la Universidad de Belgrano. Profesor de la Escuela Judicial de la Nación. Miembro de la Comisión Iberoamericana de Ética Judicial.

empezar a pensar en los problemas que tenemos en materia procesal. Y Salil Shetty dijo una frase que, en la Argentina es muy desagradable: "… y no me vengan con eso de que quien no tiene nada que ocultar, no tiene nada que temer". Esa fue la respuesta que dio. No nos vengan con eso, porque nos hace a acordar mucho al "algo habrán hecho". No empecemos por ahí.

El 24 de febrero recibí un mail de la empresa Dropbox, y ese mail que muchos recibieron, ya que lo recibimos todos los usuarios, dice más o menos así: "hola Luis, deseamos comunicarle algunas de las próximas actualizaciones de nuestras condiciones de servicio y de nuestra política de privacidad", y sobre ese rubro, dicen "agregamos un apartado en el de la política de privacidad en el que se describen nuestros recientes principios para solicitudes de datos del gobierno". Al día siguiente, en el periódico *La Nación*, pudimos leer que la Agencia Británica de Espionaje grabó imágenes privadas de cámaras web de un millón ochocientos mil usuarios de Yahoo para someterlas a un programa de reconocimiento facial.

Bueno, por eso quiero hablarles de esto que es un panóptico ya sin fronteras, directamente. Estamos siendo objeto de una vigilancia que no tiene comparación con ningún momento de la historia de la humanidad. El nivel de vigilancia al que estamos siendo sometidos no se compara con nada. Y, lamentablemente, los datos son terribles.

Les hago una pregunta. Mencioné tres datos recientes: uno, del 31 de enero; otro, del 24 de febrero; y, por fin, la noticia publicada en el periódico *La Nación*, que fue para esos días de febrero también. ¿De cuántos derechos fundamentales estamos hablando tanto? Si esas tres noticias se hubieran vinculado con la inviolabilidad del domicilio estaríamos realmente escandalizados. Es decir, ¿cuántos derechos fundamentales hay en la Constitución, y de cuántos hablamos? Pero la otra pregunta que tenemos que hacernos es —y yo no voy a entrar en la discusión de intimidad-privacidad, la cual me parece una discusión totalmente estéril, para mis 15 minutos, por lo menos—: cómo la devaluamos nosotros mismos. Debemos ver quién la devalúa primero.

Somos los primeros responsables en perder nuestra privacidad. La exposición de la misma a través de las redes sociales es un mensaje claro de que estamos diciendo: "¡no nos interesa!". Si nosotros no la cuidamos, por qué se la va a resguardar, o por qué vamos a pedirle al derecho que la proteja. No estamos dispuestos a hacer absolutamente nada para cuidarla. La intimidad es cosa del pasado. Ya nadie va a tener un diario íntimo bajo llave. Actualmente, se expone la intimidad en Facebook y otras redes y se ponen

las fotos de las vacaciones. Respecto de ello es importante el plural, ya que una foto es una imagen, pero diez fotos constituyen una historia. Diez fotos, es un cuento, una narración. Entonces, la primera reflexión que tenemos es que el primer adversario de un sistema de protección de datos es el mismo usuario. Somos nosotros mismos. El riesgo que se corre, ¿cuál es? Es que el Estado comience a protegernos, y entonces ahí caeríamos en otra posibilidad, en otro gran riesgo: sería decir que todo usuario de redes sociales es un menor de edad y que lo vamos a tratar como si fuese un menor de edad. Esa es una de las políticas que hay en materia de protección de datos.

No sé si se sabe, pero el 28 de enero es el día europeo de protección de datos. Eso lo estableció el Consejo de Europa el año pasado, fundamentalmente para promover, justamente en los menores de edad, que los ciudadanos les hablen, como nos hablaban en el colegio el día de la escarapela, de lo importante que es la protección de datos. Continuando con este orden de ideas, analicemos el consentimiento, ese que se brinda cada vez que uno se pone en Facebook, en Twitter, etc., que uno acepta los términos de ese servicio. El consentimiento para ser tal tiene que ser espontáneo, libre e informado. Ahora bien, Dropbox me acaba de informar que modificaron las condiciones del servicio para conmigo, pero no me dicen "señor venga a aceptar las nuevas". Me advierten y, si quiero, puedo dar de baja el servicio o seguir en las condiciones que se me imponen. Como sucede con todo contrato de adhesión.

Entonces, ¿cuáles son las manifestaciones de este derecho de privacidad que tengo en Internet? Lo primero que tengo es la protección de mis datos personales. Traje algunos datos. La primera pregunta es: ¿dónde están mis datos personales? ¿En qué lugar físico están? ¿Qué juez tiene competencia para solicitar mis datos personales? Hay países que están haciendo gran defensa de esto y están colocando los servidores y estableciendo normas en las que, por ejemplo, los ciudadanos de la Unión Europea y los servidores que tienen datos personales de estos ciudadanos deben estar ubicados en el territorio europeo. Hoy estamos viendo una migración de servidores a Canadá, con la excusa del frío, ya que el calor es un gran enemigo de los datos. Con esta excusa se escapan de la *Patriot Act* y se van a Canadá. Brasil está instalando un cable submarino directo a Londres, ya que no quiere pasar por los Estados Unidos. Y ya veremos por qué. La segunda cuestión es la protección de la privacidad interna de mis comunicaciones. Este sí es el dato. Y la tercera es mi derecho a navegar anónimamente en la red. El derecho que tengo yo a que nadie sepa si miré una vidriera, si entré a un

negocio y pregunté el precio de un producto, si lo compré o no lo compré, si leo tal o cual revista, si me interesa la política internacional o los deportes, etc., porque si eso pasara en la puerta de mi casa yo me sentiría muy molesto. Creo que ese es un derecho básico que tengo.

Yo traje acá los datos de una empresa nada más, que es Google. Los datos del semestre que va de enero a junio del 2013. Y es interesante. En los datos aparecen los distintos requerimientos de información que hicieron diversos países, cuántos hicieron, sobre cuántas cuentas o usuarios —ya que un usuario puede tener una cuenta o puede tener muchas cuentas— fueron realizados. También aparecen cuántos fueron respondidos afirmativamente. La información no aclara qué autoridad nacional pidió los datos; si fue un juez, un fiscal, una agencia de seguridad, pero la base de discusión común es que, obviamente, se trata de requerimientos que reúnen los requisitos legales. Así, Alemania hizo 2311 sobre 3079 cuentas y respondió el 48%. Argentina hizo 114 sobre 132 cuentas y respondió el 48%. Sobre Australia, respondió el 64%, sobre Bélgica, el 66%, mientras que en el caso de Canadá cayó al 27% y en el caso de Chile, el 51%; estos porcentajes parecen bastante similares. Por otro lado, en el caso de los Estados Unidos, el porcentaje fue de 83%, en Rusia de 0%, Turquía también 0% y en Hungría, 0%. Puede ser que estén mal hechos los requerimientos o, simplemente, que no estén cubiertos los requisitos legales. Puede ser, también, que no haya convenio de reciprocidad. Pero el dato puro y duro es ese, sobre un total de 258.039, se ha afectado 42.500 cuentas.

Estos no son problemas técnicos, son problemas jurídicos. Yo puedo, técnicamente, navegar de forma anónima. Todos sabemos que en Google Chrome podemos abrir la pestaña incógnita que se limita a no guardar datos en nuestra computadora, aunque siempre nuestro paso por tal o cual página dejará sus rastros. Pero yo no quiero hacerlo técnicamente; yo quiero que el derecho me proteja acerca de esa posibilidad. Tener una esfera de privacidad jurídicamente protegida es un derecho básico y elemental de todos nosotros.

¿Qué pasa con los metadatos? Cuando Snowden hizo el escándalo que hizo, la presidenta del Comité de Inteligencia del Senado dijo que no era tan grave, ya que eran metadatos. Los metadatos son tan invasivos como los datos. ¿Cuál es la diferencia? El metadato es la información del dato. Sacamos una foto con la cámara, la imagen en sí es el dato. El metadato es el día que la sacamos, la geolocalización donde la sacamos, la hora, la forma en la que la sacamos, la abertura del diafragma, la velocidad del

obturador. Ahora bien, nosotros tenemos una norma, que es el art. 236 de la Segunda Parte del Código Procesal Penal de la Nación, que dice que el juez podrá ordenar la obtención de los registros que hubiere de las comunicaciones del imputado o de quienes se comunicaren con él. Y esto es para mí un metadato. En consecuencia, para mí, todo metadato está dentro de la órbita de la protección de los papeles privados y de la correspondencia epistolar y solo puede obtenerse, en nuestro medio, por orden judicial.

No obstante ello, advertimos que el secuestro de computadoras no se rige por las mismas normas que el secuestro de correspondencia. Las previsiones de los arts. 234 y 235 del Código Procesal Penal ya son anacrónicas. ¿Qué es lo que recibimos por carta y en sobre cerrado? En mi caso, creo que solo algunas facturas de servicios. De modo tal que para leer mi diario íntimo en mi notebook hay menos restricciones que para leer la factura del gas que llega en un sobre cerrado al buzón de mi casa. El juez la tiene que abrir en presencia del secretario, ver si tiene interés para la causa, etc. Para revisar los archivos de una computadora ninguna norma obliga al juez a abrirlos en presencia de un secretario y ver si tiene interés para la causa o no. No son papeles privados, mis archivos. El consejo de un abogado, entonces, debería ser que hay que imprimir todo y borrar los archivos para que pasen a ser "papeles privados", lo que es simplemente un disparate. Bueno no voy a hablar de las posibilidades de embargar los *bitcoins*.

Aquí la cuestión es simple. La Constitución Nacional dice en qué casos y con qué justificativos se puede proceder y en "Halabi" la Corte fue muy clara. Casos y justificativos se requieren para todo. En consecuencia, la pregunta que nos tenemos que hacer frente a esta idea de un derecho penal de máxima intervención es cuál es el alcance. Y, perdónenme, pero siempre voy a la historia. En las *Partidas* de Alfonso, el Sabio, con el procedimiento inquisitivo, prohibía expresamente la llamada **pesquisa general**. Estaba expresamente prohibida en 1265. Estaba prohibido investigar, en general, salvo en un caso: cuando una justicia nueva llegaba a un lugar y podía levantar información sobre el delito que se cometía en la comarca. Pero era con fines estadísticos, diríamos. En consecuencia, el principio sigue siendo, para mí, lo que contiene "Halabi", es decir, toda medida que implique un avance sobre derechos individuales debe estar justificada primero por un caso —y en qué caso y con qué justificativos— y no puede ser empleada para saber si se cometen delitos o no. Esto es más o menos lo que quería plantear.

Perspectiva del Derecho Penal Internacional

COLOQUIOS PREPARATORIOS PARA EL XIX CONGRESO INTERNACIONAL DE DERECHO PENAL: "SOCIEDAD DE LA INFORMACIÓN Y DERECHO PENAL" (1)

Sección 4

Documento de reflexión y cuestionario de la AIDP
Relator General: **ANDRÉ KLIP**

Respuestas del Grupo Nacional Argentino:
JAVIER A. DE LUCA, MARCELO RIQUERT, CHRISTIAN C. SUEIRO, MARÍA ÁNGELES RAMOS y **FRANCISCO FIGUEROA**

(A) Objeto del cuestionario

Las preguntas de esta Sección tratan generalmente del "Ciberdelito". Este término se entiende en el sentido de dar cobertura a las conductas criminales que afectan a intereses asociados con el uso de la tecnología de la información y comunicación (TIC), como el funcionamiento adecuado de los sistemas de ordenadores y de internet, la intimidad y la integridad de los datos almacenados o transferidos a o a través de las TIC o la identidad virtual de los usuarios de internet. *El denominador común y rasgo característico de todas las figuras de ciberdelitos y de la investigación sobre ciberdelitos puede hallarse en su relación con sistemas, redes y datos de ordenadores, de un lado, y con los sistemas, redes y datos cibernéticos, del otro. El ciberdelito cubre delitos que tienen que ver con los ordenadores en sentido tradicional y también con la nube del ciberespacio y las bases datos cibernéticas.*

Si se precisa cualquier aclaración, por favor, contactar con el Relator General, Prof. Dr. André Klip por email: andre.klip@maastrichtuniversity.nl

(B) Cuestiones sobre la jurisdicción

(1) (a) ¿Cómo localiza su país el lugar de comisión de un delito cometido en el ciberespacio?

En Argentina, en la mayoría de los casos, se determina el lugar de la comisión del delito a través de la dirección IP que utiliza el ordenador al conectarse

(1) AIDP, Río de Janeiro, Brasil, 31 de agosto al 6 de septiembre de 2014.

a la red y mediante el cual se realiza el acto delictivo. En los casos en que la IP es enmascarada o adulterada, el lugar de comisión se determina a través de último lugar de donde hubo una conexión con el número de IP.

En Argentina, la aplicación de la ley penal está determinada en el art. 1 CP, que establece que dicho Código se aplica a aquellos delitos cometidos en el territorio nacional, cuyos efectos se produzcan allí o en lugares sometidos a nuestra jurisdicción. Es decir, únicamente tendríamos jurisdicción para juzgar los delitos cometidos en Argentina o aquellos cuyos efectos se produzcan en nuestro país aún en los casos en que la acción haya sido realizada fuera de nuestras fronteras.

(b) ¿Su legislación nacional considera necesario y posible localizar el lugar donde se encuentran la información y las pruebas? ¿Dónde está la información que se puede encontrar en la web? ¿Se encuentra donde el ordenador del usuario está físicamente presente? ¿Allí donde el proveedor de la red tiene su sede (jurídica o de hecho)? ¿Qué proveedor? ¿O es el lugar de la persona que posibilitó la disponibilidad de los datos? Si estas preguntas no se consideran jurídicamente relevantes, por favor, indique por qué.

En primer lugar, debemos poner de resalto que, por el momento, nuestro país carece de una ley de procedimientos en materia penal que contemple las situaciones planteadas.

No obstante, consideramos que resultan trascendental conocer dónde se almacena la información que puede llegar a ser prueba digital en un proceso penal.

Si bien en la mayoría de los casos donde se considera que puede haber prueba digital se suele secuestrar ordenadores y sus discos rígidos, lo cierto es que actualmente la evidencia ya no se guarda en esas fuentes de almacenamiento, sino que se suele guardar la información en la nube (*cloud computing*), el ciberespacio o servidores en el extranjero. Por tal razón es que entendemos que resulta necesario conocer dónde se almacena la información para proceder con la mayor celeridad del caso y evitar la pérdida de prueba relevante para el proceso penal.

En ese sentido, creemos que la computación en la nube (*cloud computing*), será uno de los temas sobre los que deberá versar la discusión legislativa en material procesal penal, para así lograr su introducción con las medidas de seguridad informática y evitar almacenar información en servidores situados fuera del territorio nacional.

(2) ¿En su sistema penal se puede prescindir de la determinación del locus delicti en caso de cometerse un ciberdelito? ¿Por qué (no)?

En principio, cuando estamos frente a un ciberdelito propiamente dicho, no se podría prescindir del *locus delicti*. Sin embargo, sí se podría evitar en caso de encontrarnos ante un delito de jurisdicción universal cometido a través de la Internet o en el cual las pruebas fundamentales están en la Internet.

(3) ¿Qué normas de competencia jurisdiccional se aplican a los ciberdelitos tales como la incitación al odio a través de Internet, hacking, ataques contra los sistemas informáticos, etc.? Si su Estado no tiene jurisdicción sobre estos delitos, ¿se considera es esto problemático?

Ante los casos planteados se aplicarían las normas generales ya descriptas.

(4) ¿Su legislación nacional contiene normas relativas a la prevención o a la solución de los conflictos de jurisdicción? ¿Hay alguna práctica sobre ello?

La legislación nacional argentina no posee normas específicas relativas a la prevención o solución de conflictos de jurisdicción en materia de ciberdelitos. No obstante, se aplican los principios generales de aplicación de la ley penal, es decir, el principio de territorialidad y extraterritorialidad; de extensión de la jurisdicción tanto real o de defensa, universal o personal.

(5) ¿En su sistema penal se puede prescindir de los principios jurisdiccionales en caso de que se cometa un ciberdelito, lo que en esencia significa que el Derecho penal nacional es de aplicación universal? ¿Debería esto limitarse a ciertos delitos, o estar condicionada a la existencia de un tratado?

La legislación de la República Argentina no prevé que se pueda prescindir de los principios jurisdiccionales en ningún caso y tampoco contempló una regulación especial para la criminalidad informática.

(C) Derecho penal sustantivo y sanciones

(1) ¿Qué ciberdelitos tipificados en su sistema penal nacional considera usted que tienen una dimensión transnacional?

Consideramos que unos de los delitos con mayor dimensión transnacional es el de ofrecer, almacenar y distribuir pornografía infantil (art. 128 CP).

Además, también consideramos relevantes, a raíz de la intangibilidad del software y del almacenamiento digital de información, los siguientes delitos: 1) Violación de correspondencia electrónica (art. 153 CP), 2) Acceso ilegítimo a un sistema informático (art. 153 *bis* CP), 3) Publicación abusiva de correspondencia (art. 155 CP), 4) Revelación de secretos (art. 157 CP), 5) Delitos relacionados con la protección de datos personales (art. 157 *bis* CP), 6) Defraudación informática (art. 173, inc. 16, CP), 7) Daños (arts. 183 y 184 CP), 8) Interrupción o entorpecimiento de las comunicaciones (art. 197 CP), y 9) La alteración, sustracción, ocultación, destrucción e inutilización de medios de prueba (art. 255 CP),

(2) ¿En qué medida las definiciones de los ciberdelitos contienen elementos jurisdiccionales?

La reforma realizada en materia de criminalidad informática (ley 26.388) no introdujo en la descripción típica de las conductas ningún elemento que haga referencia a la jurisdicción.

(3) ¿Hasta qué punto las reglas de la parte general sobre la comisión, conspiración o cualquier otra forma de participación contienen elementos jurisdiccionales?

La parte general de nuestro derecho penal se aplica a todos los delitos; sin embargo, no contiene elementos jurisdiccionales en materia de ciberdelitos.

(4) ¿Considera usted que los ciberdelitos constituyen un asunto que un Estado puede regular por sí mismo? Si es así, indique cómo puede hacerlo un Estado. Si no es así, indique por qué no puede hacerlo.

Consideramos que los Estados pueden (y deben) regular por sí mismos los ciberdelitos. Sin embargo, para que ello sea posible es indispensable que haya cooperación internacional y compatibilidad de legislaciones. Sobre todo en esta clase de delitos que tienen la particularidad de ser transnacionales a raíz de la fluidez de la información en Internet y el gran problema que presenta la aplicación de la ley penal en el espacio.

(5) ¿Su Derecho penal nacional prevé la responsabilidad penal de las empresas/proveedores (internacionales)? ¿Tiene la atribución de responsabilidad implicaciones jurisdiccionales?

En la actualidad, y por el momento, nuestra legislación penal no prevé la responsabilidad penal de las personas jurídicas en materia de criminalidad informática.

(D) Cooperación en materia penal

(1) ¿Hasta qué punto las especificidades de la tecnología de la información cambian la naturaleza de la asistencia mutua?

No debería cambiarlas desde una perspectiva teórica. En lo práctico, las asimetrías de disponibilidad tecnológica entre los estados pueden obstar a una efectiva asistencia mutua.

(2) (a) ¿Se prevé en su país la interceptación de telecomunicaciones (inalámbricas)? ¿Bajo qué condiciones?

Sí, nuestra legislación prevé la interceptación de telecomunicaciones. Sin embargo, no puede ser ordenada por cualquier actor procesal sino que únicamente puede hacerlo el juez mediante una resolución fundada.

(b) ¿En qué medida es relevante que un proveedor o un satélite puedan estar ubicados fuera de las fronteras del país?

Consideramos que resulta relevante para poder someterlo a la jurisdicción nacional.

(c) ¿Su legislación nacional prevé la asistencia judicial mutua en relación a la interceptación de las telecomunicaciones? ¿Ha celebrado su país convenios internacionales al respecto?

Históricamente, la Argentina participó de los tratados internacionales de cooperación en materia de adquisición y producción de pruebas. En el ámbito interno, rige la Ley de Cooperación Internacional en Materia Penal (ley 24.768 de 1998), cuyos principios generales podría ser aplicados en materia de interceptación de telecomunicaciones.

(3) ¿En qué medida las causas generales de denegación se aplican en relación a las investigaciones en Internet y otros medios para acceder a los ordenadores y las redes ubicadas en otros lugares?

La medida es la misma que para cualquier acto de cooperación, ya que no hay previsión específica aún acerca de investigaciones en Internet.

(4) ¿Se exige en su legislación nacional el requisito de la doble incriminación para la cooperación en aquellas situaciones en las que el autor haya causado los efectos desde un Estado en el que se permite la conducta en un Estado en el que se tipifica como delito la conducta?

Sí se exige, al igual que en los procesos de extradición.

(5) ¿Permite su legislación nacional las investigaciones extraterritoriales? ¿Bajo qué condiciones? Por favor, responda tanto a la situación en la que las autoridades nacionales de aplicación de la ley necesitan información, como cuando las autoridades extranjeras necesitan la información disponible en su Estado.

Toda investigación en el exterior se rige por los principios generales de la cooperación internacional, tanto si nuestros magistrados y funcionarios se constituyen en el extranjero como si las autoridades extranjeras se hacen presente en nuestro país. En cualquier caso, se necesita la aprobación de los magistrados del país requerido.

(6) ¿Se permite el autoservicio (self service) (obtención de pruebas en otro Estado sin pedir permiso)? ¿Qué condiciones deben cumplirse para permitir el autoservicio? Por favor, diferenciar la información pública y la protegida. ¿Cuál es la práctica (tanto activa como pasiva) en su país?

No se permite. En los casos que se trate de información privada, se rige por las reglas del derecho internacional y los principios de libertad probatoria.

No existe legislación procesal penal específica sobre ese asunto en materia de cibercriminalidad.

(7) Si es así, ¿se aplica esta legislación también a las búsquedas que se llevan a cabo en la web de acceso público, o en ordenadores que se encuentran fuera del país?

Sí, se puede hacer desde la Argentina. En ese caso, rige el principio de libertad probatoria, pero también el de defensa en juicio, que exige que la defensa haya tenido la posibilidad de controlar la prueba.

(8) ¿Es su país parte en acuerdos sobre el Registro de Nombre de Pasajero (PNR) (transacciones financieras, intercambio de ADN, cuestiones de visados o similares)? Por favor especificar y explicar cómo se lleva a cabo el intercambio de datos en la legislación nacional. ¿Tiene su país una llamada unidad que está disponible 24 horas al día y 7 días a la semana para el intercambio de datos? Limítese a las cuestiones relevantes sobre uso de la información para la investigación criminal.

Hasta la fecha no se cuenta con una unidad especializada en el intercambio de datos.

(9) ¿Hasta qué punto los datos a que se refiere en su respuesta a la pregunta anterior se intercambian para la investigación criminal y cuál

es el fundamento jurídico? ¿Hasta qué punto la persona concernida tiene la posibilidad de impedir / corregir / eliminar la información? ¿En qué medida puede esta información ser utilizada como prueba? ¿La ley de su país permite la detección y retirada de un sitio web que contiene información ilegal? ¿Existe alguna una práctica? ¿Desempeña algún papel el sitio del proveedor, propietario del sitio o cualquier otro elemento extranjero?

En la Constitución Nacional Argentina se prevé la acción de *habeas data*, que es una herramienta de fácil y ágil acceso para el ciudadano a efectos de detectar, hacer corregir o retirar los datos personales que figuren en bases que pudieran ser no autorizados, excesivos o incorrectos.

(10) ¿Cree usted que es posible un sistema de aplicación internacional para ejecutar las decisiones (por ejemplo, órdenes de suspensión de Internet o inhabilitaciones) en el área de la delincuencia cibernética? ¿Por qué (no)?

Sí, conforme las recomendaciones realizadas por el Convenio de Cibercriminalidad de Budapest.

(11) ¿Su país permite la consulta directa de bases de datos nacionales o internacionales que contienen información relevante para las investigaciones criminales (sin solicitud)?

Si bien existen registros públicos a los que se pueden acceder sin solicitud, también existen otros registros a los que solo se puede acceder con orden judicial.

(12) ¿Participa su país en Interpol/Europol/Eurojust o cualquier otro organismo supranacional que aborde el intercambio de información? ¿Bajo qué condiciones?

En la actualidad, la Argentina participa en Interpol y Europol.

(E) Aspectos relacionados con los derechos humanos

(1) ¿Qué normas de derechos humanos o constitucionales son aplicables en el contexto de las investigaciones penales con tecnología de la información? ¿Es relevante para la determinación de las normas aplicables de derechos humanos dónde se considera que se han realizado las investigaciones?

Todas las normas de derechos humanos o constitucionales se aplican en los procesos penales. Sin embargo, no hay ninguna específica sobre cibercriminalidad.

(2) ¿Cómo se regula la responsabilidad o rendición de cuentas (accountability) de su Estado involucrado en la cooperación internacional? Por ejemplo, ¿es su Estado responsable del uso de la información recolectada por otro Estado en violación de las normas internacionales de derechos humanos?

No está regulado de manera específica.

(F) Desarrollos futuros

(1) Las modernas telecomunicaciones ofrecen la posibilidad de contactar directamente con los acusados, víctimas y testigos a través de las fronteras. ¿Se debería permitir eso y, en caso afirmativo, en qué condiciones? Si no es así, ¿se deberían aplicar las reglas clásicas de asistencia mutua (solicitud y respuesta), y por qué?

En Argentina, en la actualidad, en varias causas penales se permite la videoconferencia para recibir prueba. Sin embargo, donde más se está utilizando esta modalidad es en las causas vinculadas a graves violaciones a los derechos humanos y de megacriminalidad, en las que se permitió que las videoconferencias se realicen con personas que se encuentran residiendo en el extranjero. Lo mismo ocurre con el envío de documentos escaneados, cuando son certificados en el país de origen, por ejemplo, por nuestro Consulado.

En ese sentido, creemos que es sumamente aconsejable y, por suerte, ya lo estamos implementado.

(2) ¿Existe algún impedimento legal en su legislación para las audiencias a través de medios audiovisuales (a través de Skype o de otro medio) en casos transnacionales? Si es así ¿cuál? Si no es así, ¿hay alguna práctica?

Si bien no existe ningún impedimento legal para utilizas esos medios audiovisuales, por el momento no se encuentra específicamente regulado, aunque cada vez se utiliza con mayor asiduidad.

(3) ¿Hay alguna otra cuestión relacionada con la sociedad de la información y el Derecho penal internacional que actualmente juega un papel en su país y no ha sido tratado en las preguntas anteriores?

La computación en la nube (*cloud computing*) y el almacenamiento de información en servidores situados fuera de la jurisdicción nacional, en particular cuando la información a resguardarse es información que pueda provenir de los organismos públicos del Estado.

Panel 4

Convenio sobre Cibercriminalidad de Budapest y el MERCOSUR

Propuestas de derecho penal material y su armonización con la legislación regional sudamericana

MARCELO A. RIQUERT[1]

1. Introducción

Luego de que, en noviembre de 1996, el **Comité Europeo sobre Problemas Penales** creó un Comité de Expertos para trabajar el fenómeno de la delincuencia asociada a la tecnología; el Consejo de Europa impulsó y abrió a la firma el conocido **Convenio sobre Cibercriminalidad**,[2] en su reunión celebrada en la ciudad de Budapest el 23 de noviembre de 2001. Dicho Convenio está en vigor desde el 1° de julio de 2004, con un Protocolo adicional del 28 de enero de 2003 sobre la lucha contra el racismo y la xenofobia por Internet.

---

(1) Profesor de Derecho Penal, Facultad de Derecho de la Universidad Nacional de Mar del Plata. Presidente (2013-2015) de la Asociación Argentina de Profesores de Derecho Penal (AAPDP).

(2) Ver Morales García, "Apuntes de política criminal en el contexto tecnológico. Una aproximación a la Convención del Consejo de Europa sobre Cyber-crime", en AAVV, *Delincuencia Informática. Problemas de responsabilidad*, Madrid, Cuadernos de Derecho Judicial IX-2002, Consejo General del Poder Judicial 2002, p. 17. No obstante, algunos prefieren situar el germen del Convenio aún más atrás, en 1983, cuando una reunión de expertos recomendó a la OCDE (Organización para la Cooperación y Desarrollo Económico) la necesidad de

Para Óscar Morales García, fue el proyecto legislativo más ambicioso en la materia. Además, afirma que, por atemperar algunas de sus propuestas originales durante la revisión de los borradores, ha terminado plasmando "en una Convención político criminalmente aceptable".[3]

Justamente por la búsqueda de consensos entre los Estados que participaron en su confección, Rovira del Canto dijo que se trataba de una "Convención de mínimos".[4] Si bien es una iniciativa de la Unión Europea, ha sido firmado por numerosos países extracomunitarios, como Estados Unidos o Japón. Argentina adhirió en 2010.[5] Además, dentro del margen latinoamericano, se encuentran Costa Rica, República Dominicana, México y Chile.

Esta nota comparte la concepción sobre el Consejo de Europa hecha por Walter Perron en tanto organización de derecho internacional que, claramente, tiene un alcance que va más allá de los Estados miembros de la Unión Europea, cuyo núcleo está expuesto en la Convención Europea sobre derechos humanos. El Consejo no tiene facultades soberanas propias, sino que su objeto es influir en el desarrollo de los Estados miembros a través de recomendaciones y tratados. Su instrumento más importante es el Tribunal Europeo de Derechos Humanos (TEDH), cuya jurisprudencia es de superlativa importancia y ante el que todo ciudadano de un estado miembro puede comparecer en el marco de una petición individual. El nombrado individualiza precisamente como el segundo sector más importante las numerosas convenciones respecto de distintos aspectos del derecho penal y procesal penal; tales como las relativas a extradición,

---

armonización en los delitos informáticos. Esto se materializó tres años después, cuando el Consejo de Europa tomó la iniciativa y publicó en 1989 la Recomendación 89, mostrando la tendencia que desembocó en Budapest (Ver: Díaz Gómez, Andrés, "El delito informático, su problemática y la cooperación internacional como paradigma de su solución: el Convenio de Budapest", en *Revista Electrónica de Derecho* de la *Universidad de La Rioja* (REDUR), n° 8, diciembre de 2010, p. 195.

(3) Morales García, *ibid.*, p. 16.

(4) Rovira del Canto, Enrique, "Ciberdelincuencia intrusiva: hawking y grooming", conferencia brindada en Barcelona, noviembre de 2010, p. 4., [en línea] http://www.iaitg.eu/media-pool/67/671026/data/Ciberdelincuencia_intrusiva_hacking_y_grooming_Enrique_Rovira.pdf

(5) En el marco de la Conferencia de Estrasburgo sobre Cibercrimen, celebrada en marzo de 2010, lo que hace —como bien resalta Cherñavsky— que se realicen las reformas pertinentes para ratificar la Convención (Cherñavsky, Nora, "El delito informático", en De Luca, Javier A. (coord.), *XI Encuentro de Profesores de Derecho Penal de la República Argentina*, Buenos Aires, La Ley/UBA/AAPDP, 2013, p. 288.

asistencia jurídica recíproca, lucha contra el terrorismo o un variado conjunto de delitos conglobados bajo la designación de "criminalidad organizada" —lavado, tráfico de drogas, financiamiento del terrorismo— y otros que solo pueden ser protegidos a nivel transnacional —corrupción pública y privada, protección del medio ambiente, tráfico ilegal de personas, explotación sexual de niños, *insider trading,* manipulaciones del mercado y delitos informáticos—.[6]

Por eso, en un trabajo previo,[7] señalé que el citado Convenio se ha constituido en una referencia insoslayable en términos de armonización legislativa en la materia[8] y que la normativa argentina no tiene al presente mayor problema de compatibilidad con los estándares mínimos que aquél reclama en lo referente al derecho penal sustancial. Mientras que en lo adjetivo o formal es donde puede advertirse algún déficit de mayor significación.[9] No se trata de un problema exclusivo de nuestro país, sino que, como bien advierte Marcos Salt, se trata de un rasgo extendido en toda la legislación latinoamericana. Pues sus previsiones procesales han sido diseñadas pensando en la evidencia física y no en la digital. En muchos casos los problemas que se presentan terminan siendo solucionados por vía jurisprudencial, aplicándose analógicamente criterios y reglas de las pruebas físicas. El retraso en la adopción de reformas procesales respecto

(6) Perron Walter, "Perspectivas de la unificación del derecho penal y del derecho procesal en el marco de la Unión Europea", en AAVV, *Estudios sobre Justicia Penal. Homenaje al Profesor Julio B. J. Maier*, Bs. As., Editores del Puerto, 2005, pp. 734/735 y 737/738.

(7) Riquert, Marcelo, "Delincuencia informática y control social: ¿excusa y consecuencia?", en *Revista Jurídica Facultad de Derecho de la UNMDP,* n° 6, 2011, pp. 67/99; y [en línea] http://perso.unifr.ch/derechopenal/assets/files/articulos/a_20120208_01.pdf

(8) Se trataría de uno de esos casos puntuales en que se provoca una cierta unificación por una "necesidad práctica" en un "ámbito parcial" del derecho penal, conforme la terminología de Hans Joachim Hirsch, quien no se muestra particularmente favorable hacia un posible avance en pos de una unificación general del derecho penal europeo (ver Hirsh, Hans Joachim, "Cuestiones acerca de la armonización del derecho penal y procesal penal en la Unión Europea", en AAVV, *Estudios sobre..., op. cit.,* p. 668).

(9) El Convenio prevé reglas relativas al ámbito de aplicación (art. 14), condiciones y garantías (art. 15), competencia, conservación inmediata de datos, preservación de datos incluidos los de tráfico (art. 16), registro y decomiso de datos informáticos almacenados (Título 4 de la Sección 2°), recogida en tiempo real de datos informáticos y datos de tráfico (art. 20), interceptación de datos relativos al contenido (art. 21), cooperación (cuyos principios generales enuncia el art. 23), colaboración y asistencia internacionales en investigación (art. 31) y medidas cautelares (art. 29; incluyendo en su art. 35 la llamada "Red 24x7", es decir, constituir un punto de contacto las 24 horas del día, los 7 días de la semana) o a la extradición (art. 24).

de las modificaciones en el derecho penal material se verifica también en otras regiones —Alemania, Portugal y España—.[10]

La situación de nuestra región es curiosa. Con la adopción de modernos códigos de corte acusatorio, se ha producido una masiva transformación de los sistemas procesales en los últimos quince años. Sin embargo, ha dejado sin mayores variaciones los s dedicados a la prueba, que permanecen con una semejanza notable a los de los viejos digestos inquisitivos o mixtos.

Hecha la aclaración recuerdo que, para fundar la necesidad de provocar aquella armonización, desde hace tiempo se hace hincapié en que las fronteras nacionales constituyen un obstáculo evidente para la detección, investigación, persecución y castigo de los autores de los delitos perpetrados mediante el uso de las nuevas tecnologías de la información y comunicación (TIC). En cambio, Internet está configurada como un espacio sin fronteras para aquéllos. Hay una ineludible dimensión supranacional[11] y, para afrontarla, es claro que la vía más conveniente no es la antigua cooperación bilateral; sino el impulso de esfuerzos de armonización regional mediante convenios multilaterales, como el que ahora nos ocupa.[12] Además, como resalta Lezertua, la armonización sustantiva es un elemento indispensable pero no suficiente para llevar a cabo un combate eficaz contra la ciberdelincuencia. Debe ser acompañada de otro relativo a los instrumentos apropiados para detectar, investigar, procesar y castigar a los autores de esas infracciones.[13]

Jansky y Lombaert destacan que la Comisión Europea, en su comunicación "Hacia una estrategia general en la lucha contra la ciberdelincuencia",

---

(10) Ver Salt, Marcos, *Criminal procedure law provisions on cybercrime in Latin American regarding their compliance with the Budapest Convention (Argentina, Chile, Colombia, Costa Rica, México, Paraguay and Perú)*, Estrasburgo, council of Europe, 12 de abril de 2011, p. 4.

(11) En este sentido, parece importante no perder de vista que, en el caso de nuestro objeto de atención aquí, estamos en general frente a lo que constituiría en su evolución un "derecho penal transnacional". Es decir, referido a crímenes transnacionales. Y no un "derecho penal internacional" stricto sensu, referido a crímenes internacionales como los reconocidos por el Estatuto de Roma. A saber: genocidio, crímenes de lesa humanidad, de guerra y el crimen de agresión (Romeo Malanda, Sergio, "Un nuevo modelo de derecho penal transnacional: el derecho penal de la Unión Europea tras el Tratado de Lisboa", en *Estudios Penales y Criminológicos*, Servicio de Publicaciones de la Universidad de Santiago de Compostela, vol. XXXII, 2012, p. 318. El autor, aquí, alude a las opiniones de autores como Boister y Sieber).

(12) Díaz Gómez, *op. cit.*, p. 183.

(13) Lezertua, Manuel, "El proyecto de Convenio sobre el Cybercrimen del Consejo de Europa", en López Ortega, Juan José (dir.), *Internet y Derecho Penal*, Madrid, *Cuadernos de Derecho Judicial* X-2001, Consejo General del Poder Judicial, 2001, p. 25.

distingue una tercer área de actividades principales en la elaboración de una estrategia europea coherente para luchar contra la ciberdelincuencia en cooperación con los Estados miembros de la Unión Europea; tanto con las instituciones de la región como las internacionales. Señalan, además, que la legislación y la ejecución de la ley a nivel transfronterizo debe articularse con la colaboración de los sectores público y privado.(14) Cherñavsky ha destacado la experiencia adquirida por Europol en la coordinación de programas sobre cibercrimen, de respuestas y estrategias, incluso respecto de la lucha contra el terrorismo. A su vez destacó la necesidad de que Argentina desarrolle esa experticia en cooperación internacional y con el intercambio de información tanto contra del cibercrimen como de los delitos financieros, del lavado de dinero y del terrorismo.(15)

En el presente trabajo, solo será objeto de tratamiento lo concerniente al derecho penal material. Queda, entonces, para una futura oportunidad lo vinculado a aspectos procesales y operativos.

En un estudio comparativo de derecho regional anterior cotejé la situación argentina con los restantes países miembros plenos del MERCOSUR,(16) partiendo de nuestra regulación nacional. En cambio, en este, la tarea no solo comprende una base mayor de países comparados —se incorporan los Estados asociados—,(17) sino que se concreta tomando como eje el articulado que propone Budapest en su capítulo II —"Medidas que deben ser adoptadas a nivel nacional"—, cuya sección 1 se dedica al "Derecho penal material" (arts. 2 a 13) y se subdivide en cinco títulos.

---

(14) Radomir Jansky y Ruben Lombaert, "Hacia una estrategia europea unificada para combatir la ciberdelincuencia", en *E) NAC. E-newsletter. En la lucha contra el cibercrimen*, n° 4, octubre de 2009, p. 39.

(15) Cherñavsky, *op. cit.*, p. 288. Díaz Gómez sugiere que la cooperación internacional —que liga a la constitución de un derecho procesal penal internacional— resultaría el paradigma de la solución a la problemática de la ciberdelincuencia (*op. cit.*, p. 187), aunque más adelante en su trabajo rescata la dimensión de armonización en materia sustantiva, que constituiría un derecho penal internacional (*ibid.*, p. 191).

(16) Riquert, Marcelo, *Delincuencia informática en la Argentina y el Mercosur*, Bs. As., EDIAR, 2009, prologada por el Prof. Emérito de la UBA, Dr. David Baigún. Ver, en particular, el capítulo VII. Téngase presente, además, que en ese momento los miembros plenos eran solo la República Argentina, la República Federativa de Brasil, la República del Paraguay y la República Oriental del Uruguay. Estaba en trámite de acceder a tal condición la República Bolivariana de Venezuela, al presente finalizado. Se encuentra en vías de adquirir la calidad plena el Estado Plurinacional de Bolivia.

(17) Estos son en la actualidad Chile, Colombia, Ecuador y Perú. Aún están en trámite de asociación Guyana y Surinam, por lo que no forman parte de la base comparada.

La situación de nuestro bloque regional —más allá de su ampliación,[18] en cuanto se lo relaciona con el de origen del instrumento internacional citado, la Unión Europea,— no ha sufrido cambios.

Con buena voluntad, del MERCOSUR puede decirse que se mantiene en el estadio correspondiente al momento previo al fundacional Tratado de Maastricht —año 1992—, cuando desde la estructura comunitaria no había competencia alguna en el ámbito del derecho penal y procesal penal aunque, como resalta Walter Perron:

> "ya entonces se era consciente de que, debido a los múltiples problemas provocados por la criminalidad transnacional e internacional, que afectaba bienes jurídicos regionales, se había tornado necesaria una colaboración más estrecha entre los países, así como una armonización del derecho penal".[19]

Debe tenerse presente que en el Convenio no se proporciona una definición general de "delito informático", "ciberdelito" o de "cibercrimen". Por lo que podría decirse que, frente al dilema en la teoría criminológica, ante las nuevas formas de delito generadas por las TIC —sintetizado por

---

(18) Vale aclarar que esta afirmación se corresponde estrictamente con la cuestión penal ya que, como señalan Piccone y Mangini, hoy se habla de la aparición de un nuevo paradigma en el regionalismo sudamericano —cuya expresión más acabada sería la UNASUR—, definido como "post-comercial" (Celli, Salles, Tussie y Peixoto), "post-liberal" (Motta Veiga y Ríos), "post-neoliberal" o "post-hegemónico" (Serbin). Sus elementos distintivos serían: a) la revalorización de la agenda política frente a la agenda económico-comercial; b) la adopción de una nueva agenda de desarrollo, distanciándose de las estrategias de liberalización comercial del "regionalismo abierto"; c) el despliegue de una agenda positiva de integración orientada a una mayor coordinación político-estratégica y el desarrollo de una institucionalidad común en áreas no comerciales, como paz y seguridad regional (Piccone, V.; Mangini, M., "UNASUR en el contexto del regionalismo y los paradigmas de la integración latinoamericana", en *Revista Derecho Público*, año II, nº 5, Buenos Aires, Ediciones Infojus, pp. 196/197). Al presente hay una simetría en la conformación del MERCOSUR y la UNASUR. Ya que todos los miembros y asociados del primero integran la segunda y Guyana y Surinam, que integran la segunda, ya se ha señalado que han solicitado ser considerados Estados asociados al primero.

(19) Perrón, *op. cit.*, pp. 729/730. Con "Maasricht", el derecho europeo comunitario hasta entonces existente configuró la denominada "primera columna", lo relativo a política exterior y seguridad común de todos los estados miembros pasó a ser la "segunda columna" y, finalmente, la "tercera columna" se conformó con lo relativo a la cooperación interestatal en los ámbitos de Interior y Justicia lo que, como destaca Perron, no implicaba la creación de un nuevo derecho supranacional pero sí dejaba en claro que la cooperación internacional en materia jurídico-penal resultaba un objeto que hacía al interés común de todos los Estados miembros de la Unión Europea.

Zavrsnik como los enfoques "vino viejo, botella nueva" (Grabosky) y "vino nuevo sin botella" (Wall)—,[20] no ha tomado partido.

En los cuatro primeros títulos se enumera una serie de comportamientos —en total nueve, que contienen una o varias conductas, siempre "intencionales" para la tradición anglosajona, o "dolosas" para el modelo dogmático europeo-continental— a la que los Estados son exhortados a considerar como infracciones penales en su legislación interna.

No se trata, entonces, de la provisión de una **redacción tipo** de delitos, cual suerte de receta inalterable; sino de una formulación genérica, abierta y, en algunos casos, con alternativas que los signatarios puedan adaptar conforme a su propio diseño de derecho local. Esta característica, lógica y apropiada para una suerte de Convenio-marco, dificulta el cotejo con la normativa nacional, ya que dentro del universo de casos en consideración hay legislación pre-Convenio y post-Convenio de países que lo han firmado y otros que no; que han realizado una tipificación más amplia o más restrictiva y, a la vez, que lo hicieron en forma más concentrada o más dispersa en un doble sentido:

a. en cuanto a la adopción de una ley especial o un capítulo específico en su Código Penal, o en alternadas modificaciones en leyes especiales y el propio Código, o difuminada o sectorizada dentro del último;

b. en cuanto el Convenio brinda en algún artículo una serie de verbos típicos para los que no hay una sola norma nacional que los reciba juntos, sino que puede hacerlo desperdigados entre diferentes tipicidades o, incluso, solo parcialmente.

Es esencial no perder de vista este factor; porque, al concretar la comparación tendiente a establecer asertiva o negativamente la recepción de una propuesta en el nivel nacional, en ocasiones, se improvisa una respuesta que sería aproximada. Es decir, puede darse el caso de que, sin haber correspondencia precisa, aun con algún déficit menor de tipicidad; no pueda sostenerse la absoluta laguna de punibilidad local y, por eso, se entienda que existe cumplimiento con el requerimiento externo, aunque sea parcial.

(20) Zavrsnik, Ales, "La intervención del sistema de justicia penal en las amenazas a la ciberseguridad: ¿panacea o caja de Pandora?", en *E-newsletter,* nº 44, diciembre de 2008, p. 3. Señala el autor que, en la actualidad, pareciera que ambos enfoques son correctos, o no, pero que los nuevos conceptos sobre información, computadoras y redes han posicionado al segundo en la vanguardia de la investigación criminológica.

Tampoco en el Convenio se indica o sugiere en cada caso algún tipo de sanción concreta. En el art. 13, en forma general, se habla de la respuesta penal de personas físicas y jurídicas. Esta debe ser efectiva, proporcionada y disuasoria. En el caso de las personas jurídicas, puede tratarse tanto de sanciones penales como civiles o administrativas. Y dentro de las penas, puede incluirse las pecuniarias. En cambio, en caso de las personas físicas, puede incluirse las penas privativas de libertad.

2. Las infracciones contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos

Se comenzará siguiendo el orden propuesto en el Convenio de Budapest —Título 1 de la Sección 1 del II, dedicado a las "Infracciones contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos"—, donde se indica que los Estados tipificarán penalmente las siguientes conductas, agrupadas en cinco artículos: acceso ilícito, interceptación ilícita, atentado contra la integridad de los datos, atentado contra la integridad del sistema y abuso de equipos e instrumentos técnicos. Antes de pasar al detalle comparativo, se aclara que, luego de la transcripción del texto del Convenio, se ha seguido un orden alfabético que no distingue entre miembros plenos y asociados del MERCOSUR.

2.1. Acceso ilícito (art. 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, el acceso doloso y sin autorización a todo o parte de un sistema informático. Las Partes podrán exigir que la infracción sea cometida con vulneración de medidas de seguridad, con la intención de obtener los datos informáticos o con otra intención delictiva, o también podrán requerir que la infracción se perpetre en un sistema informático conectado a otro sistema informático".[21]

(21) Esta propuesta típica, con algún cambio, fue reafirmada mediante la Decisión Marco 2005/222/JAI del Consejo, de 24 de febrero de 2005, relativa a los ataques contra los sistemas de información, con esta redacción: "Artículo 2°. Acceso ilegal a los sistemas de información. 1) Cada Estado miembro adoptará las medidas necesarias para que el acceso intencionado sin autorización al conjunto o a una parte de un sistema de información sea sancionable como infracción penal, al menos en los casos que no sean de menor gravedad. 2) Cada Estado miembro podrá decidir que las conductas mencionadas en el apartado 1 sean objeto de acciones judiciales únicamente cuando la infracción se cometa transgrediendo medidas

a. Esta primera figura consagra uno de los supuestos prototípicos de lo que algunos clasifican como "ciberdelincuencia intrusiva". Es decir, aquellos configurados por ataques contra la intimidad y la privacidad que, autores como Rovira del Canto, extienden al honor, la intimidad personal y familiar, la propia imagen, el domicilio, el secreto de las comunicaciones o incluso el uso adecuado y correcto de la informática.[22]

Es interesante resaltar que, si bien el Convenio toma partido por considerar delito el simple *hacking*, permite que los signatarios introduzcan condicionantes —la vulneración de medidas de seguridad— y elementos subjetivos distintos del dolo —la intención de obtener datos u otra intención delictiva—. También permite que la tipificación se limite a casos de acceso a sistemas informáticos a los que esté conectado otro. Sin embargo, cuando se observa la recepción nacional, en general, se ha terminado consagrando figuras penales de mayor amplitud sin hacer uso de las posibilidades de restringir la tipicidad. Además, el Convenio admite —no exige—como sanción la pena privativa de libertad. Un problema básico de esto es que, si en el delito más leve, básico y de aplicación subsidiaria se usa la modalidad más grave de sanción; se caerá en problemas serios de proporcionalidad en el resto de las conductas. En realidad, se trata de un comportamiento sobre el que se discute si realmente es necesaria la intervención del derecho penal o si bastaría con la del contravencional o sancionador administrativo. Se estiman más lógicas las penas pecuniarias o de inhabilitación que la prisión.

b. Pasando a la recepción en el ámbito del MERCOSUR, puede señalarse que el "intrusismo informático" está expresamente tipificado en:

b.1 **Argentina**: por ley 26.388, lo ha incorporado al CP como artículo 153 *bis*.[23] La misma ley reformó el III del Título V —"Delitos contra la Libertad"—, que

---

de seguridad". A su vez, ha sido sustituido por el artículo 3° de la Directiva 2013/40/UE del Parlamento Europeo y del Consejo de 12 de agosto de 2013 relativa a los ataques contra los sistemas de información, fusionando ambos párrafos del siguiente modo: "Los Estados miembros adoptarán las medidas necesarias para que, cuando haya sido realizado intencionalmente, el acceso sin autorización al conjunto o a una parte de un sistema de información sea sancionable como infracción penal cuando se haya cometido con violación de una medida de seguridad, al menos en los casos que no sean de menor gravedad".

(22) Rovira del Canto, *op.cit.*, p. 1. Completa su clasificación tripartita con la "ciberdelincuencia económica", con los ataques de contenido patrimonial y el "ciberespionaje y ciberterrorismo", que se refiere a los ataques contra bienes supraindividuales.

(23) "Será reprimido con prisión de quince (15) días a seis (6) meses, si no resultare un delito más severamente penado, el que a sabiendas accediere por cualquier medio, sin la debida

pasó a ser "Violación de Secretos y de la Privacidad", y dotó de una nueva redacción al artículo 157 *bis*, cuyo primer párrafo[24] pune el acceso ilegítimo a un banco de datos personales.

b.2 **Bolivia**: prevé en el artículo 363 *ter*[25] de su CP del año 1997, junto a la alteración y el uso indebido de datos informáticos, la punición del acceso a aquellos datos informáticos alojados en una computadora o cualquier soporte informático.

b.3 **Colombia**: su CP —ley 599 de 2000— ha sido modificado por la ley 1273 de 2009. Esta incorporó como capítulo VII *bis* uno específico para la delincuencia informática. El acceso abusivo a un sistema informático está contemplado en el artículo 269A.[26] Además debe tenerse presente que todas las conductas del capítulo tienen previstas una serie de circunstancia de agravación en el artículo final —269H—.[27]

---

autorización o excediendo la que posea, a un sistema o dato informático de acceso restringido. La pena será de un (1) mes a un (1) año de prisión cuando el acceso fuese en perjuicio de un sistema o dato informático de un organismo público estatal o de un proveedor de servicios públicos o de servicios financieros" (art. 153 *bis* del CP).

(24) El texto vigente del art. 157 *bis*, en su parte pertinente, dice: "Será reprimido con la pena de prisión de un (1) mes a dos (2) años el que: 1. A sabiendas e ilegítimamente, o violando sistemas de confidencialidad y seguridad de datos, accediere, de cualquier forma, a un banco de datos personales…" (art. 157 *bis* del CP).

(25) Cuyo texto dice: "El que sin estar autorizado se apodere, acceda, utilice, modifique, suprima o inutilice, datos almacenados en una computadora o en cualquier soporte informático, ocasionando perjuicio al titular de la información, será sancionado con prestación de trabajo hasta un año o multa hasta doscientos días" (art. 363 *ter*).

(26) El nuevo artículo dice: "El que, sin autorización o por fuera de lo acordado, acceda en todo o en parte a un sistema informático protegido o no con una medida de seguridad, o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes".

(27) Su texto: "Las penas imponibles de acuerdo con los artículos descritos en este título, se aumentarán de la mitad a las tres cuartas partes si la conducta se cometiere:

1. Sobre redes o sistemas informáticos o de comunicaciones estatales u oficiales o del sector financiero, nacionales o extranjeros.
2. Por servidor público en ejercicio de sus funciones.
3. Aprovechando la confianza depositada por el poseedor de la información o por quien tuviere un vínculo contractual con este.
4. Revelando o dando a conocer el contenido de la información en perjuicio de otro.
5. Obteniendo provecho para sí o para un tercero.
6. Con fines terroristas o generando riesgo para la seguridad o defensa nacional.
7. Utilizando como instrumento a un tercero de buena fe.
8. Si quien incurre en estas conductas es el responsable de la administración, manejo o control de dicha información, además se le impondrá hasta por tres años, la pena de inhabilitación para el ejercicio de profesión relacionada con sistemas de información procesada con equipos computacionales".

b.4 **Ecuador**: a continuación del artículo 202 CPE, por ley 2002-67, se agregó un artículo sin número[28] cuyo primer segmento en su primer párrafo prevé el acceso u obtención de información protegida y, en el segundo, califica la conducta de acuerdo al tipo de información de que se trate.

b.5 **Paraguay**: conducta típica a partir de la reforma del CP por ley 4439 del año 2011, prevista en el nuevo artículo 174 b.[29]

b.6 **Perú**: había incorporado en su Parte Especial, por ley 27.309 —del 17 de julio de 2000—, en el Título V de los delitos contra el patrimonio; un X —"Delitos Informáticos"— con tres artículos. El primero de ellos (art. 207-A) punía, entre otras conductas, el ingreso indebido a una base de datos, sistema o red de computadoras, o cualquier parte de la misma con varias finalidades. Mientras que el último (art. 207-C) agravaba los anteriores en caso de que el acceso se hubiera logrado usando información privilegiada o se pusiera en peligro la seguridad nacional. El 22 de octubre de 2013 se publicó la nueva "Ley de Delitos Informáticos", bajo N° 30.096. Los mencionados artículos fueron derogados por su "disposición complementaria derogatoria única", a la vez que el "acceso ilícito" fue previsto en su artículo 2.[30]

b.7 **Venezuela**: prevé el "acceso indebido" en el artículo 6[31] de la "Ley Especial contra los Delitos Informáticos" (LECDI) del año 2001. A su vez, el artículo 9 establece como agravante que el sistema que utilice tecnologías de la información esté destinado a funciones públicas o contenga información personal o patrimonial de personas naturales o jurídicas, caso en

(28) La parte pertinente dice: "art. (...) (1). (Ag. por art. 58, ley 2002-67, RO 557-S, 17-IV-2002). El que empleando cualquier medio electrónico, informático o afín, violentare claves o sistemas de seguridad, para acceder u obtener información protegida, contenida en sistemas de información; para vulnerar el secreto, confidencialidad y reserva, o simplemente vulnerar la seguridad, será reprimido con prisión de seis meses a un año y multa de quinientos a mil dólares de los EU de Norteamérica.

Si la información obtenida se refiere a seguridad nacional, o a secretos comerciales o industriales, la pena será de uno a tres años de prisión y multa de mil a mil quinientos dólares de los Estados Unidos de Norteamérica".

(29) Con el siguiente texto: "Acceso indebido a datos. 1° El que sin autorización y violando sistemas de seguridad obtuviere para sí o para terceros, el acceso a datos no destinados a él y especialmente protegidos contra el acceso no autorizado, será castigado con pena privativa de libertad de hasta tres años o multa. 2° Como datos en sentido del inc. 1, se entenderán solo aquellos, que se almacenan o transmiten electrónicamente, magnéticamente o de otra manera no inmediatamente visible".

(30) Dice: "El que accede sin autorización a todo o parte de un sistema informático, siempre que se realice con vulneración de medidas de seguridad establecidas para impedirlo, será reprimido con pena privativa de libertad no menor de uno ni mayor de cuatro años y con treinta a noventa días multa. Será reprimido con la misma pena el que accede a un sistema informático excediendo lo autorizado" (art. 2).

(31) Su texto: Toda persona que "sin la debida autorización o excediendo la que hubiere obtenido, acceda, intercepte, interfiera o use un sistema que utilice tecnologías de información, será pena con prisión de uno a cinco años y multa de diez a cincuenta unidades tributarias".

que se incrementaría la pena entre una tercera parte y la mitad. A su vez, el artículo 21, referido a la violación de la privacidad de las comunicaciones, sanciona con pena de dos a seis años y multa de doscientas a seiscientas unidades tributaria al que, mediante el uso de las tecnologías de la información, acceda a cualquier mensaje de datos o señal de transmisión o comunicación ajena.

c. En cambio, no han modificado sus legislaciones:

c.1 **Brasil**: donde la conducta sería atípica. Aunque existe una salvedad en la regulación especial de su Ley Electoral N° 9100 del año 1995. El motivo fue la incorporación del sistema de voto electrónico en las elecciones de 1996; por lo que se introdujo (art. 67 inc. VII) un tipo penal para punir con reclusión de uno a dos años y multa la obtención indebida de acceso, o su intento, a un sistema de tratamiento automatizado de datos utilizado por el servicio electoral con el fin de alterar el cómputo o cálculo de votos.

c.2 **Chile**: tampoco lo prevé en forma directa.

c.3 **Uruguay**: no hay un tipo específico, pero se ha verificado una condena por esta conducta —subsumida bajo la figura del artículo 300 del CP—,[32] que pena el "conocimiento fraudulento de secretos", aparentemente más apto para los casos de intercepción ilícita.

2.2. Interceptación ilícita (art. 3)

> "Las Partes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias para prever como infracción penal, conforme a su derecho interno, la interceptación, dolosa y sin autorización, cometida a través de medios técnicos, de datos informáticos —en transmisiones no públicas— en el destino, origen o en el interior de un sistema informático, incluidas las emisiones electromagnéticas provenientes de un sistema informático que transporta tales datos informáticos. Las Partes podrán exigir que la infracción sea cometida con alguna intención delictiva o también podrán requerir que la infracción se perpetre en un sistema informático conectado a otro sistema informático".[33]

(32) Dice: "El que, por medios fraudulentos, se enterare del contenido de documentos públicos o privados que por su propia naturaleza debieran permanecer secretos, y que no constituyeran correspondencia, será castigado, siempre que del hecho resultaren perjuicios, con multa de 20 U.R. (veinte unidades reajustables) a 400 U.R. (cuatrocientas unidades reajustables)".

(33) Si bien la DM del año 2005 mencionada respecto del anterior artículo no previó equivalente al ahora transcripto, su sustituta Directiva 2013/40/UE del Parlamento Europeo y del Consejo de 12 de agosto de 2013 relativa a los ataques contra los sistemas de información, ha reafirmado la propuesta típica en su artículo 6°: "Los Estados miembros adoptarán las

a. Al igual que en el caso anterior, el Convenio contempla que los signatarios incorporen la conducta descripta sujetando su tipicidad a la exigencia de alguna intención delictiva, o que se perpetre con relación a un sistema informático interconectado. Pero, sin embargo, cuando se han dado casos de tipificación posterior, no se observa la adopción de tales limitaciones.

b. En los países del MERCOSUR se observa lo siguiente:

b.1 **Argentina**: la protección de las comunicaciones por vía electrónica se procura a través del concurso de diferentes normas. Para ello se distinguen dos perspectivas: las que afectan el secreto y la privacidad, y las que conciernen a la seguridad del medio de comunicación mismo —pertinentes a los fines del art. 5 de Budapest—. En consecuencia, se han sustituido o incorporado tipos en los s respectivos de la parte especial.

En lo que hace a la "Violación de secretos y de la privacidad", con la ley 26.388 —año 2008 — se cerró la discusión concerniente a la protección o desprotección penal del correo electrónico, sustituyendo al 153 CP;[34] incluyendo el tema de la publicación abusiva de correspondencia para que alcance a la "comunicación electrónica" con la sustitución del artículo 155.[35]

b.2 **Brasil**: los e-mails tienen parcial protección en el artículo 151 CP, con alguna discusión en cuanto a la exigencia de que la correspondencia esté "cerrada"; mientras que serían atípicas las conductas de suprimir, agregar o modificar el contenido del mensaje. Túlio L. Vianna opina en contra de

---

medidas necesarias para garantizar que la interceptación, por medios técnicos, de transmisiones no públicas de datos informáticos hacia, desde o dentro de un sistema de información, incluidas las emisiones electromagnéticas de un sistema de información que contenga dichos datos informáticos, intencionalmente y sin autorización, sea sancionable como infracción penal, al menos en los casos que no sean de menor gravedad".

(34) Tiene ahora el siguiente texto: "Será reprimido con prisión de quince (15) días a seis (6) meses el que abriere o accediere indebidamente a una comunicación electrónica, una carta, un pliego cerrado, un despacho telegráfico, telefónico o de otra naturaleza, que no le esté dirigido; o se apoderare indebidamente de una comunicación electrónica, una carta, un pliego, un despacho u otro papel privado, aunque no esté cerrado; o indebidamente suprimiere o desviare de su destino una correspondencia o una comunicación electrónica que no le esté dirigida. En la misma pena incurrirá el que indebidamente interceptare o captare comunicaciones electrónicas o telecomunicaciones provenientes de cualquier sistema de carácter privado o de acceso restringido. La pena será de prisión de un (1) mes a un (1) año, si el autor además comunicare a otro o publicare el contenido de la carta, escrito, despacho o comunicación electrónica. Si el hecho lo cometiere un funcionario público que abusare de sus funciones, sufrirá además, inhabilitación especial por el doble del tiempo de la condena".

(35) Su redacción actual: "Será reprimido con multa de pesos un mil quinientos ($ 1500) a pesos cien mil ($ 100.000), el que hallándose en posesión de una correspondencia, una comunicación electrónica, un pliego cerrado, un despacho telegráfico, telefónico o de otra naturaleza, no destinados a la publicidad, los hiciere publicar indebidamente, si el hecho causare o pudiere causar perjuicios a terceros. Está exento de responsabilidad penal el que hubiere obrado con el propósito inequívoco de proteger un interés público".

la subsunción en el artículo 151 citado, aunque propició otra por la que la correspondencia electrónica tiene protección penal, partiendo del propio artículo 5°, XII de la Constitución Federal, que incluyó la inviolabilidad y secreto de la comunicación de datos.[36] Sostiene que el delito de violación de mails está tipificado en el marco de la genérica redacción del artículo 56 del Código Brasilero de Telecomunicaciones[37] —ley 4117 de 27 de agosto de 1962—, en función del artículo 58 del mismo texto, que deriva a la pena del mencionado artículo 151 del CP —detención de uno a seis meses o multa—; además de fijar algunas particulares para los concesionarios o permisionarios —elevando hasta uno a dos años de detención—. Se trata, simplemente, de un agente que efectivamente recoge o toma el mensaje del servidor sin autorización legal o reglamentaria.

En el artículo 10 de la ley 9296 del 24 de julio de 1996 —que reglamenta el citado artículo 5° CF—, se tipificó la conducta de quien realiza intercepción de comunicación telefónica, informática o telemática; o viola el secreto de justicia sin autorización judicial o con objetivos no autorizados legalmente.[38] Para Vianna, esta norma —que prevé la reclusión de dos a cuatro años y multa— vino, aparentemente, a aumentar la pena del delito de violación de e-mails. Al ser la "interceptación" una acción típica, concluye que sólo serán aprehendidos por esta figura los casos en que el autor impida que el mensaje llegue intacto al destinatario. Por eso, los supuestos casos en los que simplemente se acceda al servidor y se lea los mails, sin modificar o borrarlos, no serían intercepciones ya que no interrumpirían el curso del mensaje. De allí que sostenga que la mera lectura o copia de mails deben ser encuadrados en los citados artículos 56 y 58 del Código Brasilero de Telecomunicaciones (parág. 2.4).

b.3 **Chile**: contempla el que denomina "Espionaje informático" en el artículo 2° de la ley 12.223 del año 2003.

b.4 **Colombia**: en su CP —ley 599, del año 2000—, por ley 1273 de 2009, se incorporó la figura de interceptación de datos informáticos en el artículo 269C.[39]

---

(36) Vianna, Túlio Lima, "Dos crimes por computador", [en línea] www.mundojuridico.adv.br, en 16/4/03. La parte pertinente del artículo citado de la C.F. dice: *"é inviolavel o sigilo da correspondencia e das comunicações telegráficas, de dados e das comunicações telefônicas…"*.

(37) Dice: *"Pratica crime de violação de telecomunicações quem, transgredindo lei ou regulamento, exiba autógrafo ou qualquer documento ou arquivo, divulgue ou comunique, informe ou capte, transmita a outrem ou utilize o conteúdo, resumo, significado, interpretação, indicação ou efeito de qualquer comunicação dirigida a terceiro"*.

(38) Ver Lopes da Silva, "Direito Penal e Sistema Informático", en *Editora Revista dos Tribunais, Série Ciência do Direito Penal Contemporânea*, vol. 4, San Pablo, Brasil, 2003, p. 70.

(39) Su texto: "El que, sin orden judicial previa intercepte datos informáticos en su origen, destino o en el interior de un sistema informático, o las emisiones electromagnéticas provenientes de un sistema informático que los transporte incurrirá en pena de prisión de treinta y seis (36) a setenta y dos (72) meses".

b.5 **Ecuador**: la interceptación de las comunicaciones está prevista en el artículo 197[40] de su CP. Además, a continuación del artículo 202 CPE se agregó por ley 2002-67 un artículo sin número[41] que tiene dos segmentos. En los párrafos tres y cuatro del primero de ellos, se pune la violación de secretos comerciales o industriales y se agrava la conducta de divulgación o utilización fraudulenta si es perpetrada por persona encargada de la custodia o utilización legítima de datos. En el segundo segmento, se tipifica directamente la obtención y uso no autorizado de información sobre datos personales.

En materia de delitos comunes de la función policial o militar, por ley sin número del 19 de mayo de 2010, se introdujo un artículo sin número[42] a

(40) Dice: "art. 197 (Sustituido por el art. 2° de la ley s/n, R.O. 555-S, 24-III-2009). Serán sancionados con penas de 2 meses a un año de prisión, quienes interceptaren sin orden judicial, conversaciones telefónicas o realizadas por medios afines y quienes se sustrajeran o abrieran sobres de correspondencia que pertenecieren a otro sin autorización expresa. Se exime la responsabilidad de quien lo hizo cuando la interceptación telefónica o la apertura de sobres se produce por error, en forma accidental o fortuita".

(41) Su parte pertinente dice: "art. (...) (1). (...) La divulgación o la utilización fraudulenta de la información protegida, así como de los secretos comerciales o industriales, será sancionada con pena de reclusión menor ordinaria de tres a seis años y multa de dos mil a diez mil dólares de los Estados Unidos de Norteamérica. Si la divulgación o la utilización fraudulenta se realiza por parte de la persona o personas encargadas de la custodia o utilización legítima de la información, éstas serán sancionadas con pena de reclusión menor de seis a nueve años y multa de dos mil a diez mil dólares de los Estados Unidos de Norteamérica.

art. (...) (2). (Ag. por art. 58, ley 2002-67, R.O. 557-S, 17-IV-2002). Obtención y utilización no autorizada de información. La persona o personas que obtuvieren información sobre datos personales para después cederla, publicarla, utilizarla o transferirla a cualquier título, sin la autorización de su titular o titulares, serán sancionadas con pena de prisión de dos meses a dos años y multa de mil a dos mil dólares de los Estados Unidos de Norteamérica".

(42) Sus textos: "art. (...) (602.11). Violación de correspondencia. (Agregado por el art. 4° de la ley s/n, R.O. 196-S, 19-V-2010). Será sancionado con prisión de tres meses a un año, la servidora o servidor militar o policial que, sin la debida autorización legal, intercepte, examine, retenga, grabe o difunda correspondencia o comunicaciones privadas o reservadas de cualquier tipo y por cualquier medio".

"art. (...) (602.12). Delitos contra la información pública no clasificada legalmente. (Agregado por el art. 4 de la ley s/n, R.O. 196-S, 19-V-2010). Será sancionado con prisión de tres meses a un año, la servidora o servidor militar o policial que, utilizando cualquier medio electrónico, informático o afín, obtenga información a la que tenga acceso en su condición de servidora o servidor policial o militar, para después cederla, publicarla, divulgarla, utilizarla o transferirla a cualquier título sin la debida autorización. La misma pena será aplicable a quien destruyere o inutilizare este tipo de información.

Si la divulgación o la utilización fraudulenta son realizadas por cualquier persona o personas encargadas de la custodia o utilización legítima de la información, éstas serán sancionadas con el máximo de la pena".

"art. (...) (602.13). Delitos contra la información pública clasificada legalmente. (Agregado por el art. 4 de la ley s/n, R.O. 196-S, 19-V-2010). Será sancionado con reclusión menor ordinaria

continuación del artículo 602 del CP, cuyos segmentos undécimo a décimo tercero consagran tipos especiales de violación de correspondencia y contra la información pública clasificada o no clasificada legalmente.

b.6 **Paraguay**: por vía de la reciente ley 4439 —año 2011—, se incorporó la interceptación de datos como nuevo artículo 146 c[43] a su CP. Con carácter previo, puede mencionarse la existencia de regulación vinculada al secreto de empresa, que tiene protección penal expresa conforme el Código Penal de 1997 en el capítulo VII —"Hechos punibles contra el ámbito de la vida y la intimidad de la persona"—, en el artículo 147 —"Revelación de un secreto de carácter privado"—.[44]

b.7 **Perú**: el artículo 207-A del CP de 1991 —conforme ley 27.309 del 17 de julio de 2000— punía, entre otras conductas, el uso o ingreso indebido a una base de datos, sistema, red de computadoras o cualquier parte de la misma con finalidad de interferir, interceptar, acceder o copiar información en tránsito o contenida en una base de datos. Regían también los agravantes del artículo 207-C. Fueron derogados mediante la "disposición complementaria derogatoria única" de la ley 30.096 de 2013; por la que ha pasado a ser el tipo aplicable el de su artículo 7° —"Interceptación de datos informáticos"—,[45] que integra su capítulo IV —"Delitos informáticos

---

de tres a seis años, la servidora o servidor militar o policial que, utilizando cualquier medio electrónico, informático o afín, obtenga información clasificada de conformidad con la ley. La misma pena será aplicable a quien destruyere o inutilizare este tipo de información.

Si la divulgación o la utilización fraudulenta son realizadas por cualquier persona o personas encargadas de la custodia o utilización legítima de la información, éstas serán sancionadas con el máximo de la pena".

(43) El texto introducido al CP es el siguiente: "Art. 146 c. Interceptación de datos. El que, sin autorización y utilizando medios técnicos: 1° obtuviere para sí o para un tercero, datos en sentido del art. 146 b, inc. 2, no destinados para él; 2° diera a otro una transferencia no pública de datos; o 3° transfiriera la radiación electromagnética de un equipo de procesamiento de datos, será castigado con pena privativa de libertad de hasta dos años o multa, salvo que el hecho sea sancionado por otra disposición con una pena mayor".

(44) Cuya parte pertinente reza: "1° El que revelara un secreto ajeno: 1. llegado a su conocimiento en su actuación como, a) médico, dentista o farmacéutico; b) abogado, notario o escribano público, defensor en causas penales, auditor o asesor de Hacienda; c) ayudante profesional de los mencionados anteriormente o persona formándose con ellos en la profesión; o 2. respecto del cual le incumbe por ley o en base a una ley una obligación de guardar silencio, será castigado con pena privativa de libertad de hasta un año o con multa. ...3° Cuando el secreto sea de carácter industrial o empresarial, la pena privativa de libertad podrá ser aumentada hasta tres años. Será castigada también la tentativa".

(45) Dice: "El que a través de las tecnologías de la información o de la comunicación, intercepta datos informáticos en transmisiones no públicas, dirigidas a un sistema informático, originadas en un sistema informático o efectuadas dentro del mismo, incluidas las emisiones electromagnéticas provenientes de un sistema informático que transporte dichos datos informáticos, será reprimido con pena privativa de libertad no menor de tres ni mayor de seis años.

contra la intimidad y el secreto de las comunicaciones"—. Se complementa con el artículo 6°,[46] que pune el "Tráfico ilegal de datos".

b.8 **Uruguay**: por ley 18.383 —del 17de octubre de 2008—, se modificó el artículo 217[47] del CP, a partir del que se pena al atentado contra la regularidad de las telecomunicaciones. A su vez, por ley 18.515 —del 26 de junio de 2009—, se volvieron a modificar los artículos del CP relativos a la protección de los medios de comunicación. Además, puede acotarse que por ley 18.494 —del 5 de junio de 2009— se modificó el régimen sobre prevención y control de lavados de activos y del financiamiento del terrorismo, regulándose lo relativo a las vigilancias electrónicas "legales".

b.9 **Venezuela**: prevé el espionaje informático en el artículo 11[48] de su LECDI del año 2001. Tiene, además, una figura de "hurto" (art. 13)[49] y, en el citado artículo 21, referido a la violación de la privacidad de las comunicaciones; sanciona al que mediante el uso de las tecnologías de la información capture o interfiera cualquier mensaje de datos o señal de transmisión o comunicación ajena con pena de dos a seis años y multa de doscientas a seiscientas unidades tributarias.

La pena privativa de libertad será no menor de cinco ni mayor de ocho años cuando el delito recaiga sobre información clasificada como secreta, reservada o confidencial de conformidad con las normas de la materia.

La pena privativa de libertad será no menor de ocho ni mayor de diez años cuando el delito comprometa la defensa, la seguridad o la soberanía nacionales".

(46) Dice: "El que crea, ingresa o utiliza indebidamente una base de datos sobre una persona natural o jurídica, identificada o identificable, para comercializar, traficar, vender, promover, favorecer o facilitar información relativa a cualquier ámbito de la esfera personal, familiar, patrimonial, laboral, financiera y otro de naturaleza análoga, creando o no perjuicio, será reprimido con pena privativa de libertad no menor de tres ni mayor de cinco años".

(47) Su texto actual: "El que, de cualquier manera, atentare contra la regularidad de las comunicaciones telefónicas, telegráficas o inalámbricas, poniendo en peligro la seguridad de los transportes públicos, será castigado con tres meses de prisión a tres años de penitenciaría".

(48) Dice que toda persona: "... que indebidamente obtenga, revele o difunda la data o información contenidas en un sistema que utilice tecnologías de la información o en cualesquiera de sus componentes, será penada con prisión de tres a seis años y multa de trescientas a seiscientas unidades tributarias. La pena se aumentará de un tercio a la mitad, si el delito previsto en el presente artículo se cometiere con el fin de obtener algún tipo de beneficio para sí o para otro.

El aumento será de la mitad a dos tercios, si se pusiere en peligro la seguridad del Estado, la confiabilidad de la operación de las instituciones afectadas o resultare algún daño para las personas naturales o jurídicas, como consecuencia de la revelación de las informaciones de carácter reservado".

(49) Su texto: "El que a través del uso de tecnologías de la información, acceda, intercepte, interfiera, manipule o use de cualquier forma un sistema o medio de comunicación para apoderarse de bienes o valores tangibles o intangibles de carácter patrimonial sustrayéndolos a su tenedor, con el fin de procurarse un provecho económico para sí o para otro, será sancionado con prisión de dos a seis años y multa de doscientas a seiscientas unidades tributarias".

c. En cambio no se advierten normas específicas en **Bolivia**, ya que su CP de 1997 solo tipifica las tradicionales violaciones de secretos (arts. 300/302).

2.3. Atentados contra la integridad de los datos (art. 4)

> "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, la conducta de dañar, borrar, deteriorar, alterar o suprimir dolosamente y sin autorización los datos informáticos.
>
> 2. Las Partes podrán reservarse el derecho a exigir que el comportamiento descrito en el párrafo primero ocasione daños que puedan calificarse de graves". (50)

a. En este caso, resaltan de la Mata Barranco y Hernández Díaz, se otorga protección directa únicamente a los elementos lógicos de los sistemas informáticos sin especificar cómo debe ser la modalidad de ataque, contemplando conductas que no implican necesariamente la destrucción de un objeto sino, simplemente, la variación del contenido de un dato. (51)

Vale enfatizar que la propuesta de tipificación de las conductas que importan atentados contra la integridad de datos admite ese límite exigiendo que, para la intervención penal, se trate de la producción de daños graves. Ésto, para aquellos países imbuidos de la tradicional dogmática continental europea, es una fórmula que les permite tipificar en forma congruente con el principio de lesividad y dejar afuera del derecho penal las afectaciones bagatelares o menores. Como destaca Morales García tomando como ejemplo del artículo 260 del CPE, en muchos casos se trasluce en la adopción de una cuantía económica mínima como perjuicio para expresar penalmente el desvalor de la conducta. El problema puede presentarse

---

(50) Esta propuesta típica fue reafirmada mediante la Decisión Marco 2005/222/JAI del Consejo, de 24 de febrero de 2005, relativa a los ataques contra los sistemas de información, con esta redacción: "Artículo 4. Intromisión ilegal en los datos. Cada Estado miembro adoptará las medidas necesarias para que el acto intencionado, cometido sin autorización, de borrar, dañar, deteriorar, alterar, suprimir o hacer inaccesibles datos informáticos contenidos en un sistema de información sea sancionable como infracción penal, al menos en los casos que no sean de menor gravedad". A su vez, ha sido sustituido por el art. 5° de la Directiva 2013/40/UE del Parlamento Europeo y del Consejo de 12 de agosto de 2013 relativa a los ataques contra los sistemas de información, "Interferencia ilegal en los datos", manteniendo similar redacción.

(51) De la Mata Barranco, Norberto J.; Hernández Díaz, Leyre, "El delito de daños informáticos: una tipificación defectuosa", en *Estudios Penales y Criminológicos*, Servicio de Publicaciones de la Universidad de Santiago de Compostela, vol. XXIX, 2009, p. 322.

al momento de precisar qué se debe tomar como referencia para la valoración del daño: ¿el valor en sí mismo del dato informático? Y, si es así, ¿cómo lo mensuro?, ¿se tomará el valor de cambio del dato informático? Si fuera de ese modo, ¿qué pasa con la destrucción de un dato respecto del que existe copia de seguridad, en cuyo caso el valor de cambio permanecería inalterado?, ¿sería un caso de tentativa posible y punible, o imposible e impune?(52) Puede anticiparse que en ninguna de las normas sudamericanas que seguidamente se indicarán se ha optado por fijar una cuantía para deslindar entre un daño delictivo y otro contravencional.

b. Al bucear en las legislaciones regionales, puede advertirse la presencia de tipos específicos en:

b.1 **Argentina**: donde la reforma por ley 26.388 —año 2008— incorporó el daño en datos, documentos, programas o sistemas informáticos mediante un segundo párrafo agregado al artículo 183(53) y la sustitución del artículo 184(54) del CP.

Previamente, había sido normada la "alteración dolosa de registros fiscales" en el artículo 12(55) de la vigente Ley Penal Tributaria y Previsional Nro. 24.769 —año 1997—. Luego, se amplió la tipificación por la incorporación de la "alteración dolosa de sistemas informáticos o equipos electrónicos" como artículo 12 *bis*,(56) por ley 26.735 de fines de 2011.

---

(52) Morales García, *op. cit.*, p. 30.

(53) Dice: "… En la misma pena incurrirá el que alterare, destruyere o inutilizare datos, documentos, programas o sistemas informáticos; o vendiere, distribuyere, hiciere circular o introdujere en un sistema informático, cualquier programa destinado a causar daños" (2° párr.).

(54) Con este texto: "La pena será de tres (3) meses a cuatro (4) años de prisión, si mediare cualquiera de las circunstancias siguientes: (...) 5. Ejecutarlo en archivos, registros, bibliotecas, museos o en puentes, caminos, paseos u otros bienes de uso público; o en tumbas, signos conmemorativos, monumentos, estatuas, cuadros u otros objetos de arte colocados en edificios o lugares públicos; o en datos, documentos, programas o sistemas informáticos públicos; 6. Ejecutarlo en sistemas informáticos destinados a la prestación de servicios de salud, de comunicaciones, de provisión o transporte de energía, de medios de transporte u otro servicio público".

(55) El tipo del régimen especial dice: "Será reprimido con prisión de dos a seis años, el que de cualquier modo sustrajere, suprimiere, ocultare, adulterare, modificare o inutilizare los registros o soportes documentales o informáticos del fisco nacional, relativos a las obligaciones tributarias o de recursos de la seguridad social, con el propósito de disimular la real situación fiscal de un obligado".

(56) Con esta redacción: "Será reprimido con prisión de uno (1) a cuatro (4) años, el que modificare o adulterare los sistemas informáticos o equipos electrónicos, suministrados u homologados por el fisco nacional, provincial o de la Ciudad Autónoma de Buenos Aires, siempre y cuando dicha conducta fuere susceptible de provocar perjuicio y no resulte un delito más severamente penado".

La inserción o la inducción a la inserción ilegítima de datos en un archivo de datos personales comenzó a punirse con la modificación del CP por la LPDP del año 2000. Pero el artículo 157 *bis* fue nuevamente reformado por la citada ley 26.388; quedando como su inc. 3°,[57] que agrava la conducta cuando es desplegada por un funcionario público.

La protección de datos personales se complementa, más allá de lo que requiere Budapest, con una actualizada sección dedicada a la violación de secretos. En el citado art. 157 *bis,* inc. 2° se pune también al que "Ilegítimamente proporcionare o revelare a otro información registrada en un archivo o en un banco de datos personales cuyo secreto estuviere obligado a preservar por disposición de la ley". A su vez, la simple revelación de secretos del art. 157[58] también fue actualizada por ley 27.388 incluyendo la palabra "datos".

b.2 **Bolivia**: la modificación, supresión o inutilización de datos está contemplada en el ya transcripto artículo 363 *ter*[59] del CP de 1997.

b.3 **Brasil**: presenta una situación similar a la Argentina antes de la reforma de 2008 en relación al delito de daño. La discusión giraba alrededor del artículo 163 del CP de 1940,[60] por lo que podía considerarse sin tipo expreso. Pero debe ahora tenerse presente la posible concurrencia para subsumir algunos casos del art. 154-A del CPB conforme a la ley 12.737; así, la destrucción de daños o informaciones en dispositivo informático.

También a semejanza del caso argentino, por ley 9983 —año 2000—, se introdujo un tipo de violación de secretos calificado por vía de la modificación de los artículos 153 y 325 del CPB. En efecto, el artículo 153, parág. 1°, letra "A" —"Violación de secreto"—, prevé pena de detención de 1 a 4 años y multa para el que divulgue, sin justa causa, informaciones secretas o reservadas, así definidas por ley, contenidas en sistemas informáticos o bancos de datos de la Administración Pública. Mientras que el art. 325, parágs. 1° y 2° —"Violación de secreto funcional"—, prevé pena de detención de 6 meses a 2 años o multa para el que permitiere o facilitare

(57) El segmento pertinente del art. 157 *bis* dice: "Será reprimido con la pena de prisión de un (1) mes a dos (2) años el que: (…) 3. Ilegítimamente insertare o hiciere insertar datos en un archivo de datos personales. Cuando el autor sea funcionario público sufrirá, además, pena de inhabilitación especial de un (1) a cuatro (4) años".

(58) Ahora dice: "Será reprimido con prisión de un (1) mes a dos (2) años e inhabilitación especial de un (1) a cuatro (4) años, el funcionario público que revelare hechos, actuaciones, documentos o datos, que por ley deben ser secretos".

(59) Su texto: "Alteración, acceso y uso indebido de datos informáticos. El que sin estar autorizado se apodere, acceda, utilice, modifique, suprima o inutilice, datos almacenados en una computadora o en cualquier soporte informático, ocasionando un perjuicio al titular de la información, será sancionado con prestación de trabajo hasta un año o multa de hasta doscientos días".

(60) Dice: "art. 163. *Destruir, inutilizar ou deteriorar coisa alheia: Pena – detenção, de 1 (um) a 6 (seis) meses, ou multa"*.

mediante atribución, provisión y préstamo de clave o cualquier otra forma, el acceso de persona no autorizada a sistemas informáticos o banco de datos de la Administración Pública; o utilizare, indebidamente, el acceso restringido. Califica por daño a la Administración Pública o a otro, con pena de reclusión de 2 a 6 años y multa.

Dentro del marco de los delitos contra la Administración Pública, la ley citada agregó al CPB los artículos 313-A[61] y 313-B,[62] con los que vino a tutelar la seguridad de los sistemas de información de aquélla exclusivamente. Es decir, sus previsiones no son aplicables a los sistemas de informaciones de entidades particulares o privadas.

Por ley 12.737 —año 2012— se ha incorporado la protección de los secretos comerciales o industriales, la información secreta definida por ley y las comunicaciones electrónicas privadas mediante la reforma introducida al artículo 154-A del CP —ley 2848 del 7 de diciembre de 2004—. Además, por ley 12.737, un nuevo parágrafo (parág. 3º) prevé pena de reclusión de seis meses a dos años y multa, siempre que no constituya un delito más grave. Se agrava de uno a dos tercios si media divulgación, comercialización o transmisión a terceros a cualquier título de los datos obtenidos (parág. 4º).

b.4 **Chile**: la ley 19.223 —año1993— contempla el "Sabotaje informático" en su artículo 1°.[63] El primer párrafo describe la conducta básica, mientras que el segundo agrava cuando se afectan datos contenidos en un sistema.

b.5 **Colombia**: su CP, reformado en 2009 por ley 1273, en materia de integridad de datos, prevé el "daño informático" en el artículo 269D.[64] A su vez, en el artículo 269F[65] se pune la "violación de datos personales" y

(61) Su redacción: *"Inserir ou facilitar, o funcionário autorizado, a inserção de dados falsos, alterar ou excluir indevidamente dados corretos nos sistemas informatizados ou bancos de dados da Administração Pública com o fim de obter vantagem indevida para si ou para outrem ou para causar dano: Pena- reclusão de 2(dois) a 12 (doze) anos e multa"*.

(62) Dice: *"Modificar ou alterar, o funcionário, sistema de informações ou programa de informática sem autorização ou solicitação de autoridade competente"*. Se prevé pena de 3 meses a dos años de detención y multa. Además, califica agravando la pena de un tercio a la mitad si de ello resulta daño para la administración pública o un administrado (parágrafo único final).

(63) Su redacción: "El que maliciosamente destruya o inutilice un sistema de tratamiento de información o sus partes o componentes, o impida, obstaculice o modifique su funcionamiento, sufrirá la pena de presidio menor en su grado medio a máximo. Si como consecuencia de estas conductas se afectaren datos contenidos en un sistema, se aplicará la pena señalada en el inciso anterior, en su grado máximo".

(64) Su texto: "El que, sin estar facultado para ello, destruya, dañe, borre, deteriore, altere o suprima datos informáticos, o un sistema de tratamiento de información o sus partes o componentes lógicos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes".

(65) Dice: "El que, sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique o emplee códigos personales, datos personales contenidos en ficheros, archivos,

en el artículo 269G[66] la "suplantación de sitios web para capturar datos personales".

b.6 **Ecuador**: por ley 2002-67 se sustituyó el texto del artículo 262[67] de su Código Penal, incluyendo la destrucción o supresión dolosa de programas, datos, bases de datos, etc.; en caso de su comisión por empleado público o persona encargada de su guarda. Además, por la misma ley se agregó, a continuación del artículo 415 del CPE, un artículo sin número,[68] en cuyo primer párrafo tipifica los daños informáticos y, agrava cuando recae sobre sistema vinculado a servicios públicos o defensa en el segundo.

b.7 **Paraguay**: pune mediante el artículo 174[69] de su CP la "alteración de datos". Encuentra complemento en el siguiente, rebautizado por ley 4439 del

---

bases de datos o medios semejantes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes".

(66) Su texto: "El que con objeto ilícito y sin estar facultado para ello, diseñe, desarrolle, trafique, venda, ejecute, programe o envíe páginas electrónicas, enlaces o ventanas emergentes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con pena más grave.

En la misma sanción incurrirá el que modifique el sistema de resolución de nombres de dominio, de tal manera que haga entrar al usuario a una IP diferente en la creencia de que acceda a su banco o a otro sitio personal o de confianza, siempre que la conducta no constituya delito sancionado con pena más grave.

La pena señalada en los dos incisos anteriores se agravará de una tercera parte a la mitad, si para consumarlo el agente ha reclutado víctimas en la cadena del delito".

(67) Su texto actual: "Serán reprimidos con tres a seis años de reclusión menor, todo empleado público y toda persona encargada de un servicio público, que hubiere maliciosa y fraudulentamente, destruido o suprimido documentos, títulos, programas, datos, bases de datos, información o cualquier mensaje de datos con-tenido en un sistema de información o red electrónica, de que fueren depositarios, en su calidad de tales, o que les hubieren sido encomendados en razón de su cargo".

(68) Dice: "art. (...) (1). (Ag. por art. 61, L. 2002-67, R.O. 557-S, 17-IV-2002). Daños informáticos. El que dolosamente, de cualquier modo o utilizando cualquier método, destruya, altere, inutilice, suprima o dañe, de forma temporal o definitiva, los programas, datos, bases de datos, información o cualquier mensaje de datos contenido en un sistema de información o red electrónica, será reprimido con prisión de seis meses a tres años y multa de 60 a 150 dólares de los EUN.

La pena de prisión será de tres a cinco años y multa de 200 a 600 dólares…, cuando se trate de programas, datos, bases de datos, información o cualquier mensaje de datos contenido en un sistema de información o red electrónica, destinada a prestar un servicio público o vinculada con la defensa nacional".

(69) Su texto: "Artículo 174. Alteración de datos. 1) El que lesionando el derecho de disposición de otro sobre datos los borrara, suprimiera, inutilizara o cambiara, será castigado con pena privativa de libertad de hasta dos años o con multa. 2) En estos casos, será castigada también la tentativa. 3) Como datos, en el sentido del inc. 1, se entenderán sólo aquellos

año 2011 como "Sabotaje a sistemas informáticos"[70] que, conforme el texto actual, ya no exige que los datos sean de importancia vital y se incorporan a los particulares como objetos de posible ataque.

A su vez, ya en versión original del código, se dedicaron dos artículos a los hechos punibles contra la prueba documental en los que se alude a la alteración de datos y conectan expresamente con el inc. 3° del artículo 174, antes citado. Se trata de los artículos 248[71] y 249.[72]

b.8 **Perú**: la alteración, daño y destrucción de base de datos, se incorporó al CP de 1991 por ley 27.309 el 17 de julio de 2000 como nuevo artículo 207-B. Recibió los agravantes del artículo 207-C. Luego, fueron derogados por la "disposición complementaria derogatoria única" de la ley 30.096 de 2013, cuyo artículo 3° —"Atentado contra la integridad de datos informáticos"— es el tipo actualmente regente.[73]

Además, en general, la violación de la intimidad está tipificada en el artículo 154 del CP y se prevé autónomamente la punición del uso indebido de archivos computarizados (art. 157).[74] El tipo referido a la interferencia telefónica

---

que sean almacenados o se transmitan electrónica o magnéticamente, o en otra forma no inmediatamente visible".

(70) La nueva redacción es: "Artículo 175. 1° El que obstaculizara un procesamiento de datos de un particular, de una empresa, asociación o de una entidad de la administración pública, mediante: 1) un hecho punible según el art. 174, inc. 1; o 2) la destrucción, inutilización, sustracción o alteración de una instalación de procesamiento de datos, de una unidad de almacenamiento o de otra de sus partes componentes indispensable. será castigado con pena privativa de libertad de hasta cinco años o con multa. 2° En estos casos será castigada también la tentativa".

(71) Su texto: "Artículo 248. Alteración de datos relevantes para la prueba. 1) El que con la intención de inducir al error en las relaciones jurídicas, almacenara o adulterara datos en los términos del art. 174, inc. 3, relevantes para la prueba de tal manera que, en caso de percibirlos se presenten como un documento no auténtico, será castigado con pena privativa de libertad de hasta cinco años o con multa. 2) En estos casos será castigada también la tentativa. 3) En lo pertinente se aplicará también lo dispuesto en el art. 246, inc. 4".

(72) Dice: "Artículo 249. Equiparación para el procesamiento de datos. La manipulación que perturbe un procesamiento de datos conforme al art. 174, inc. 3, será equiparada a la inducción al error en las relaciones jurídicas".

(73) Dice: "El que, a través de las tecnologías de la información o de la comunicación, introduce, borra, deteriora, altera, suprime o hace inaccesibles datos informáticos, será reprimido con pena privativa de libertad no menor de tres ni mayor de seis años y con ochenta a ciento veinte días multa".

(74) Su texto: "El que, indebidamente, organiza, proporciona o emplea cualquier archivo que tenga datos referentes a las convicciones políticas o religiosas y otros aspectos de la vida íntima de una o más personas, será reprimido con pena privativa de libertad no menor de uno ni mayor de cuatro años.
Si el agente es funcionario o servidor público y comete el delito en ejercicio del cargo, la pena será no menor de tres ni mayor de seis años e inhabilitación conforme al art. 36, incs. 1, 2 y 4".

(art. 162)[75] ha sido expresamente modificado conforme la disposición complementaria modificatoria "cuarta" de la ley 30.096 mencionada.

b.9 **Venezuela**: en el capítulo I de su LECDI de 2001 —"De los delitos contra los sistemas que utilizan tecnologías de la información"—, se prevé el sabotaje o daño a sistemas, tanto en su forma dolosa (art. 7°);[76] como culposa (art. 8°);[77] considerándose agravada la conducta de acceso indebido o sabotaje cuando se trate de sistemas protegidos destinados a funciones públicas o con información personal o patrimonial de personas naturales o jurídicas en el ya referido artículo 9°. Vale enfatizar que, mientras el Convenio reclama la punición de la conducta a título doloso; la legislación venezolana va mucho más allá al punir también daños imprudentes.

En el capítulo III —"De los delitos contra la privacidad de las personas y de las comunicaciones"— de la LECDI de 2001, hay otras normas protectoras, tanto de la integridad como del secreto de los datos personales: los delitos de violación de la privacidad de la data o información de carácter personal (art. 20);[78]

(75) El nuevo texto dice: "El que, indebidamente, interfiere o escucha una conversación telefónica o similar será reprimido con pena privativa de libertad no menor de tres ni mayor de seis años.

Si el agente es funcionario público, la pena privativa de libertad será no menor de cuatro ni mayor de ocho años e inhabilitación conforme al art. 36, incs. 1, 2 y 4.

La pena privativa de libertad será no menor de cinco ni mayor de ocho años cuando el delito recaiga sobre infracción clasificada como secreta, reservada o confidencial de conformidad con las normas de la materia. La pena privativa de libertad será no menor de ocho años ni mayor de diez años cuando el delito comprometa la defensa, la seguridad o la soberanía nacionales".

(76) Dice: "Artículo 7. Sabotaje o daño a sistemas. El que destruya, dañe, modifique o realice cualquier acto que altere el funcionamiento o inutilice un sistema que utilice tecnologías de información o cualquiera de los componentes que lo conforman, será penado con prisión de cuatro a ocho años y multa de cuatrocientas a ochocientas unidades tributarias.

Incurrirá en la misma pena quien destruya, dañe, modifique o inutilice la data o la información contenida en cualquier sistema que utilice tecnologías de información o en cualquiera de sus componentes. La pena será de cinco a diez años de prisión y multa de quinientas a mil unidades tributarias, si los efectos indicados en el presente artículo se realizaren mediante la creación, introducción o transmisión, por cualquier medio, de un virus o programa análogo".

(77) Se transcribe. "Artículo 8. Sabotaje o daño culposo. Si el delito previsto en el artículo anterior se cometiere por imprudencia, negligencia, impericia o inobservancia de las normas establecidas, se aplicará la pena correspondiente según el caso, con una reducción entre la mitad y dos tercios".

(78) Tiene la siguiente redacción: "Artículo 20. Violación de la privacidad de la data o información de carácter personal. Toda persona que intencionalmente se apodere, utilice, modifique o elimine por cualquier medio, sin el consentimiento de su dueño, la data o información personales de otro o sobre las cuales tenga interés legítimo, que estén incorporadas en un computador o sistema que utilice tecnologías de información, será penada con prisión de dos a seis años y multa de doscientas a seiscientas unidades tributarias.

La pena se incrementará de un tercio a la mitad si como consecuencia de los hechos anteriores resultare un perjuicio para el titular de la data o información o para un tercero".

violación de la privacidad de las comunicaciones (art. 21)[79] y la revelación indebida de data o información de carácter personal (art. 22).[80]

La siguiente norma de la Constitución de 1999 opera de pauta interpretativa al establecer, con respecto a la posibilidad de grabar comunicaciones y emplearlas como medios probatorios en juicio, lo siguiente:

"Se garantiza el secreto e inviolabilidad de las comunicaciones privadas en todas sus formas. No podrán ser interferidas sino por orden de un tribunal competente, con el cumplimiento de las disposiciones legales y preservándose el secreto de lo privado que no guarde relación con el correspondiente proceso"(art. 48).

c. En cambio, no se ha producido aún una reforma que se ocupe de esta propuesta típica en **Uruguay**. Por lo que allí se mantendría la discutida situación de la capacidad de rendimiento para subsumir estas conductas en las tradicionales figuras de "daño". Puede acotarse que allí se ha sancionado el 11 de agosto de 2008 la Ley 18331 de Protección de Datos Personales, cuyo artículo 1° comienza reconociéndoles estatus de derecho humano fundamental —"el derecho a la protección de datos personales es inherente a la persona humana…"—, aplicable por extensión a las personas jurídicas (ver art. 2º). Entre otros principios que rigen la tutela de datos personales está el de reserva (art. 11), enfatizado por la remisión al artículo 302[81] del CP en cuanto a la estrecha guarda del secreto profesional.

2.4. Atentados contra la integridad del sistema (art. 5)

"Las Partes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias para prever como infracción penal, conforme a su derecho interno, la obstaculización grave, cometida de

(79) En lo pertinente, ya que lo contempla entre otras conductas, sanciona al que mediante el uso de las tecnologías de la información reproduzca, modifique o elimine cualquier mensaje de datos o señal de transmisión o comunicación ajena, con pena de dos a seis años y multa de doscientas a seiscientas unidades tributarias.

(80) Con la siguiente redacción: "Artículo 22. Revelación indebida de data o información de carácter personal. Quien revele, difunda o ceda, en todo o en parte, los hechos descubiertos, las imágenes, el audio o, en general, la data o información obtenidos por alguno de los medios indicados en los arts. 20 y 21, será sancionado con prisión de dos a seis años y multa de doscientas a seiscientas unidades tributarias.

Si la revelación, difusión o cesión se hubieren realizado con un fin de lucro, o si resultare algún perjuicio para otro, la pena se aumentará de un tercio a la mitad".

(81) Dice: "El que, sin justa causa, revelare secretos que hubieran llegado a su conocimiento, en virtud de su profesión, empleo o comisión, será castigado, cuando el hecho causare perjuicio, con multa de 100 U.R. (cien unidades reajustables) a 600 U.R. (seiscientas unidades reajustables)".

forma dolosa y sin autorización, del funcionamiento de un sistema informático, mediante la introducción, transmisión, daño, borrado, deterioro, alteración o supresión de datos informáticos".[82]

a. Al considerar no ya las afectaciones a la integridad de datos, sino del sistema; pueden verificarse tipos específicos en:

a.1 **Argentina**: en el marco de la reforma generalizada del CP por vía de la ley 26.388, en materia de "Delitos contra la seguridad de los medios de transporte y de comunicación", se ha sustituido el artículo dedicado a la "Interrupción o resistencia al restablecimiento de las comunicaciones" (art. 197 del CP),[83] dotándolo de una amplitud comprensiva de los sistemas informáticos con relación al "entorpecimiento" como modalidad típica que guarda correspondencia con la "obstaculización grave".

Complementariamente, puede recordarse que por ley 25.891 —año 2004—, que regula los servicios móviles de telefonía y comunicación, se introdujeron los tipos de alteración, reemplazo, duplicación o modificación de número de línea o de serie electrónico o mecánico de un equipo terminal o de un módulo de identificación removible (MIR) en equipos terminales provistos; de modo que pueda ocasionar perjuicio al titular o usuario del terminal celular o terceros (art. 10), e idéntica conducta respecto de tarjeta de telefonía o el acceso a los códigos informáticos de habilitación de créditos del servicio de comunicaciones móviles (SCM) para aprovecharse ilegítimamente (art. 11). También se tipifica la adquisición o uso a sabiendas de la procedencia ilegítima de terminales celulares, MIR o tecnología similar que la reemplace en el futuro (art. 12). Las conductas se agravan si fueron cometidas con ánimo de lucro o como medio para perpetrar otro delito (art. 13), o por dependientes de empresas licenciatarias de SCM o quien posee en el desempeño de sus funciones acceso a las facilidades técnicas de aquellas (art. 14).

a.2 **Brasil**: ha consagrado en el marco de la protección de los derechos del consumidor dos tipos penales relativos a la información almacenada de conteni-

(82) Esta propuesta típica, ampliando al incluir la directa interrupción, fue reafirmada mediante la Decisión Marco 2005/222/JAI del Consejo, de 24 de febrero de 2005, relativa a los ataques contra los sistemas de información, con esta redacción: "Artículo 3. Intromisión ilegal en los sistemas de información. Cada Estado miembro adoptará las medidas necesarias para que el acto intencionado, cometido sin autorización, de obstaculizar o interrumpir de manera significativa el funcionamiento de un sistema de información, introduciendo, transmitiendo, dañando, borrando, deteriorando, alterando, suprimiendo o haciendo inaccesibles datos informáticos, sea sancionable como infracción penal, al menos en los casos que no sean de menor gravedad". A su vez, ha sido sustituido por el art. 4 de la Directiva 2013/40/UE del Parlamento Europeo y del Consejo de 12 de agosto de 2013 relativa a los ataques contra los sistemas de información, "Interferencia ilegal en los sistemas de información", manteniendo una redacción similar.

(83) Dice: "Será reprimido con prisión de seis (6) meses a dos (2) años, el que interrumpiere o entorpeciere la comunicación telegráfica, telefónica o de otra naturaleza o resistiere violentamente el restablecimiento de la comunicación interrumpida".

do privado. Se trata de los artículos 72 y 73 del Código de Defensa del Consumidor, ley 8079/90. El primero pune con detención de seis meses a un año o multa el impedir o dificultar el acceso del consumidor a las informaciones que constan en bancos de datos, fichas o registros, referentes a su persona, mientras que el segundo lo hace con detención de uno a seis meses o multa respecto de la omisión del agente que no procede a la corrección inmediata de la tal información del consumidor que sabe o debería saber inexacta.

Por ley 12.737, del 30 de noviembre de 2012, se modificó el artículo 266[84] del CP. Se incluyó dentro de las tipicidades de interrupción o perturbación de servicio la que se brinda por medio telemático o de información de utilidad pública, o la que impida o dificulte su restablecimiento (parág. 1°).

a.3 **Colombia**: incorporó al CP la figura de obstaculización ilegítima de sistema informático o red de telecomunicación (art. 269B)[85] en el marco de reforma por ley 1273 del año 2009.

a.4 **Ecuador**: a partir de la reforma introducida por ley 2002-37 se agregó, a continuación del artículo 415 del CPE, un artículo sin número,[86] cuyo segundo segmento tipifica la conducta de alteración o inutilización de las instalaciones físicas necesarias para la transmisión, recepción o procesamiento de mensajes de datos. La interrupción o violenta resistencia al restablecimiento de las comunicaciones está contemplada en el artículo 422[87] del CPE.

a.5 **Paraguay**: la obstaculización en un procesamiento de datos de un particular, de una empresa, asociación o de una entidad de la administración pública; así como la destrucción, inutilización, sustracción o alteración de una instalación de procesamiento de datos, de una unidad de almacenamiento o de otra de sus partes componentes indispensable son contempladas en el tipo de sabotaje informático del artículo 175 del CP de 1997, ya transcripto.

---

(84) Su texto: "*art. 266 - Interromper ou perturbar serviço telegráfico, radiotelegráfico ou telefônico, impedir ou dificultar-lhe o restabelecimento: Pena - detenção, de um a três anos, e multa. § 1º Incorre na mesma pena quem interrompe serviço telemático ou de informação de utilidade pública, ou impede ou dificulta-lhe o restabelecimento.*
§ 2º Aplicam-se as penas em dobro se o crime é cometido por ocasião de calamidade pública".

(85) Dice: "El que, sin estar facultado para ello, impida u obstaculice el funcionamiento o el acceso normal a un sistema informático, a los datos informáticos allí contenidos, o a una red de telecomunicaciones, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con una pena mayor".

(86) Tiene la siguiente redacción: "art. (...) (2). Si no se tratare de un delito mayor, la destrucción, alteración o inutilización de la infraestructura o instalaciones físicas necesarias para la transmisión, recepción o procesamiento de mensajes de datos, será reprimida con prisión de 8 meses a 4 años y multa de 200 a 600 dólares…".

(87) Su parte pertinente dice: "Será reprimido con prisión de seis meses a dos años el que interrumpiere la comunicación postal, telegráfica, telefónica, radiofónica o de otro sistema, o resistiere violentamente al restablecimiento de la comunicación interrumpida…"(art. 422).

Por la reforma de 2011, ley 4439, junto al artículo 174, es delito de instancia privada (art. 175b).

a.6 **Perú**: la alteración, daño y destrucción de sistema, red o programa de computadoras se había incorporado al CP de 1991 por ley 27.309 del 17 de julio de 2000 (art. 207-B). Eran aplicables los agravantes del artículo 207-C. Fueron derogados por la "disposición complementaria derogatoria única" de la ley 30096 de 2013 sobre "Delitos informáticos", que prevé el "Atentado contra la integridad de sistemas informáticos" (art. 4°).(88)

a.7 **Venezuela**: el artículo 6° de la LECDI, ya citado y transcripto porque tipifica una variada alternativa de conductas, pena la interferencia de sistema que utilice tecnologías de la información; además, el evocado artículo 7° sanciona la directa inutilización. Estas conductas también serían punibles a título culposo conforme la remisión que formula el artículo 8°. A su vez, el artícu-lo 21 pena al que mediante el uso de las tecnologías de la información desvía cualquier mensaje de datos o señal de transmisión o comunicación ajena.

b. Por su lado, los restantes estados —**Bolivia, Chile y Uruguay**— no han sancionado figuras receptivas de la propuesta del Convenio.

2.5. Abuso de equipos e instrumentos técnicos (art. 6)

"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, venta, obtención para su utilización, importación, difusión u otras formas de puesta a disposición:

- de un dispositivo, incluido un programa informático, principalmente concebido o adaptado para permitir la comisión de una de las infracciones establecidas en los arts. 2 a 5 arriba citados;
- 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 arts. 2 a 5; y

b. la posesión de alguno de los elementos descritos en los parágrafos (a) (1) o (2) con la intención de utilizarlos como medio para

(88) Su texto: "El que, a través de las tecnologías de la información o de la comunicación, inutiliza, total o parcialmente, un sistema informático, impide el acceso a este, entorpece o imposibilita su funcionamiento o la prestación de sus servicios, será reprimido con pena privativa de libertad no menor de tres ni mayor de seis años y con ochenta a ciento veinte días multa".

> cometer alguna de las infracciones previstas en los arts. 2-5. Los Estados podrán exigir en su derecho interno que concurra un determinado número de elementos para que nazca responsabilidad penal.
>
> 2. 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 párr. 1 no persigan la comisión de una infracción prevista en los arts. 2 a 5 del presente Convenio, como en el caso de ensayos autorizados o de la protección de un sistema informático.
>
> 3. Las Partes podrán reservarse el derecho de no aplicar el párr. 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 parágrafo 1 (a) (2)".[89]

a. En este artículo el Convenio propone la tipificación de una etapa previa al uso con relación a los dispositivos concebidos o adaptados para permitir alguna de las conductas descriptas en los anteriores o de contraseñas, códigos de acceso o datos que lo permitan a todo o parte de un sistema informático: la de su producción, venta, obtención para su utilización, importación, difusión u otras formas de puesta a disposición.

También la simple posesión de aquellos elementos con intención de uso para cometer alguna de las infracciones de los arts. 2 a 5, aunque en este caso se indica posible limitación vía exigencia local de la concurrencia de un determinado número de elementos para que nazca responsabilidad penal. En particular, se trata de una directriz expansiva del Convenio que

(89) Si bien la DM del año 2005 no previó equivalente, su sustituta Directiva 2013/40/UE del Parlamento Europeo y del Consejo de 12 de agosto de 2013 relativa a los ataques contra los sistemas de información, ha reafirmado la propuesta típica en su artículo 7°, con un texto más económico que dice: "Los Estados miembros adoptarán las medidas necesarias para garantizar que la producción intencional, venta, adquisición para el uso, importación, distribución u otra forma de puesta a disposición de los siguientes instrumentos, sin autorización y con la intención de que sean utilizados con el fin de cometer cualquiera de las infracciones mencionadas en los arts. 3 a 6, sea sancionable como infracción penal, al menos en los casos que no sean de menor gravedad:

a) un programa informático, concebido o adaptado principalmente para cometer una infracción de las mencionadas en los arts. 3 a 6;
b) una contraseña de ordenador, un código de acceso o datos similares que permitan acceder a la totalidad o a una parte de un sistema de información".

viene a postular la criminalización de la simple posesión de los llamados *hacking tools* u otro software peligroso, como resalta con acierto Anarte Borrallo, quien la menciona como ejemplo de lo que puede resultar en algún caso como producto de disfunciones en la tendencia armonizadora hacia un sistema de persecución universalizado.(90)

El parág. 2, tal vez redundante, deja afuera los casos en que no hay intención de cometer las infracciones descriptas ejemplificando con ensayos autorizados o la protección de un sistema informático. A su vez, el parág. 3 contempla la posible reserva de aplicación del parág. 1, salvo en lo concerniente a la venta, distribución o cualquier otra forma de puesta a disposición de tales elementos.

En general, implica un adelantamiento de la intervención penal que constituiría la punición autónoma de actos preparatorios de las restantes tipicidades, lo que explica la amplitud de las posibles reservas que se describen.

b. El repaso normativo regional verifica tipos vinculados en:

b.1 **Argentina**: la reforma del artículo 183 del CP por ley 26.388 del año 2008 —ya transcripto—, introdujo, en su última parte, la punición de la venta, distribución, puesta en circulación o introducción en un sistema informático de cualquier programa destinado a causar daños.

En cambio, con directa vinculación con observación formulada en el punto anterior, Nora Cherñavsky destaca que no se ha tipificado la mera tenencia o posesión de códigos, contraseñas u otros datos que permitan acceder a un sistema informático en relación con la posible lesión a la integridad y confidencialidad de los mismos, incriminación de peligro abstracto prevista en el inc. b del artículo 6° antes transcripto.(91)

b.2 **Brasil**: en su Ley Electoral N° 9100 —año 1995—, prevé reclusión de tres a seis años y multa para quien intente desarrollar o introducir un comando, instrucción o programa de computación capaz de destruir, apagar, eliminar, alterar, grabar o transmitir dato, instrucción o programa o provocar cualquier otro resultado diverso del esperado en el sistema de tratamiento automatizado de datos utilizado por el sistema electoral (art. 67, inc. VIII).

Más reciente es la modificación del artículo 154-A del CP por ley 12.737 —año 2012— que, entre otras conductas base, prevé la de instalar vulnerabilidades para obtener una ventaja ilícita y, con idéntica pena —detención

(90) Anarte Borrallo, Enrique, "Incidencia de las nuevas tecnologías en el sistema penal. Aproximación al derecho penal en la sociedad de la información", en *Derecho y Conocimiento*, Servicio de Publicaciones de la Facultad de Derecho de la Universidad de Huelva, vol. 1, p. 214.

(91) Cherñavsky, *op. cit.*, pp. 284/285.

de 3 meses a un año y multa—, para el que produzca, ofrezca, distribuya, venda o difunda dispositivo o programa de computación con el propósito de permitir alguna de las conductas anteriores (parág. 1º). Se agrava la pena de un sexto a un tercio si resulta perjuicio económico (parág. 2º). También se agrava, pero de un tercio a la mitad, si el delito es practicado contra los más altos funcionarios de los poderes del Estado.

b.3 **Colombia**: la indicada modificación al CP del año 2009 por ley 1273 incluyó un tipo de "uso de software malicioso" como artículo 269E.[92]

b.4 **Paraguay**: mediante la ley 4439 —año 2011— se incorporó al Código Penal la preparación de acceso indebido e interceptación de datos (art. 146d).[93]

b.5 **Perú**: con su nueva ley 30.096 de 2013 ha incorporado un tipo específico correspondiente en su capítulo VII —"Disposiciones comunes"—, artículo 10 —"Abuso de mecanismos y dispositivos informáticos"—.[94] A su vez, aplicable a todas las figuras de la ley especial, el artículo 11[95] prevé los "Agravantes" de orden genérico que, según se podrá advertir de una lectura integral, en muchos casos aparece como redundante, en la medida que las circunstancias de agravación ya han sido incorporadas expresamente en algunas de las figuras que le preceden.

---

(92) Su redacción: "El que, sin estar facultado para ello, produzca, trafique, adquiera, distribuya, venda, envíe, introduzca o extraiga del territorio nacional software malicioso u otros programas de computación de efectos dañinos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes".

(93) Su texto: "Artículo 146 d. Preparación de acceso indebido e interceptación de datos. 1° El que prepare un hecho punible según el art. 146 b o el art. 146 c produciendo, difundiendo o haciendo accesible de otra manera a terceros: 1) las claves de acceso u otros códigos de seguridad, que permitan el acceso a datos en sentido del art. 146 b, inc. 2; o 2) los programas de computación destinados a la realización de tal hecho, será castigado con pena privativa de libertad de hasta un año o multa. 2° Se aplicará, en lo pertinente, lo previsto en el art. 266, incs. 2 y 3".

(94) Dice: "El que fabrica, diseña, desarrolla, vende, facilita, distribuye, importa u obtiene para su utilización uno o más mecanismos, programas informáticos, dispositivos, contraseñas, códigos de acceso o cualquier otro dato informático, específicamente diseñados para la comisión de los delitos previstos en la presente Ley, o el que ofrece o presta servicio que contribuya a ese propósito, será reprimido con una pena privativa de libertad no menor de uno ni mayor de cuatro años y con treinta a noventa días multa".

(95) Su redacción: "El juez aumentará la pena privativa de libertad hasta en un tercio por encima del máximo legal fijado para cualquiera de los delitos previstos en la presente ley cuando:

1. El agente comete el delito en calidad de integrante de una organización criminal.
2. El agente comete el delito mediante el abuso de una posición especial de acceso a la data o información reservada o al conocimiento de esta información en razón del ejercicio de un cargo o función.
3. El agente comete el delito con el fin de obtener un beneficio económico, salvo en los delitos que prevén dicha circunstancia.
4. El delito compromete fines asistenciales, la defensa, la seguridad y la soberanía nacionales".

b.6 **Venezuela**: pune mediante el artículo 10[96] de su LECDI —año 2001— la "Posesión de equipos o prestación de servicios de sabotaje".

c. En los restantes estados bajo comparación —**Bolivia, Chile, Ecuador** y **Uruguay**—, no se advierten figuras penales específicas vigentes que aprehendan la propuesta de Budapest.

3. Las infracciones informáticas

El Título II de la Sección 1 —"Infracciones informáticas"—, se compone de dos artículos mediante los que se indica la necesidad de tipificar la falsedad y la estafa informáticas, del siguiente modo:

3.1. Falsedad informática (art. 7)

> "Las Partes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias para prever como infracción penal, conforme a su derecho interno, 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. Las Partes podrán reservarse el derecho a exigir la concurrencia de un ánimo fraudulento o de cualquier otro ánimo similar para que nazca responsabilidad penal".

a. La generación de datos falsos —sean o no directamente legibles— con intención de que a los efectos legales fueren percibidos o utilizados como auténticos, admite como limitación para los estados signatarios la de exigir en su derecho interno la concurrencia de ánimo de fraude.

b. Puede advertirse en este caso que, tipos o figuras penales locales que fueron individualizados al tratar los atentados a la integridad de datos, brindan parcial cobertura a esta tipicidad. Además, la posible exigencia de intención fraudulenta conduciría muchos otros casos al ámbito de los fraudes informáticos. Ésto dificulta el hallazgo de figuras expresas que reproduzcan la descripción básica del Convenio sin que, sin embargo,

(96) Su texto: "Quien importe, fabrique, distribuya, venda o utilice equipos, dispositivos o programas, con el propósito de destinarlos a vulnerar o eliminar la seguridad de cualquier sistema que utilice tecnologías de la información; o el que ofrezca o preste servicios destinados a cumplir los mismos fines, será penado con prisión de tres a seis años y multa de trescientas a seiscientas unidades tributarias".

pueda considerarse que existen "vacíos" o "lagunas" de punición locales. Así, por ejemplo, la confluencia entre la regulación que protege la integridad de datos personales y la que pune las defraudaciones, permitiría evitar lo que, a primera vista, luciría como atípico por no haber una regla especial que reproduzca con similar terminología el artículo 7 del Convenio. Sentado ello, pueden encontrarse otras normas que guardan vinculación y que no han sido incluidas en ninguno de los acápites mencionados en:

b.1 **Argentina**: ha modificado su regulación de las falsedades documentales. Primero, por vía de la LPDP del año 2000. Luego, por la ley 26.388 del año 2008, incorporó tres nuevos párrafos finales en la parte general al artículo 77[97] del CP, en los que se define al documento y la firma digital. Se provocó con ello una suerte de efecto cascada que amplificó todas las referencias de los tipos de la parte especial.

b.2 **Brasil**: en materia de falsedades, por ley 12.737 del 30 de noviembre de 2012, se modificó el tipo de la falsificación de documento particular (art. 298 del CP), que prevé pena de reclusión de uno a cinco años y multa, e incluye equiparadamente las tarjetas de crédito o débito.

b.3 **Chile**: por artículo 5[98] de la ley 20.009 del 1° de abril de 2005, se introdujeron al derecho chileno varios tipos penales relativos al uso de tarjetas de crédito y débito y a las claves asociadas como modalidades de fraude, por lo que se lo verá en perspectiva del artículo 8° del Convenio.

---

(97) Con el siguiente texto: "… El término documento comprende toda representación de actos o hechos, con independencia del soporte utilizado para su fijación, almacenamiento, archivo o transmisión. Los términos firma y suscripción comprenden la firma digital, la creación de una firma digital o firmar digitalmente. Los términos instrumento privado y certificado comprenden el documento digital firmado digitalmente".

(98) Dice: "Artículo 5°. Las siguientes conductas constituyen delito de uso fraudulento de tarjeta de crédito o débito:

a) Falsificar tarjetas de crédito o débito.

b) Usar, vender, exportar, importar o distribuir tarjetas de crédito o débito falsificadas o sustraídas.

c) Negociar, en cualquier forma, con tarjetas de crédito o débito falsificadas o sustraídas.

d) Usar, vender, exportar, importar o distribuir los datos o el número de una tarjeta de crédito o débito, haciendo posible que terceros realicen operaciones de compra o de acceso al crédito o al débito que corresponden exclusivamente al titular.

e) Negociar, en cualquier forma, con los datos o el número de la tarjeta de crédito o débito, para las operaciones señaladas en la letra anterior.

f) Usar maliciosamente una tarjeta bloqueada, en cualquiera de las formas señaladas en las letras precedentes.

La pena por este delito será de presidio menor en cualquiera de sus grados. Esta pena se aplicará en su grado máximo, si la acción realizada produce perjuicio a terceros".

b.4 **Paraguay**: ha incorporado por ley 4439 del año 2011, un tipo que pune la falsificación o alteración de tarjetas de crédito o de débito o cualquier otro medio electrónico de pago (art. 248b).[99] Se incluye también su adquisición para sí o para tercero, el ofrecimiento, la entrega a otro o el uso de esas tarjetas o medio electrónico de pago.

b.5 **Uruguay**: por ley 16.002 del 25 de octubre de 2088, introdujo los delitos que punen la falsificación documentaria en casos de transmisión a distancia por medios electrónicos (arts. 129[100] y 130),[101] con remisión a los artículos 236 a 239[102] del CP, que se refieren a los documentos públicos. Luego, por

(99) Con la siguiente redacción: "Artículo 248b. Falsificación de tarjetas de débito o de crédito y otros medios electrónicos de pago. 1° El que, con la intención de inducir en las relaciones jurídicas al error o de facilitar la inducción a tal error: 1) falsificare o alterare una tarjeta de crédito o débito u otro medio electrónico de pago; o 2) adquiera para sí o para un tercero, ofreciere, entregare a otro o utilizare tales tarjetas o medios electrónicos, será castigado con pena privativa de libertad de hasta cinco años o con multa. 2° Se castigará también la tentativa. 3° Cuando el autor actuara comercialmente o como miembro de una organización criminal dedicada a la realización de los hechos punibles señalados, la pena privativa de libertad podrá ser aumentada hasta diez años. 4° Tarjetas de crédito, en sentido del inc. 1, son aquellas que han sido emitidas por una entidad de crédito o de servicios financieros para su uso en dicho tipo de transacciones y que, por su configuración o codificación, son especialmente protegidas contra su falsificación. 5° Medios electrónicos de pago en el sentido del inc. 1, son aquellos instrumentos o dispositivos que actúan como dinero electrónico, permitiendo al titular efectuar transferencias de fondos, retirar dinero en efectivo, pagar en entidades comerciales y acceder a los fondos de una cuenta".

(100) Dice: "La documentación emergente de la transmisión a distancia, por medios electrónicos, entre dependencias oficiales, constituirá, de por sí, documentación auténtica y hará plena fe a todos sus efectos en cuanto a la existencia del original trasmitido".

(101) Su texto: "El que voluntariamente trasmitiere a distancias entre dependencias oficiales un texto del que resulte un documento infiel, incurrirá en los delitos previstos por los arts. 236 a 239 del Código Penal, según corresponda".

(102) Sus textos: "236 (Falsificación material en documento público, por funcionario público). El funcionario público que ejerciendo un acto de su función, hiciere un documento falso o alterare un documento verdadero, será castigado con tres a diez años de penitenciaría. Quedan asimilados a los documentos, las copias de los documentos inexistentes y las copias infieles de documento existente.

237 (Falsificación o alteración de un documento público, por un particular o por un funcionario, fuera del ejercicio de sus funciones). El particular o funcionario público que fuera del ejercicio de sus funciones, hiciere un documento público falso o alterare un documento público verdadero, será castigado con dos a seis años de penitenciaría.

238 (Falsificación ideológica por un funcionario público). El funcionario público que, en el ejercicio de sus funciones, diere fe de la ocurrencia de hechos imaginarios o de hechos reales, pero alterando las circunstancias o con omisión o modificación de las declaraciones prestadas con ese motivo o mediante supresión de tales declaraciones, será castigado con dos a ocho años de penitenciaría.

239 (Falsificación ideológica por un particular). El que, con motivo del otorgamiento o formalización de un documento público, ante un funcionario público, prestare una declaración falsa sobre su identidad o estado, o cualquiera otra circunstancia de hecho, será castigado con tres a veinticuatro meses de prisión".

ley 18.600 de documento electrónico y firma digital —del 21 de septiembre de 2009—, estableció un tipo de mayor especificidad (art. 4, inc. 2).[103]

b.6 **Venezuela**: También tipifica las falsificaciones documentales en su LECDI de 2001 (art. 12)[104] y, además, la posesión de equipos destinados a falsificar tarjetas inteligentes o instrumentos análogos (art. 19).[105]

c. Los Estados regionales que carecen de tipo específico y que no cubrirían el vacío en la forma indicada en el precedente primer párrafo "b" serían Bolivia, Colombia, Ecuador y Perú. En este último caso, la nueva ley 30.096 de 2013, en el capítulo VI —dedicado a los "Delitos Informáticos contra la Fe Pública"—, sólo prevé la figura de "suplantación de identidad" en el único artículo que lo integra (art. 9°).[106]

3.2. Estafa informática (art. 8)

> "Las Partes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias para prever como infracción penal, conforme a su derecho interno, la producción de un perjuicio patrimonial a otro, de forma dolosa y sin autorización, a través de:
>
> - la introducción, alteración, borrado o supresión de datos informáticos,
> - cualquier forma de atentado al funcionamiento de un sistema informático, con la intención, fraudulenta o delictiva, de obtener sin autorización un beneficio económico para sí mismo o para tercero".

---

(103) Su redacción es la siguiente: "El que voluntariamente transmitiere un texto del que resulte un documento infiel, adultere o destruya un documento almacenado en soporte magnético, o su respaldo, incurrirá en los delitos previstos por los arts. 236 a 239 del CP, según corresponda".

(104) Dice: "Falsificación de documentos. Quien, a través de cualquier medio, cree, modifique o elimine un documento que se encuentre incorporado a un sistema que utilice tecnologías de información; o cree, modifique o elimine datos del mismo; o incorpore a dicho sistema un documento inexistente, será penado con prisión de tres a seis años y multa de trescientas a seiscientas unidades tributarias. Cuando el agente hubiere actuado con el fin de procurar para sí o para otro algún tipo de beneficio, la pena se aumentará entre un tercio y la mitad.
El aumento será de la mitad a dos tercios si del hecho resultare un perjuicio para otro".

(105) Su texto: "Posesión de equipo para falsificaciones. Todo aquel que sin estar debidamente autorizado para emitir, fabricar o distribuir tarjetas inteligentes o instrumentos análogos, reciba, adquiera, posea, transfiera, comercialice, distribuya, venda, controle o custodie cualquier equipo de fabricación de tarjetas inteligentes o los instrumentos destinados a los mismos fines, o cualquier otro equipo o componente que capture, grabe, copie o transmita la data o información de dichas tarjetas o instrumentos, será penado con prisión de tres a seis años y multa de trescientas a seiscientas unidades tributarias".

(106) Dice: "El que, mediante las tecnologías de la información o de la comunicación suplanta la identidad de una persona natural o jurídica, siempre que de dicha conducta resulte algún perjuicio, material o moral, será reprimido con pena privativa de libertad no menor de tres ni mayor de cinco años".

a. Se trata de una de las previsiones del Convenio que ha recibido críticas de la doctrina, en vistas a que no proporciona una definición de estafa ni brinda una respuesta clara a la utilización abusiva de tarjetas.[107] Con relación a ella se encuentran normas receptivas en los siguientes estados:

a.1 **Argentina**: introdujo dos reformas al CP que consistieron en el agregado de incisos al artículo 173, que ya preveía 14 modalidades de estafas y fraudes pero no vinculadas a las nuevas tecnologías. Por ley 25.930 —año 2004— se incorporó el inc. 15,[108] vinculado a las tarjetas; mientras que por ley 26.388 —año 2008— se agregó el 16.[109] La pena, por remisión al artículo 172, es de un mes a seis años de prisión.

a.2 **Bolivia**: el artículo 363 *bis*[110] del CP —año1997—, bajo la designación de "Manipulación informática", es el que cubre el reclamo de tipicidad.

a.3 **Chile**: por el ya transcripto artículo 5° de la ley 20.009, del 1° de abril de 2005, se introdujo varios tipos penales relativos al uso de tarjetas de crédito y débito y a las claves asociadas.

a.4 **Colombia**: en el marco del capítulo II del nuevo Título incorporado al CP por ley 1273 —año 2009—, se prevén las conductas de "hurto por medios informáticos y semejantes" (art. 269-I)[111] y de "transferencia no consentida de activos" (art. 269-J).[112]

---

(107) Ver García-Cervigón, Josefina, "El fraude informático en España e Italia. Tratamiento jurídico-penal y criminológico", en *ICADE. Revista cuatrimestral de las Facultades de Derecho y Ciencias Económicas y Empresariales*, UNED, n° 74, mayo-agosto 2008, p. 291; y Hirsh, *op. cit.*

(108) Dice: "15) El que defraudare mediante el uso de una tarjeta de compra, crédito o débito, cuando la misma hubiere sido falsificada, adulterada, robada, perdida u obtenida del legítimo emisor mediante ardid o engaño, o mediante el uso no autorizado de sus datos, aunque lo hiciese por medio de una operación automática".

(109) Su texto: "El que defraudare a otro mediante cualquier técnica de manipulación informática que altere el normal funcionamiento de un sistema informático o la transmisión de datos".

(110) Con esta redacción: "El que con la intención de obtener un beneficio indebido para sí o un tercero, manipule un procesamiento o transferencia de datos informáticos que conduzca a un resultado incorrecto o evite un proceso tal cuyo resultado habría sido correcto, ocasionando de esta manera una transferencia patrimonial en perjuicio de tercero. Sanción: reclusión de 1 a 5 años y multa de 60 a 200 días".

(111) Su texto: "El que, superando medidas de seguridad informáticas, realice la conducta señalada en el art. 239 manipulando un sistema informático, una red de sistema electrónico, telemático u otro medio semejante, o suplantando a un usuario ante los sistemas de autenticación y de autorización establecidos, incurrirá en las penas señaladas en el art. 240 de este Código".

(112) Dice: "El que, con ánimo de lucro y valiéndose de alguna manipulación informática o artificio semejante, consiga la transferencia no consentida de cualquier activo en perjuicio de un tercero, siempre que la conducta no constituya delito sancionado con pena más grave, incurrirá en pena de prisión de cuarenta y ocho (48) a ciento veinte (120) meses y en multa de 200 a 1500 salarios mínimos legales mensuales vigentes. La misma sanción se le impondrá a quien fabrique, introduzca, posea o facilite programa de computador destinado a la comisión del delito descrito en el inciso anterior, o de una estafa.

a.5 **Ecuador**: por ley 2002-67 se introdujo —a continuación del artículo sobre conductas asimiladas al robo (art. 553 CPE)— un artículo sin número[113] con dos segmentos. El primero, dedicado a la apropiación ilícita a través del uso fraudulento de sistemas de información o redes electrónicas. El segundo, precisando las circunstancias agravantes. Además, en materia de conductas fraudulentas, se indica una consideración agravada por su perpetración usando medios electrónicos o telemáticos (art. 563).[114]

a.6 **Paraguay**: el nuevo Código Penal ha introducido en su capítulo dedicado a los delitos contra el patrimonio dos tipos específicos vinculados. Uno, de operaciones fraudulentas por computadora (art. 188);[115] y otro, de

---

Si la conducta descrita en los dos incisos anteriores tuviere una cuantía superior a 200 salarios mínimos legales mensuales, la sanción allí señalada se incrementará en la mitad".

(113) Dice: "art. (...) (1). (Ag. por art. 62, L. 2002-67, R.O. 557-S, 17-IV-2002). Apropiación ilícita. Serán reprimidos con prisión de seis meses a cinco años y multa de quinientos a mil dólares de los EU de N, los que utilizaren fraudulentamente sistemas de información o redes electrónicas, para facilitar la apropiación de un bien ajeno, o los que procuren la transferencia no consentida de bienes, valores o derechos de una persona, en perjuicio de ésta o de un tercero, en beneficio suyo o de otra persona alterando, manipulando o modificando el funcionamiento de redes electrónicas, programas informáticos, sistemas informáticos, telemáticos o mensajes de datos.
art. (...) (2). (Ag. por art. 62, L. 2002-67, R.O. 557-S, 17-IV-2002). La pena de prisión de uno a cinco años y multa de mil a dos mil dólares de los EUN, si el delito se hubiere cometido empleando los sigs. medios:

1. Inutilización de sistemas de alarma o guarda;
2. Descubrimiento o descifrado de claves secretas o encriptadas;
3. Utilización de tarjetas magnéticas o perforadas;
4. Utilización de controles o instrumentos de apertura a distancia; y,
5. Violación de seguridades electrónicas, informáticas u otras semejantes".

(114) Su texto: "art. 563 (inc. 2. Ag. por art. 63, L. 2002-67, R.O. 557-S, 17-IV-2002, ref. por art. 159, L. 2002-75, R.O. 635, 7-VIII-2002 y el último inc. ag. por art. 3, L. 2002-91, R.O. 716, 2-XII-2002). El que, con propósito de apropiarse de una cosa perteneciente a otro, se hubiere hecho entregar fondos, muebles, obligaciones, finiquitos, recibos, ya haciendo uso de nombres falsos, o de falsas calidades, ya empleando manejos fraudulentos para hacer creer en la existencia de falsas empresas, de un poder, o de un crédito imaginario, para infundir la esperanza o el temor de un suceso, accidente, o cualquier otro acontecimiento quimérico, o para abusar de otro modo de la confianza o de la credulidad, será reprimido con prisión de seis meses a cinco años y multa de ocho a ciento cincuenta y seis dólares de los Estados Unidos de Norte América.
Será sancionado con el máximo de la pena prevista en el inciso anterior y multa de quinientos a mil dólares de los Estados Unidos de Norteamérica, el que cometiere el delito utilizando medios electrónicos o telemáticos.
La pena será de reclusión menor ordinaria de tres a seis años, si la defraudación se cometiera en casos de migraciones ilegales".

(115) Su texto: "Art. 188. Estafa mediante sistemas informáticos.
1° El que, con la intención de obtener para sí o para un tercero un beneficio patrimonial indebido, influyera sobre el resultado de un procesamiento de datos mediante:

1) una programación incorrecta;

aprovechamiento clandestino de una prestación (art. 189).[116] El primero ha sido modificado por la ley 4439 del 5 de octubre de 2011, que la rebautizó como "Estafa mediante sistemas informáticos".

a.7 **Perú**: su regulación sobre las estafas era genérica. A partir de la modificación del CP —año 1991— por ley 29.316 del 14 de enero de 2009 protegía las señales satelitales portadoras de programas; puniendo tanto la cadena que va desde la fabricación hasta la distribución de dispositivos para asistir a la decodificación (art. 186-A), como hasta la distribución misma de señales (art. 194-A).[117] El artículo 186-A citado ha sido derogado por la nueva ley 30.096 de 2013 —no así el 194-A—, por vía de su disposición complementaria derogatoria única. A su vez, en su capítulo V —"Delitos informáticos contra el patrimonio"—, dedica al "Fraude informático" (art. 8°) su único artículo.[118]

---

2) el uso de datos falsos o incompletos;

3) el uso indebido de datos; u

4) la utilización de otra maniobra no autorizada; y con ello causara un perjuicio al patrimonio de otro, será castigado con pena privativa de libertad de hasta cinco años o con multa.

2° En estos casos, se aplicará también lo dispuesto en el art. 187, incs. 2 al 4.

3° El que preparare un hecho punible señalado en el inc. 1, mediante la producción, obtención, venta, almacenamiento u otorgamiento a terceros de programas de computación destinados a la realización de tales hechos, será castigado con pena privativa de libertad de hasta tres años o con multa.

4° En los casos señalados en el inc. 3, se aplicará lo dispuesto en el art. 266, incs. 2 y 3".

(116) Dice: "Artículo 189. Aprovechamiento clandestino de una prestación.

1° El que con la intención de evitar el pago de la prestación, clandestinamente:

1) se aprovechara del servicio de un aparato automático, de una red de telecomunicaciones destinada al público, o de un medio de transporte; o

2) accediera a un evento o a una instalación, será castigado con pena privativa de libertad de hasta un año o con multa, siempre que no estén previstas penas mayores en otro artículo.

2° En estos casos, será castigada también la tentativa.

3° En lo pertinente se aplicará lo dispuesto en los arts. 171 y 172".

(117) Su texto: "Artículo 194-A. Distribución de señales de satélite portadoras de programas. El que distribuya una señal de satélite portadora de programas, originariamente codificada, a sabiendas que fue decodificada sin la autorización del distribuidor legal de dicha señal, será reprimido con pena privativa de la libertad no menor de dos años ni mayor de seis años y con treinta a noventa días multa".

(118) Su texto: "El que, a través de las tecnologías de la información o de la comunicación, procura para sí o para otro un provecho ilícito en perjuicio de tercero mediante el diseño, introducción, alteración, borrado, supresión, clonación de datos informáticos o cualquier interferencia o manipulación en el funcionamiento de un sistema informático, será reprimido con una pena privativa de libertad no menor de tres ni mayor de ocho años y con sesenta a ciento veinte días multa.

La pena será privativa de libertad no menor de cinco ni mayor de diez años y de ochenta a ciento cuarenta días multa cuando se afecte el patrimonio del Estado destinado a fines asistenciales o a programas de apoyo social".

a.8 **Venezuela**: su LECDI dedica el capítulo II a los "Delitos contra la Propiedad", donde se prevén tipos especiales de fraude (art. 14),[119] obtención indebida de bienes o servicios (art. 15),[120] manejo fraudulento de tarjetas inteligentes o instrumentos análogos (art. 16),[121] apropiación de tarjetas inteligentes o instrumentos análogos (art. 17)[122] y provisión indebida de bienes o servicios (art. 18).[123]

b. Aunque en términos estrictos no implique que sean casos de atipicidad sino que se subsumen en tipos clásicos, puede advertirse la carencia de normas específicas en:

b.1 **Brasil**: su situación es la de disputa doctrinaria; similar a la de Argentina previo a la ley 26.388, descripta anteriormente. Al mantenerse la redacción

(119) Sería el tipo básico. Dice: "Fraude. Todo aquel que, a través del uso indebido de tecnologías de información, valiéndose de cualquier manipulación en sistemas o cualquiera de sus componentes, o en la data o información en ellos contenida, consiga insertar instrucciones falsas o fraudulentas, que produzcan un resultado que permita obtener un provecho injusto en perjuicio ajeno, será penado con prisión de tres a siete años y multa de trescientas a setecientas unidades tributarias".

(120) Dice: "Obtención indebida de bienes o servicios. Quien, sin autorización para portarlos, utilice una tarjeta inteligente ajena o instrumento destinado a los mismos fines, o el que utilice indebidamente tecnologías de la información para requerir la obtención de cualquier efecto, bien o servicio; o para proveer su pago sin erogar o asumir el compromiso de pago de la contraprestación debida, será castigado con prisión de dos a seis años y multa de doscientas a seiscientas unidades tributarias".

(121) Su redacción: "Manejo fraudulento de tarjetas inteligentes o instrumentos análogos. Toda persona que por cualquier medio cree, capture, grabe, copie, altere, duplique o elimine la data o información contenidas en una tarjeta inteligente o en cualquier instrumento destinado a los mismos fines; o la persona que, mediante cualquier uso indebido de tecnologías de información, cree, capture, duplique o altere la data o información en un sistema, con el objeto de incorporar usuarios, cuentas, registros o consumos inexistentes o modifique la cuantía de estos, será penada con prisión de cinco a diez años y multa de quinientas a mil unidades tributarias.
En la misma pena incurrirá quien, sin haber tomado parte en los hechos anteriores, adquiera, comercialice, posea, distribuya, venda o realice cualquier tipo de intermediación de tarjetas inteligentes o instrumentos destinados al mismo fin, o de la data o información contenidas en ellos o en un sistema".

(122) Su texto: "Apropiación de tarjetas inteligentes o instrumentos análogos. Quien se apropie de una tarjeta inteligente o instrumento destinado a los mismos fines, que se haya perdido, extraviado o que haya sido entregado por equivocación, con el fin de retenerlo, usarlo, venderlo o transferirlo a una persona distinta del usuario autorizado o entidad emisora, será penado con prisión de uno a cinco años y multa de diez a cincuenta unidades tributarias.
La misma pena se impondrá a quien adquiera o reciba la tarjeta o instrumento a que se refiere el presente artículo".

(123) Dice: "Provisión indebida de bienes o servicios. Todo aquel que, a sabiendas de que una tarjeta inteligente o instrumento destinado a los mismos fines, se encuentra vencido, revocado; se haya indebidamente obtenido, retenido, falsificado, alterado; provea a quien los presente de dinero, efectos, bienes o servicios, o cualquier otra cosa de valor económico será penado con prisión de dos a seis años y multa de doscientas a seiscientas unidades tributarias".

histórica de la estafa, se discute si se trata de una modalidad de aquella o de un hurto. Hay un tipo vinculado al fraude fiscal. Por ley 8137 del 27 de diciembre de 1990, sobre "Crímenes contra el orden económico y las relaciones de consumo", se establece una nueva forma de uso ilícito del ordenador definida como la acción de utilizar o divulgar programas de procesamiento de datos que permitan al contribuyente poseer información contable diversa a la que es, por ley, proporcionada a la Hacienda Pública. Tiene pena de detención de 6 meses a 2 años y multa.

b.2 **Uruguay**: introdujo como actualización normativa la penalización del uso indebido de señales destinadas a ser recibidas en régimen de suscripción por ley 17.520 del 19 de julio de 2002, puniendo la captación (art. 1°)[124] y el efectuarla a favor de tercero (art. 2°),[125] con distintas agravantes (art. 3°);[126] así como también conductas favorecedoras relacionadas con los aparatos de decodificación o similares (art. 4°).[127]

4. Infracciones relativas al contenido

4.1. Infracciones relativas a la pornografía infantil (art. 9)

En el Título 3 —"Infracciones relativas al contenido"— se prevé un solo artículo, "Infracciones relativas a la pornografía infantil" (art. 9°), que incluye una serie de conductas que propone tipificar y conceptos que precisan lo que serían para nosotros elementos normativos del tipo. En este sentido, el texto dice:

---

(124) Su redacción: "El que, para provecho propio o de un tercero, captare señales trasmitidas por cualquier medio destinadas exclusivamente a ser recibidas en régimen de abonados, sin serlo, será castigado con 80 UR (ochenta unidades reajustables) a 800 UR (ochocientas unidades reajustables), de multa o prisión equivalente".

(125) Dice: "El que, con o sin ánimo de lucro, efectuare a favor de un tercero, las instalaciones, manipulaciones, o cualquier otra actividad necesaria para la obtención de los hechos que determinan la conducta típica descrita en el artículo anterior, será castigado con pena de tres meses de prisión a tres años de penitenciaría".

(126) Con esta redacción: "Las penas de los delitos anteriores serán aumentadas de un tercio a la mitad:

1) Si las conductas se realizaren mediante la producción de un daño a la red, instalaciones conexas, equipos o cualquier otro elemento técnico pertenecientes a la empresa autorizada prestadora del servicio, cualquiera sea el lugar que ellos estuvieran colocados.
2) Si las conductas ocasionaren una interrupción o perturbación del servicio o un menoscabo efectivo de su calidad, en perjuicio de otros suscriptores.
3) Cuando el agente revista la calidad de empleado, ex-empleado o arrendador de servicios de la empresa permisaria o del instalador autorizado".

(127) Su texto: "El que fabrique, importe, venda u ofrezca en venta, arriende o ponga en circulación decodificadores o cualquier otro artefacto, equipo o sistema diseñado exclusivamente para eliminar, impedir, desactivar o eludir los dispositivos técnicos que los titulares autorizados de la señal hayan instalado, para su protección, será castigado con pena de tres a veinticuatro meses de prisión".

"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:

- la producción de pornografía infantil con la intención de difundirla a través de un sistema informático;
- el ofrecimiento o la puesta a disposición de pornografía infantil a través de un sistema informático;
- la difusión o la transmisión de pornografía infantil a través de un sistema informático;
- el hecho de procurarse o de procurar a otro pornografía infantil a través de un sistema informático;
- 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:

- un menor adoptando un comportamiento sexualmente explícito;
- una persona que aparece como un menor adoptando un comportamiento sexualmente explícito;
- 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 menor de 18 años. Las Partes podrán exigir un límite de edad inferior, que debe 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)".[128]

(128) Rovira del Canto recuerda que la propuesta fue reafirmada mediante la DM 2004/68/JAI del Consejo, de 22 de diciembre de 2003, relativa a la lucha contra la explotación sexual de los niños y la pornografía infantil, cuyo art. 2 indica que los Estados miembros del Consejo adoptarán las medidas necesarias para la punibilidad como infracciones relacionadas con la explotación sexual de los niños, de las conductas intencionales siguientes: "a) coaccionar a un niño para que se prostituya o participe en espectáculos pornográficos, o lucrase con ello o explotar de cualquier otra manera a un niño para tales fines; b) captar a un niño para que se prostituya o participe en espectáculos pornográficos; d) practicar con un niño actividades sexuales recurriendo a algunos de los medios siguientes: i) hacer uso de la coacción, la fuerza o la amenaza; ii) ofrecer al niño dinero u otras formas de remuneración o de atenciones a cambio de que se preste a practicar actividades sexuales; iii) abusar de una posición de reconocida confianza, autoridad o influencia sobre el niño" (Rovira del Canto, *op. cit.*, p. 6).

a. En relación con la pornografía, la propuesta del Convenio limita la intervención penal a los casos que compromete a menores; por lo que, desde esta perspectiva, la conflictividad con los ordenamientos locales, en principio, no existe. La salvedad corresponde, en general, porque resulta inevitable la verificación de discrepancias al momento de interpretar los alcances de un elemento normativo teñido fuertemente por condicionantes culturales, como qué es "pornografía" u "obscenidad". Y, en particular, porque resulta inevitable la verificación de discrepancias al momento de la punición de casos en los que efectivamente no hay intervención de menores en el material pornográfico, sino de personas que aparecen como menores; o se trata de imágenes realistas que representan a un menor (incs. 2.b y 2.c). De lo contrario, quedarían comprendidos casos de imágenes puramente virtuales sin ninguna base real.

Para muchos estados que han firmado 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 concepto de **pornografía infantil**, en concordancia con la previsión de Budapest que ahora nos ocupa, es "toda representación, por cualquier medio, de un niño dedicado a actividades sexuales explícitas, reales o simuladas, o todo representación de las partes genitales de un niño con fines primordialmente sexuales" (art. 2° inc. c).

Tanto en la región de Argentina como Brasil, luego de la primera aproximación —año 2003— en la discusión parlamentaria de sus respectivas leyes modificatorias internas, se optó por excluir las meras simulaciones de los tipos penales por su conflictividad constitucional; ya sea por contraposición con la libertad de expresión —representaciones artísticas, por ejemplo— o por posible derecho penal de autor —punición de la tendencia pederasta—. No obstante, se trata conforme el inc. 4° del Convenio, de dos de los casos en que los estados pueden formular reserva —los otros son el procurarse o procurarle a otro, y la simple posesión de material prohibido—. Corresponde aclarar que, en su segunda reforma del año 2008, en Brasil, se cambió de posición e incluyó la pornografía "virtual" y también la simple tenencia de imágenes como las referidas.

b. Una vez escrutadas las legislaciones nacionales de la región, se encuentran tipos específicos en:

b.1 **Argentina**: por la ley 26.388 —año 2008— se modificó el CP con la actualización del art. 128.[129] Debe tenerse presente que el citado "Protocolo facultativo…" ha sido incorporado a nuestro derecho interno por ley 25.763 —año 2003—, sin perjuicio de lo cual las actividades "simuladas" fueron excluidas. También lo ha sido la simple posesión, bajo consideración de tratarse de un tipo que merece un debate amplio que, por un lado, conlleva el problema de la polémica acerca de su posible incursión en ámbitos de reserva de moral sexual en equiparación con otras conductas mucho más graves y de directa lesividad y, por otro, no difiere demasiado del genérico alrededor de las figuras de "tenencia" punibles y los delitos de peligro abstracto.

b.2 **Brasil**: el Estatuto del Menor y del Adolescente (ECA, *Estatuto da Criança e Adolescente*, ley 8069/90) tipifica la conducta ampliando el crimen de "pornografía infantil" desde la reforma del art. 241 —12 de noviembre de 2003— por ley 10.764. En 2008, el ECA fue masiva y nuevamente modificado en sus previsiones penales por ley 11.829/08, con la intención de actualizarlo en el tema pedofilia.

Al presente, las normas de interés en la materia que nos ocupa son los arts. 240;[130] 241;[131] 241-A,[132] cuyo parág. 2° incluye la responsabilidad

(129) El texto vigente reza: "Será reprimido con prisión de seis (6) meses a cuatro (4) años el que produjere, financiare, ofreciere, comerciare, publicare, facilitare, divulgare o distribuyere, por cualquier medio, toda representación de un menor de dieciocho (18) años dedicado a actividades sexuales explícitas o toda representación de sus partes genitales con fines predominantemente sexuales, al igual que el que organizare espectáculos en vivo de representaciones sexuales explícitas en que participaren dichos menores. Será reprimido con prisión de cuatro (4) meses a dos (2) años el que tuviere en su poder representaciones de las descriptas en el párrafo anterior con fines inequívocos de distribución o comercialización. Será reprimido con prisión de un (1) mes a tres (3) años el que facilitare el acceso a espectáculos pornográficos o suministrare material pornográfico a menores de catorce (14) años".

(130) Su texto: *"Produzir, reproduzir, dirigir, fotografar, filmar ou registrar, por qualquer meio, cena de sexo explícito ou pornográfica, envolvendo criança ou adolescente. Pena – reclusão, de 4 (quatro) a 8 (oito) anos, e multa.*
§ 1 Incorre nas mesmas penas quem agencia, facilita, recruta, coage, ou de qualquer modo intermedeia a participação de criança ou adolescente nas cenas referidas no caput deste artigo, ou ainda quem com esses contraseña.
§ 2 Aumenta-se a pena de 1/3 (um terço) se o agente comete o crime:
I – no exercício de cargo ou função pública ou a pretexto de exercê-la;
II – prevalecendo-se de relações domésticas, de coabitação ou de hospitalidade; ou
III – prevalecendo-se de relações de parentesco consangüíneo ou afim até o terceiro grau, ou por adoção, de tutor, curador, preceptor, empregador da vítima ou de quem, a qualquer outro título, tenha autoridade sobre ela, ou com seu consentimento".

(131) Dice: *"Vender ou expor à venda fotografia, vídeo ou outro registro que contenha cena de sexo explícito ou pornográfica envolvendo criança ou adolescente: Pena – reclusão, de 4 (quatro) a 8 (oito) anos, e multa".*

(132) Con esta redacción: *"Oferecer, trocar, disponibilizar, transmitir, distribuir, publicar ou divulgar por qualquer meio, inclusive por meio de sistema de informática ou telemático,*

del ISP que debidamente notificado no deshabilita el acceso al contenido; el 241-B,[133] referido a la punición de la simple tenencia de material pornográfico infantil; el 241-C,[134] que incorpora la punición de las escenas simuladas, también incluidas en la previsión de aclaración conceptual en el art. 241-E;[135] y, finalmente, el art. 241-D[136], referido la punición del *grooming*.

---

fotografia, vídeo ou outro registro que contenha cena de sexo explícito ou pornográfica envolvendo criança ou adolescente: Pena – reclusão, de 3 (três) a 6 (seis) anos, e multa.
§ 1 Nas mesmas penas incorre quem:
I – assegura os meios ou serviços para o armazenamento das fotografias, cenas ou imagens de que trata o caput deste artigo;
II – assegura, por qualquer meio, o acesso por rede de computadores às fotografias, cenas ou imagens de que trata o caput deste artigo.
§ 2 As condutas tipificadas nos incisos I e II do § 1 deste artigo são puníveis quando o responsável legal pela prestação do serviço, oficialmente notificado, deixa de desabilitar o acesso ao conteúdo ilícito de que trata o caput deste artigo".

(133) Su texto: "*Adquirir, possuir ou armazenar, por qualquer meio, fotografia, vídeo ou outra forma de registro que contenha cena de sexo explícito ou pornográfica envolvendo criança ou adolescente:*
Pena – reclusão, de 1 (um) a 4 (quatro) anos, e multa.
§ 1 A pena é diminuída de 1 (um) a 2/3 (dois terços) se de pequena quantidade o material a que se refere o caput deste artigo.
§ 2 Não há crime se a posse ou o armazenamento tem a finalidade de comunicar às autoridades competentes a ocorrência das condutas descritas nos arts. 240, 241, 241-A e 241-C desta Lei, quando a comunicação for feita por:
I – agente público no exercício de suas funções;
II – membro de entidade, legalmente constituída, que inclua, entre suas finalidades institucionais, o recebimento, o processamento e o encaminhamento de notícia dos crimes referidos neste parágrafo;
III – representante legal e funcionários responsáveis de provedor de acesso ou serviço prestado por meio de rede de computadores, até o recebimento do material relativo à notícia feita à autoridade policial, ao Ministério Público ou ao Poder Judiciário.
§ 3 As pessoas referidas no § 2 deste artigo deverão manter sob sigilo o material ilícito referido".

(134) Dice: "*Simular a participação de criança ou adolescente em cena de sexo explícito ou pornográfica por meio de adulteração, montagem ou modificação de fotografia, vídeo ou qualquer outra forma de representação visual: Pena – reclusão, de 1 (um) a 3 (três) anos, e multa. Parágrafo único. Incorre nas mesmas penas quem vende, expõe à venda, disponibiliza, distribui, publica ou divulga por qualquer meio, adquire, possui ou armazena o material produzido na forma do caput deste artigo".*

(135) Con la siguiente redacción: "*Para efeito dos crimes previstos nesta Lei, a expressão "cena de sexo explícito ou pornográfica" compreende qualquer situação que envolva criança ou adolescente em atividades sexuais explícitas, reais ou simuladas, ou exibição dos órgãos genitais de uma criança ou adolescente para fins primordialmente sexuais".*

(136) Su texto: "*Aliciar, assediar, instigar ou constranger, por qualquer meio de comunicação, criança, com o fim de com ela praticar ato libidinoso: Pena – reclusão, de 1 (um) a 3 (três) anos, e multa.*
Parágrafo único. Nas mesmas penas incorre quem:
I – facilita ou induz o acesso à criança de material contendo cena de sexo explícito ou pornográfica com o fim de com ela praticar ato libidinoso;
II – pratica as condutas descritas no caput deste artigo com o fim de induzir criança a se exibir de forma pornográfica ou sexualmente explícita".

b.3 **Chile**: en la ley 19.927 —14 de enero de 2004—, que modifica tanto al código sustantivo como al adjetivo, se trata la pornografía infantil, entre otros delitos contra la integridad sexual de los menores. En lo que hace al código sustantivo, que es el que aquí interesa, los tipos de relevancia son: los arts. 366 *quáter,*[137] referido a conductas de significación sexual frente a menores; 366 *quinquies,*[138] referido a producción de material pornográfico con menores; 374 *bis,* [139] referido a cadena de comercialización a exhibición en cualquier soporte del material prohibido, así como adquisición y almacenamiento de aquél; y 374 *ter,*[140] que fija competencia a partir de un punto de acceso en territorio chileno.

b.4 **Colombia**: los tipos penales concernientes a la pornografía infantil han quedado delineados mediante sendas reformas al C.P. del año 2009: la pornografía con personas menores de 18 años (ley 1336, art. 218)[141] y la utilización o fa-

---

(137) Su texto: "Artículo 366 *quáter.* El que, sin realizar una acción sexual en los términos anteriores, para procurar su excitación sexual o la excitación sexual de otro, realizare acciones de significación sexual ante una persona menor de catorce años, la hiciere ver o escuchar material pornográfico o presenciar espectáculos del mismo carácter, será castigado con presidio menor en su grado medio a máximo.
Si, para el mismo fin de procurar su excitación sexual o la excitación sexual de otro, determinare a una persona menor de catorce años a realizar acciones de significación sexual delante suyo o de otro, la pena será presidio menor en su grado máximo.
Con iguales penas se sancionará a quien realice alguna de las conductas descritas en los incisos anteriores con una persona menor de edad pero mayor de catorce años, concurriendo cualquiera de las circunstancias del numerando 1º del art. 361 o de las enumeradas en el art. 363".

(138) Dice: "Artículo 366 *quinquies.* El que participare en la producción de material pornográfico, cualquiera sea su soporte, en cuya elaboración hubieren sido utilizados menores de dieciocho años, será sancionado con presidio menor en su grado máximo.
Para los efectos de este artículo y del art. 374 *bis,* se entenderá por material pornográfico en cuya elaboración hubieren sido utilizados menores de dieciocho años, toda representación de éstos dedicados a actividades sexuales explícitas, reales o simuladas, o toda representación de sus partes genitales con fines primordialmente sexuales".

(139) Tiene la siguiente redacción: "Artículo 374 *bis.* El que comercialice, importe, exporte, distribuya, difunda o exhiba material pornográfico, cualquiera sea su soporte, en cuya elaboración hayan sido utilizados menores de dieciocho años, será sancionado con la pena de presidio menor en su grado medio a máximo.
El que maliciosamente adquiera o almacene material pornográfico, cualquiera sea su soporte, en cuya elaboración hayan sido utilizados menores de dieciocho años, será castigado con presidio menor en su grado medio".

(140) Su texto: "Artículo 374 *ter.* Las conductas de comercialización, distribución y exhibición señaladas en el artículo anterior, se entenderán cometidas en Chile cuando se realicen a través de un sistema de telecomunicaciones al que se tenga acceso desde territorio nacional".

(141) Su texto: "El que fotografíe, filme, grabe, produzca, divulgue, ofrezca, venda, compre, posea, porte, almacene, trasmita o exhiba, por cualquier medio, para uso personal o intercambio, representaciones reales de actividad sexual que involucre persona menor de 18 años de edad, incurrirá en prisión de 10 a 20 años y multa de 150 a 1500 salarios mínimos legales mensuales vigentes.

cilitación de medios de comunicación para ofrecer actividades sexuales con personas menores de 18 años (ley 1329, art. 219-A).[142]

b.5 **Ecuador**: mediante la ley 2005-2 —23 de junio de 2005— introdujo en su CP un capítulo sin número concerniente a los "Delitos de Explotación Sexual" que, a través de varios artículos también sin número, pune la pornografía infantil entre otras conductas disvaliosas que incluyen hasta la oferta de turismo sexual. La norma que aquí interesa es el primer artículo sin número.[143]

b.6 **Paraguay**: la ley 2861/06 —"De represión del comercio y la difusión comercial o no comercial de material pornográfico, utilizando la imagen u otra representación de menores o incapaces"— introdujo la punición de la utilización de niños, niñas y adolescentes en pornografía (art. 1°) o su exhibición en actos sexuales (art. 3°); la difusión o comercialización de pornografía infantil (art. 2°), contemplándose diversas situaciones agravantes (art. 4°). Luego, la reforma del CP por ley 4439 —año 2011— modificó el art. 140,[144] que es el ahora regente. Entre su variado catálogo de conductas típicas, incluye la simple posesión de material prohibido (parág. 4°).

Igual pena se aplicará a quien alimente con pornografía infantil bases de datos de Internet, con o sin fines de lucro.

La pena se aumentará de una tercera parte a la mitad cuando el responsable sea integrante de la familia de la víctima".

(142) Dice: "El que utilice o facilite el correo tradicional, las redes globales de información, telefonía o cualquier medio de comunicación, para obtener, solicitar, ofrecer o facilitar contacto o actividad con fines sexuales con personas menores de 18 años de edad, incurrirá en pena de prisión de diez (10) a catorce (14) años y multa de sesenta y siete (67) a (750) salarios mínimos legales mensuales vigentes.

Las penas señaladas en el inciso anterior se aumentarán hasta en la mitad ($^1/_2$) cuando las conductas se realizaren con menores de catorce (14) años".

(143) En su parte pertinente dice: "art. (...) (1). (Agregado por el art. 18 de la ley 2005-2, R.O. 45, 23-VI-2005). Quien produjere, publicare o comercializare imágenes pornográficas, materiales visuales, audiovisuales, informáticos, electrónicos o de cualquier otro soporte físico o formato, u organizare espectáculos en vivo, con escenas pornográficas en que participen los mayores de catorce y menores de dieciocho años, será reprimido con la pena de seis a nueve años de reclusión menor ordinaria, el comiso de los objetos y de los bienes producto del delito, la inhabilidad para el empleo, profesión u oficio.

Con la misma pena incurrirá quien distribuyere imágenes pornográficas, cuyas características externas hiciere manifiesto que en ellas sea (SIC) grabado o fotografiado la exhibición de mayores de doce y menores de dieciocho años al momento de creación de la imagen.

Con la misma pena será reprimido quien facilitare el acceso a espectáculos pornográficos o suministrare material pornográfico en cuyas imágenes participen menores de edad…".

(144) Dice: "Pornografía relativa a niños y adolescentes.

1° El que:

1) produjere publicaciones, en el sentido del art. 14, inc. 3, que representen actos sexuales con participación de personas menores de dieciocho años de edad o la exhibición de sus partes genitales;
2) organizara, financiara o promocionara espectáculos, públicos o privados, en los que participe una persona menor de dieciocho años en la realización de actos sexuales, o;

b.7 **Perú**: por la modificación al art. 181-A[145] del CP mediante ley 29.408 —del 18 de septiembre de 2009— se tipificó la promoción, publicidad, favorecimiento o facilitación de la explotación sexual comercial de menores por cualquier medio; incluyendo expresamente los electrónicos, magnéticos y a través de Internet. A su vez, dentro de las ofensas al pudor público, el artículo 182-A sanciona la publicación en los medios de comunicación sobre delitos de libertad sexual a menores. Más específicamente a nuestro objeto, el art. 183 pena las exhibiciones y publicaciones obscenas de menores; y el artículo 183-A[146] —modificado por ley 28.251 del 8 de junio

3) distribuyera, importara, exportara, ofertara, canjeara, exhibiera, difundiera, promocionara o financiara la producción o reproducción de publicaciones en sentido del numeral 1, será castigado con pena privativa de libertad de hasta cinco años o multa.

2° El que reprodujera publicaciones según el numera l 1 del inc. 1, será castigado con pena privativa de libertad de hasta tres años o multa.

3° La pena de los incisos anteriores podrá ser aumentada hasta diez años cuando:

1) las publicaciones y espectáculos en el sentido de los incs. 1 y 2 se refieran a menores de catorce años o se dé acceso a los menores de dicha edad a publicaciones y espectáculos, en sentido de los incisos citados;
2) el autor tuviera la patria potestad, deber de guarda o tutela del niño o adolescente, o se le hubiere confiado la educación o cuidado del mismo;
3) el autor operara en connivencia con personas a quienes competa un deber de educación, guarda o tutela respecto del niño o adolescente;
4) el autor hubiere procedido, respecto del niño o adolescente, con violencia, fuerza, amenaza, coacción, engaño, recompensa o promesa remuneratoria de cualquier especie; o
5) el autor actuara comercialmente o como miembro de una banda dedicada a la realización reiterada de los hechos punibles señalados.

4° El que obtuviera la posesión de publicaciones en el sentido de los incs. 1 y 3, será castigado con pena privativa de libertad d e hasta tres años o con multa.

5° Se aplicará, en lo pertinente, también lo dispuesto en los arts. 57 y 94".

(145) Dice: "Artículo 181-A. Explotación sexual comercial infantil y adolescente en ámbito del turismo.

El que promueve, publicita, favorece o facilita la explotación sexual comercial en el ámbito del turismo, a través de cualquier medio escrito, folleto, impreso, visual, audible, electrónico, magnético o a través de Internet, con el objeto de ofrecer relaciones sexuales de carácter comercial de personas de catorce (14) y menos de dieciocho (18) años de edad será reprimido con pena privativa de libertad no menor de cuatro (4) ni mayor de ocho (8) años.

Si la víctima es menor de catorce años, el agente, será reprimido con pena privativa de la libertad no menor de seis (6) ni mayor de ocho (8) años.

El agente también será sancionado con inhabilitación conforme al art. 36 incs. 1, 2, 4 y 5.

Será no menor de ocho (8) ni mayor de diez (10) años de pena privativa de la libertad cuando ha sido cometido por autoridad pública, sus ascendientes, maestro o persona que ha tenido a su cuidado por cualquier título a la víctima".

(146) En su parte pertinente dice: "Artículo 183-A. Pornografía infantil. El que posee, promueve, fabrica, distribuye, exhibe, ofrece, comercializa o publica, importa o exporta por cualquier medio objetos, libros, escritos, imágenes, videos o audios, o realiza espectáculos en vivo de carácter pornográfico, en los cuales se utilice a personas de catorce y menos de dieciocho años de edad, será sancionado con pena privativa de libertad no menor de seis ni mayor de diez años y con ciento veinte a trescientos sesenta y cinco días multa.

de 2004— se ocupa de la pornografía infantil. La disposición complementaria modificatoria cuarta de este último ha sido modificada por vía de la ley 30.096 —año 2013—. El cambio más significativo es la referencia a su comisión por cualquier medio y un incremento significativo de la escala de pena conminada en abstracto.

Además, la citada nueva Ley de Delitos Informáticos ha incorporado el tipo de "Proposiciones a niños, niñas y adolescentes con fines sexuales por medios tecnológicos"(art. 5)[147] en el marco del capítulo III, "Delitos Informáticos contra la indemnidad y libertad sexuales". Se trata de la conducta conocida como *grooming*.

Finalmente, en la primera de sus disposiciones complementarias finales, "Codificación de la pornografía infantil", aclara que la Policía Nacional del Perú puede mantener tal mantener en sus archivos, con autorización y supervisión del Ministerio Público, tal material para fines exclusivos del cumplimiento de su función en una base de datos debidamente codificada.

b.8 **Uruguay**: el viejo artículo 278[148] del CP mantiene la punición de la pornografía en general. No obstante, por ley 17.559 —del 27 de septiembre de 2002— se 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 pornografía. Además, por ley 17.815 —del 6 de noviembre de 2004—, se reguló la "Violencia sexual comercial o no comercial cometida contra niños, adolescentes e incapaces". Así se consagraron varios nuevos tipos penales: la fabricación o producción de material pornográfico con utilización de personas menores de edad o incapaces (art. 1°);[149] el comercio

---

La pena privativa de libertad será no menor de diez ni mayor de doce años y de cincuenta a trescientos sesenta y cinco días multa cuando:
1. El menor tenga menos de catorce años de edad.
2. El material pornográfico se difunda a través de las tecnologías de la información o de la comunicación.

Si la víctima se encuentra en alguna de las condiciones previstas en el último párrafo del art. 173 o si el agente actúa en calidad de integrante de una organización dedicada a la pornografía infantil, la pena privativa de libertad será no menor de doce ni mayor de quince años. De ser el caso, el agente será inhabilitado conforme los numerales 1, 2 y 4 del art. 36".

(147) Su texto: "El que, a través de las tecnologías de la información o de la comunicación, contacta con un menor de catorce años para solicitar u obtener de él material pornográfico, o para llevar a cabo actividades sexuales con él, será reprimido con pena privativa de libertad no menor de cuatro ni mayor de ocho años e inhabilitación conforme a los numerales 1, 2 y 4 del art. 36 del CP.

Cuando la víctima tiene entre catorce y menos de dieciocho años de edad y medie engaño, la pena será no menor de tres ni mayor de seis años e inhabilitación conforme a los numerales 1, 2 y 4 del art. 36 del CP".

(148) Dice: "Comete delito de exhibición pornográfica el que ofrece públicamente espectáculos teatrales o cinematográficos obscenos, el que transmite audiciones o efectúa publicaciones de idéntico carácter. Este delito se castiga con la pena de tres a veinticuatro meses de prisión".

(149) Con la siguiente redacción: "El que de cualquier forma fabricare o produjere material pornográfico utilizando a personas menores de edad o personas mayores de edad incapa-

y difusión de material pornográfico en que aparezca la imagen u otra forma de representación de personas menores de edad o personas incapaces (art. 2°);[150] favorecer la comercialización y difusión de material pornográfico con la imagen u otra representación de una o más personas menores de edad o incapaces (art. 3°);[151] la retribución o promesa de retribución a personas menores de edad o incapaces para que ejecuten actos sexuales o eróticos de cualquier tipo (art. 4°);[152] la contribución a la explotación sexual de personas menores de edad o incapaces (art. 5°) [153] y el tráfico de personas menores de edad o incapaces (art. 6°).[154]

b.9 **Venezuela**: en el capítulo IV "De los delitos contra niños, niñas o adolescentes" de la LECDI de 2001 se pune la difusión o exhibición de material pornográfico (art. 23)[155] y la exhibición pornográfica de niños o adolescentes (art. 24)[156] usando tecnologías de información.

---

ces, o utilizare su imagen, será castigado con pena de veinticuatro meses de prisión a seis años de penitenciaría".

(150) Su texto: "El que comerciare, difundiere, exhibiere, almacenare con fines de distribución, importare, exportare, distribuyere u ofertare material pornográfico en el que aparezca la imagen o cualquier otra forma de representación de una persona menor de edad o persona incapaz, será castigado con pena de doce meses de prisión a cuatro años de penitenciaría".

(151) Su texto: "El que de cualquier modo facilitare, en beneficio propio o ajeno, la comercialización, difusión, exhibición, importación, exportación, distribución, oferta, almacenamiento o adquisición de material pornográfico que contenga la imagen o cualquier otra forma de representación de una o más personas menores de edad o incapaces será castigado con pena de seis meses de prisión a dos años de penitenciaría. A los efectos del presente artículo y de los anteriores, se entiende que es producto o material pornográfico todo aquel que por cualquier medio contenga la imagen u otra forma de representación de personas menores de edad o incapaces dedicadas a actividades sexuales explícitas, reales o simuladas, o la imagen o representación de sus partes genitales, con fines primordialmente sexuales".

(152) Dice: "El que pagare o prometiere pagar o dar a cambio una ventaja económica o de otra naturaleza a persona menor de edad o incapaz de cualquier sexo, para que ejecute actos sexuales o eróticos de cualquier tipo, será castigado con pena de dos a doce años de penitenciaría".

(153) Su redacción es: "El que de cualquier modo contribuyere a la prostitución, explotación o servidumbre sexual de personas menores de edad o incapaces, será castigado con pena de dos a doce años de penitenciaría. La pena será elevada de un tercio a la mitad si se produjere con abuso de las relaciones domésticas o de la autoridad o jerarquía, pública o privada, o la condición de funcionario policial del agente".

(154) Su texto: "El que de cualquier modo favorezca o facilite la entrada o salida del país de personas menores de edad o incapaces, para ser prostituidas o explotadas sexualmente, será castigado con pena de dos a doce años de penitenciaría".

(155) Dice: "Todo aquel que, por cualquier medio que involucre el uso de tecnologías de información, exhiba, difunda, transmita o venda material pornográfico o reservado a personas adultas, sin realizar previamente las debidas advertencias para que el usuario restrinja el acceso a niños, niñas y adolescentes, será sancionado con prisión de dos a seis años y multa de doscientas a seiscientas unidades tributarias".

(156) Con esta redacción: "Toda persona que por cualquier medio que involucre el uso de tecnologías de la información, utilice a la persona o imagen de un niño, niña o adolescente

c. Bolivia no ha actualizado su legislación. Pese a tener un Código relativamente joven, de 1997, mantuvo la tradicional punición de los llamados "ultrajes al pudor" en sus artículos 323[157] y 324.[158]

5. Infracciones vinculadas a los atentados a la propiedad intelectual y derechos afines

5.1. Afectación de la propiedad intelectual y derechos afines (art. 10)

Al igual que en el caso anterior, el Título 4 de la Sección 1 —"Infracciones vinculadas a los atentados a la propiedad intelectual y a los derechos afines"— está integrado por el artículo referido a la "Afectación de la propiedad intelectual y derechos afines" (art. 10), con el siguiente texto:

> "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

---

con fines exhibicionistas o pornográficos, será penada con prisión de cuatro a ocho años y multa de cuatrocientas a ochocientas unidades tributarias".

(157) Dice: "(Actos Obscenos). El que en lugar público o expuesto al público realizare actos obscenos o los hiciere ejecutar por otro, incurrirá en reclusión de tres meses a dos años".

(158) Su texto: "(Publicaciones y Espectáculos Obscenos). El que con cualquier propósito expusiere públicamente, fabricare, introdujere en el país o reprodujere libros, escritos, dibujos, imágenes u otros objetos obscenos, o el que los distribuyere o pusiere en circulación, o el que públicamente ofreciere espectáculos teatrales o cinematográficos u otros obscenos, o transmitiere audiciones de la misma índole, será sancionado con reclusión de tres meses a dos años".

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 párrs. 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 párrs. 1 y 2 del presente artículo".

a. En materia de atentados contra la propiedad intelectual o derechos afines; no debe perderse de vista que el Convenio habla de una posible intervención penal, cuando se trate de conductas dolosas a través de un sistema informático y tengan "escala comercial". Podría prescindirse de ésta si se dispusiera de otros recursos eficaces para su represión.

b. En este caso, puede afirmarse que todos los países que integran la región poseen legislación que cubre la materia.

b.1 **Argentina**: la ley 25.036 —año 1998— modificó la Ley de Propiedad Intelectual (LPI), ley 11.723, para brindar protección penal al software a partir de la inclusión de los programas de computación (arts. 1°, 4°, 9°, 55 *bis* y 57). Así se ampliaron los objetos de protección de las conductas que ya se tipificaban en los arts. 71,[159] 72 y ss., que permanecieron inalterados.

Por ley 26.285 —BO 13/09/07—, se introdujo otra modificación a la LPI que recorta el universo de supuestos típicos en términos de lesividad en el aspecto patrimonial, eximiendo del pago de derechos de autor a la reproducción y distribución de obras científicas o literarias en sistemas

(159) Limito la transcripción a este tipo porque es el básico y dice: "Será reprimido con la pena establecida por el art. 172 del Código Penal el que de cualquier manera y en cualquier forma defraude los derechos de propiedad intelectual que reconoce esta ley". La escala penal conminada en abstracto, por integración, es de un mes a seis años de prisión.

especiales para ciegos y personas con otras discapacidades perceptivas; siempre que la reproducción y distribución sean hechas por entidades autorizadas. Ésto rige también para las obras que se distribuyan por vía electrónica, encriptadas o protegidas por cualquier otro sistema que impida su lectura a personas no habilitadas. El acceso a a las obras protegidas está a cargo de aquellas entidades autorizadas a asignar y administrar las claves de acceso. Conforme el artículo 36,[160] no se aplicará la exención a la reproducción y distribución de obras que se hubieron editado originalmente en sistemas especiales para personas con discapacidades visuales o perceptivas y que se hallen comercialmente disponibles.

Además del software como objeto de la llamada "piratería", hay otras variadas expresiones de propiedad intelectual afectadas. El vocablo se aplica de forma genérica —y despectiva— a todas aquellas personas que descargan archivos con el más diverso material audiovisual desde Internet en forma gratuita y presuntamente violando los derechos emergentes de aquella. En el caso de la música y las películas y programas seriales de televisión, la cantidad de descargas es prácticamente incalculable. La masividad en el uso de los archivos MP3 y MP4, así como de las redes P2P, constituye en verdadero fenómeno social y cultural que lleva a preguntarse si tiene sentido la persecución penal de una conducta socialmente aceptada —¿teoría de la adecuación social?—. Así, Carnevale plantea la necesidad de analizar si realmente estamos frente a un problema social o es una lucha de intereses económicos lo que, sencillamente, está en juego.[161]

Otra norma relacionada de interés es la ley 24.766 —año 1997— de "Confidencialidad sobre información y productos que estén legítimamente bajo control de una persona y se divulgue indebidamente de manera contraria a los usos comerciales honestos". Esta introdujo la protección del secreto de las informaciones de personas físicas o jurídicas almacenadas en medios informáticos —bases de datos—, penándose su ilegítima divulgación con una multa de $ 1500 a $ 90.000 e inhabilitación especial de seis meses a tres años (art. 156); conforme lo establecido por el CP para el delito de violación de secretos. Concretó así la protección de la información secreta, confidencial, de la empresa y personas físicas; conforme al artículo 39 del Acuerdo sobre los Derechos de la Propiedad Intelectual suscripto por nuestro país y aprobado por ley 24.425.

b.2 **Bolivia**: la protección penal del software ha sido recogida a partir del artículo 6° de la ley 1322 de Derechos de Autor, cuyo inc. l indica: "Los programas

(160) Quedó con la siguiente redacción: "Asimismo, advertirán (las obras reproducidas y distribuidas en sistemas especiales) que el uso indebido de estas reproducciones será reprimido con pena de prisión, conforme el art. 172 del Código Penal".

(161) Carnevale, Carlos A., "¿Es posible ser condenado penalmente por descargar música de Internet? – Mp3, P2P y garantías constitucionales", en *el Suplemento de Derecho de la Alta Tecnología de la Biblioteca Jurídica Online* ", [en línea] www.elDial.com.ar, 12/3/08.

de ordenador o computación (soporte lógico o software), bajo reglamentación específica", como obras amparadas por la ley. El artículo 65 indica, con relación a las violaciones al derecho autoral y sus sanciones penales, que los procesos serán de conocimiento de la judicatura penal ordinaria y que las sanciones serán las previstas por el artícu-lo 362[162] del CP.

b.3 **Brasil**: además del artículo 184 del CP, por la ley 7646 —del 18 de diciembre de 1987— se consideró al software un derecho autoral y se consagró un tipo delictivo específico: **Violar derechos de autor de programas de ordenador**; con una pena que puede ser de 6 (seis) meses de detención a 2 (dos) años y multa (art. 35):

Con posterioridad, siguiendo con el marco de protección dentro del derecho autoral, se dictó la Ley de Software 9609/98, reglamentada por decreto 255/98, en la que se tipificó el delito de copia no autorizada de software. Su artículo 12[163] comprende, en opinión de Vianna, tres figuras distintas que, en la jerga informática, se conocen como piratería, *warez* y *crakz*, aun cuando no marca expresamente las diferencias e impresiona haber sido creado atendiendo sólo a la primera.[164] Llama la atención que, para la primera, no se incluye como exigencia típica el ánimo de lucro. Mas, el parág. 1° prevé pena agravada cuando la conducta se realiza para beneficio económico. El *warez*[165] se diferencia por la carencia del pasaje del programa a un medio físico similar. La práctica consiste en poner a disposición en Internet,

(162) Dice: "El que de manera arbitraria y por cualquier medio explotare o dispusiere, publicare o reprodujere una obra literaria, científica o artística, en perjuicio de los derechos de su legítimo autor, siempre que éste hubiera reservado sus derechos o los hubiere inscrito en los registros respectivos, será sancionado con reclusión de tres meses a dos años y multa de treinta a sesenta días".

(163) Dice: *"art. 12. Violar direitos de autor de programa de computador: Pena – Detenção de seis meses a dois anos ou multa. § 1° Se a violação consistir na reprodução, por qualquer meio, de programa de computador, no todo ou em parte, para fins de comércio, sem autorização expressa do autor ou de quem o represente: Pena – Reclusão de um a quatro anos e multa. § 2° Na mesma pena do parágrafo anterior incurre quem vende, expõe à venda, introduz no País, adquire, oculta ou tem em depósito, para fins de comércio, original ou cópia de programa de computador, producido com violação de direito autoral. § 3° Nos crimes previstos neste artigo, somente se procede mediante queixa, salvo: I- quando praticados em prejuízo de entidade de direito público, autarquía, empresa pública, sociedade de encomia mista ou fundação instituída pelo poder público; II- quando, em decorrência de ato delituoso, resultar sonegação fiscal, perda de arrecadação tributária ou prática de quaisquer dos crimes contra a ordem tributária ou contra as relações de consumo. § 4° No caso de inciso II do parágrafo anterior, a exigibilidade do tributo, ou contribuição social e qualquer accesorio, procesar-se-á independentemente de representação.*

(164) Lima Vianna, Túlio, "Dos crimes por computador", en *el portal jurídico "Mundo Jurídico"*, [en línea] www.mundojuridico.adv.br, en 16/04/2003, § 3.

(165) El término proviene de la palabra inglesa "*wares*": mercadería. El cambio de la "s" por la "z", se debe a que en la terminología informal informática el sufijo "z" sirve para identificar todo aquello que es ilegal (ver Vianna, *op. cit.*, § 3.2).

en algún servidor gratuito, el programa para que puedan ser "bajados" o copiados por cualquiera que acceda al sitio. Esta facilitación generalmente no persigue ningún beneficio económico sino que el ilícito se realiza presidido por una concepción ideológica que atribuye a las empresas de software un excesivo ánimo de lucro por el que abusan de sus derechos autorales cobrando precios excesivos. Los *crackz* son pequeños programas que permiten quebrar los códigos de seguridad que limitan el uso de programas de demostración (demos) o de experimentación previa a la compra *(sharewares)*, con lo que los tornan completos sin el pago de los derechos autorales.

b.4 **Chile**: la piratería del software se encuentra regida por la ley 17.336 de Derechos de Autor —año 1970—, varias veces modificada, a la que se incorporaran conceptos como "programa computacional" (art. 3° inc. 16) y "copia de programa computacional" (art. 5° inc. t). Los tipos penales son los arts. 79,[166] 80[167] y 81.[168]

---

(166) Dice: "art. 79. Cometen delito contra la propiedad intelectual y serán sancionados con la pena de presidio menor en su grado mínimo y multa de 5 a 50 unidades tributarias mensuales:
a) Los que, sin estar expresamente facultados para ello, utilicen obras de dominio ajeno protegidas por esta ley, inéditas o publicadas, en cualquiera de las formas o por cualquiera de los medios establecidos en el art. 18;
b) Los que, sin estar expresamente facultados para ello, utilicen las interpretaciones, producciones y emisiones protegidas de los titulares de los derechos conexos, con cualquiera de los fines o por cualquiera de los medios establecidos en el Título II de esta ley;
c) Los que falsifiquen obras protegidas por esta ley, sean literarias, artísticas o científicas, o las editen, reproduzcan o vendan ostentando falsamente el nombre del editor autorizado, suprimiendo o cambiando el nombre del autor o el título de la obra, o alterando maliciosamente su texto;
d) Los que, obligados al pago de retribución por derecho de autor o conexos derivados de la ejecución de obras musicales, omitieren la confección de las planillas de ejecución correspondiente; y
e) Los que falsificaren o adulteraren una planilla de ejecución".

(167) Su texto: "art. 80. Cometen, asimismo, delito contra la propiedad intelectual y serán sancionados con las penas que se indican en cada caso:
a) Los que falsearen el número de ejemplares vendidos efectivamente, en las rendiciones de cuentas a que se refiere el art. 50, serán sancionados con las penas establecidas en el art. 467 del CP, y
b) Los que, en contravención a las disposiciones de esta ley o a los derechos que ella protege, intervengan, con ánimo de lucro, en la reproducción, distribución al público o introducción al país, y los que adquieran o tengan con fines de venta: fonogramas, videogramas, discos fonográficos, cassettes, videocasetes, filmes o películas cinematográficas o programas computacionales.
Los autores serán sancionados con la pena de presidio o reclusión en su grado mínimo, aumentándose en un grado en caso de reincidencia".

(168) Dice: "art. 81. El que a sabiendas publicare o exhibiere una obra perteneciente al patrimonio cultural común bajo un nombre que no sea el del verdadero autor, será penado con una multa de dos a cuatro sueldos vitales anuales, escala A), del departamento de Santiago.
El recurrente puede pedir, además, la prohibición de la venta, circulación o exhibición de los ejemplares".

b.5. **Colombia**: la "violación de los derechos morales de autor" se encuentra prevista en el artículo 270 del CP,[169] reformado por ley 890 del 10 de enero de 2004, incluyendo expresas a menciones programas de ordenador y soportes lógicos.

b.6 **Ecuador**: en su Ley de Propiedad Intelectual, ley 83 —año 1998—, los programas de ordenador se consideran "objeto de derechos de autor" (art. 8, inc. k) y gozan de idéntica protección que las obras literarias y demás elementos allí descriptos, lo que se complementa en el art. 28.[170] Los tipos penales, con profusa variedad de conductas alternativas consideradas, se encuentran en los artículos 319 a 325. El artículo 327 introduce circunstancias agravantes especiales. El primero, tipo básico que abre el capítulo, prevé una pena de 3 meses a 3 años de prisión y multa de 500 a 5000 unidades de valor constante (UVC).

b.7 **Paraguay**: rige el artículo 184[171] del CP —año 1998—, en función de la ley 1328/1998 "De Derecho de Autor y Derechos Conexos".

---

(169) Su texto: "Incurrirá en prisión de treinta y dos (32) a noventa (90) meses y multa de veinte seis punto sesenta y seis (26.66) a trescientos (300) salarios mínimos legales mensuales vigentes quien:

1. Publique, total o parcialmente, sin autorización previa y expresa del titular del derecho, una obra inédita de carácter literario, artístico, científico, cinematográfico, audiovisual o fonograma, programa de ordenador o soporte lógico.
2. Inscriba en el registro de autor con nombre de persona distinta del autor verdadero, o con título cambiado o suprimido, o con el texto alterado, deformado, modificado o mutilado, o mencionando falsamente el nombre del editor o productor de una obra de carácter literario, artístico, científico, audiovisual o fonograma, programa de ordenador o soporte lógico.
3. Por cualquier medio o procedimiento compendie, mutile o transforme, sin autorización previa o expresa de su titular, una obra de carácter literario, artístico, científico, audiovisual o fonograma, programa de ordenador o soporte lógico.

Parágrafo: Si en el soporte material, carátula o presentación de una obra de carácter literario, artístico, científico, fonograma, videograma, programa de ordenador o soporte lógico, u obra cinematográfica se emplea el nombre, razón social, logotipo o distintivo del titular legítimo del derecho, en los casos de cambio, supresión, alteración, modificación o mutilación del título o del texto de la obra, las penas anteriores se aumentarán hasta en la mitad".

(170) Dice: "Los programas de ordenador se consideran obras literarias y se protegen como tales. Dicha protección se otorga independientemente de que hayan sido incorporados en un ordenador y cualquiera sea la forma en que estén expresados, ya sea en forma legible por el hombre (código fuente) o en forma legible por máquina (código objeto), ya sean programas operativos y programas aplicativos, incluyendo diagramas de flujo, planos, manuales de uso, y en general, aquellos elementos que conformen la estructura, secuencia y organización del programa".

(171) Tiene la siguiente redacción: "Artículo 184. Violación del derecho de autor o inventor. 1° El que sin autorización del titular: 1) divulgara, promocionara, reprodujera o públicamente representara una obra de literatura, ciencia o arte, protegida por el derecho de autor; o 2) exhibiera públicamente el original o una copia de una obra de las artes plásticas o visuales, protegida por el derecho de autor, será castigado con pena privativa de libertad de hasta tres años o con multa. 2° A las obras señaladas en el inciso anterior se equipararán los arreglos y otras adaptaciones protegidas por el derecho de autor. 3° Con la misma pena será castigado el que falsificara, imitara o, sin autorización del titular: 1) promocionara una marca, un dibujo

b.8 **Perú**: en su CP de 1991 se protegen los derechos intelectuales —Título VII—, distinguiendo los de autor y conexos —capítulo I— y la propiedad industrial —capítulo II—. El tipo genérico de fabricación o uso no autorizado de patente es protegido por el artículo 222; con versión actualizada, en la que se incluyen nuevas tecnologías.

En cuanto al capítulo I, la copia o reproducción no autorizada se prevé en el art. 216 con una redacción abierta "u otro medio". La falta de mención de aspectos vinculados a las TIC se mantiene en el resto del articulado, a excepción del art. 218, (172) inc. d, que tipifica el plagio y la comercialización; y el art. 220-A, (173) referido a la elusión de medidas tecnológicas efectivas; 220-B, (174) referido a los productos destinados a eludir medidas tecnológicas; 220-C, (175) referido a los servicios destinados a la elusión de medidas tecnológicas; 220-E,[176] referido a las etiquetas, carátulas

---

o un modelo industrial o un modelo de utilidad, protegidos; o 2) utilizara una invención protegida por patente. 4º La persecución penal del hecho dependerá de la instancia de la víctima. 5º En caso de condena a una pena se aplicará, a petición de la víctima o del ministerio público, lo dispuesto en el art. 60".

(172) La parte pertinente dice: "d. Se fabrique, ensamble, importe, exporte, modifique, venda, alquile, ofrezca para la venta o alquiler, o ponga de cualquier otra manera en circulación dispositivos, sistemas tangibles o intangibles, esquemas o equipos capaces de soslayar otro dispositivo destinado a impedir o restringir la realización de copias de obras, o a menoscabar la calidad de las copias realizadas, o capaces de permitir o fomentar la recepción de un programa codificado, radiodifundido o comunicado en otra forma al público, por aquellos que no están autorizados para ello".

(173) Dice: "El que, con fines de comercialización u otro tipo de ventaja económica, eluda sin autorización cualquier medida tecnológica efectiva que utilicen los productores de fonogramas, artistas, intérpretes o ejecutantes, así como los autores de cualquier obra protegida por derechos de propiedad intelectual, será reprimido con pena privativa de libertad no mayor de dos años y de diez a sesenta días multa".

(174) Dice: "El que, con fines de comercialización u otro tipo de ventaja económica, fabrique, importe, distribuya, ofrezca al público, proporcione o de cualquier manera comercialice dispositivos, productos o componentes destinados principalmente a eludir una medida tecnológica que utilicen los productores de fonogramas, artistas intérpretes o ejecutantes, así como los autores de cualquier obra protegida por derechos de propiedad intelectual, será reprimido con pena privativa de libertad no mayor de dos años y de diez a sesenta días-multa".

(175) Su texto: "El que, con fines de comercialización u otro tipo de ventaja económica, brinde u ofrezca servicios al público destinados principalmente a eludir una medida tecnológica efectiva que utilicen los productores de fonogramas, artistas intérpretes o ejecutantes, así como los autores de cualquier obra protegida por derechos de propiedad intelectual, será reprimido con pena privativa de libertad no mayor de dos años y de diez a sesenta días-multa".

(176) Con esta redacción: "El que fabrique, comercialice, distribuya o almacene con fines comerciales etiquetas o carátulas no auténticas adheridas o diseñadas para ser adheridas a un fonograma, copia de un programa de ordenador, documentación o empaque de un programa de ordenador o a la copia de una obra cinematográfica o cualquier otra obra audiovisual, será reprimido con pena privativa de libertad no menor de tres años ni mayor de seis años y de sesenta a ciento veinte días-multa".

y empaques; y 220-F,[177] referido a los manuales, licencias u otra documentación, o empaques no auténticos relacionados a programas de ordenador. Éstos fueron reformados por ley 29.263 el 2 de octubre de 2008.

b.9 **Uruguay**: el 13 de enero de 2003 se promulgó la Ley de Protección del Derecho de Autor y Derechos Conexos, ley 17.616, que modifica el texto de la ley 9739 —año1937—. Se incluyó, así, al software como una de las obras objeto de su protección, regulando de esta forma su reproducción ilícita. También modificó los delitos relativos a violaciones a los derechos de autor. De tal suerte, el artículo 46 de la ley 9739[178] establece que: quien edite, venda, reproduzca o hiciere reproducir por cualquier medio o instrumento —total o parcialmente—, distribuya, almacene para distribuir al público o ponga a disposición del mismo en cualquier forma o medio con ánimo de lucro o de causar un perjuicio injustificado, una obra programa de ordenador inédita o publicada sin la autorización escrita de su respectiva titular, contraviniendo en cualquier forma lo dispuesto en la ley; será castigado con pena de tres meses de prisión a tres años de penitenciaría.

Por otra parte, quien reproduzca o hiciere reproducir por cualquier medio o procedimiento, sin ánimo de lucro o de causar un perjuicio injustificado un programa de ordenador sin la autorización escrita de su respectivo titular, será castigado con multa de 10 UR a 1500 UR. Se han agregado por la ley 17.616 otras figuras delictivas referidas a medidas tecnológicas e información sobre la gestión de derechos. Serán sancionados con pena de tres meses de prisión a tres años de penitenciaría en primer lugar, quien fabrique, importe, venda, dé en arrendamiento o ponga de cualquier otra manera en circulación dispositivos o productos, sus componentes o herramientas. En segundo lugar, quien preste cualquier servicio cuyo propósito sea impedir, burlar, eliminar, desactivar o eludir de cualquier forma los dispositivos técnicos que los titulares hayan dispuesto para proteger sus respectivos derechos. En tercer lugar, quien altere o suprima, sin autorización del titular de los derechos protegidos por dicha ley, la información electrónica colocada por los titulares de los derechos de autor o conexos, para posibilitar la gestión de sus derechos patrimoniales y morales; de modo que puedan perjudicarse estos derechos. Con idéntica sanción, en cuarto lugar, pune a quien distribuya, importe con fines de distribución, emita o comunique al público, sin autorización, ejemplares de obras, interpretaciones o fonogramas; sabiendo que la información electrónica colocada por los titulares de derechos de autor o conexos ha sido suprimida o alterada sin autorización.

(177) Su texto: "El que elabore, comercialice, distribuya, almacene, transporte, transfiera o de otra manera disponga con fines comerciales u otro tipo de ventaja económica manuales, licencias u otro tipo de documentación, o empaques no auténticos para un programa de ordenador, será reprimido con pena privativa de libertad no menor de cuatro años ni mayor de seis años y de sesenta a ciento veinte días multa".

(178) Ver art. 15, ley 17.616

b.10 **Venezuela**: el capítulo V —"De los delitos contra el orden económico"— de la LECDI —año 2001— prevé las figuras de apropiación de propiedad intelectual (art. 25)[179] y oferta engañosa (art. 26).[180]

6. Otras formas de responsabilidad y sanción

La sección del derecho penal material finaliza con el Título 5, "Otras formas de responsabilidad y sanción", constituida por tres artículos en los que se incursiona en temas propios de la parte general del derecho penal.

6.1. Tentativa y complicidad (art. 11)

En el artículo 11,[181] "Tentativa y complicidad", el primer parágrafo requiere la adopción de reglas de extensión de responsabilidad con relación a

(179) Su texto: "Apropiación de propiedad intelectual. Quien sin autorización de su propietario y con el fin de obtener algún provecho económico, reproduzca, modifique, copie, distribuya o divulgue un software u otra obra del intelecto que haya obtenido mediante el acceso a cualquier sistema que utilice tecnologías de información, será sancionado con prisión de uno a cinco años y multa de cien a quinientas unidades tributarias".

(180) Su texto: "Oferta engañosa. Toda persona que ofrezca, comercialice o provea de bienes o servicios, mediante el uso de tecnologías de información, y haga alegaciones falsas o atribuya características inciertas a cualquier elemento de dicha oferta, de modo que pueda resultar algún perjuicio para los consumidores, será sancionada con prisión de uno a cinco años y multa de cien a quinientas unidades tributarias, sin perjuicio de la comisión de un delito más grave".

(181) Tiene la siguiente redacción: "Artículo 11 - Tentativa y complicidad

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, cualquier acto de complicidad que sea cometido dolosamente y con la intención de favorecer la perpetración de alguna de las infracciones establecidas en los arts. 2 a 10 del presente Convenio.
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, la tentativa dolosa de cometer una de las infracciones establecidas en los arts. 3 a 5, 7, 8, 9 (1) a y 9 (1) c del presente Convenio.
3. Las Partes podrán reservarse el derecho de no aplicar, en todo o en parte, el párrafo 2 del presente artículo". Esta propuesta, incluyendo la "inducción", fue reafirmada mediante la Decisión Marco 2005/222/JAI del Consejo, de 24 de febrero de 2005, relativa a los ataques contra los sistemas de información, con esta redacción: "Artículo 5. Inducción, complicidad y tentativa. 1) Cada Estado miembro garantizará que la inducción a los delitos contemplados en los arts. 2, 3 y 4 y la complicidad con ellos sean sancionables como infracciones penales. 2) Cada Estado miembro garantizará que la tentativa de cometer los delitos mencionados en los arts. 2, 3 y 4 sea sancionable como infracción penal. 3) Cada Estado miembro podrá decidir que no se aplique el apart. 2 a las infracciones mencionadas en el art. 2". Fue sustituido por el art. 8 de la Directiva 2013/40/UE del Parlamento Europeo y del Consejo de 12 de agosto de 2013 relativa a los ataques contra los sistemas de información, con similar redacción y remisión a sus propios arts. 3 a 7. Vale resaltar que los mencionados arts. 2, 3 y 4 de la DM de 2005, eran equivalentes a los arts. 2, 4 y 5 del Convenio de Budapest, mientras que los arts. 3 a 7 de la Directiva de 2013 se corresponden con los arts. 2 a 6 del CB.

los actos de complicidad dolosa y con intención de favorecer la perpetración de alguna de las conductas infractoras anteriores; lo que no provoca niguna necesidad de modificación local en la medida de que todos los códigos latinoamericanos contemplan dispositivos de amplificación típica en materia de participación. El segundo párrafo impulsa el adelantamiento de la intervención penal al momento de perfeccionarse la tentativa dolosa de los tipos previstos en los artículos 3° a 5°, 7° a 9.1.a y 9.1.c; aunque el tercer párrafo prevé la posible reserva total o parcial en este aspecto —no en relación al primero—. Entiendo que la situación es similar a la anterior. Aun cuando, excepcionalmente, en alguna de las legislaciones comparadas se ha optado por incluir en el mismo tipo de la parte especial —así, Paraguay—, la aclaración de su punición a título de tentativa en nuestros códigos; se incorpora, como previsión de la parte general, este otro mecanismo amplificador de la tipicidad al inicio de los actos de ejecución en supuestos en que la consumación no se perfecciona por razones ajenas a la voluntad del agente. Suele también acompañarse de una escala de pena reducida.

6.2. Responsabilidad de las personas jurídicas (art. 12)

En el artículo 12,[182] "Responsabilidad de las personas jurídicas"; que requiere que se adopten medidas internas que permitan responsabilizar a las personas de existencia ideal por las anteriores infracciones, sin perjuicio de la responsabilidad penal que corresponda a las personas físicas que las integran; ha evitado todo problema en el nivel nacional habida cuenta que el tercer inciso, respetuoso de los principios jurídicos propios de cada estado signatario, admite su resolución como penal, civil o administrativa. De tal suerte, si bien pueden mediar diferencias en la forma que conside-

(182) Dice: "Artículo 12 – Responsabilidad de las personas jurídicas.

1) Las Partes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias para permitir que las personas jurídicas puedan ser tenidas por responsables de las infracciones establecidas en el presente Convenio, cuando éstas sean cometidas por una persona física, actuando ya sea a título individual, ya sea como miembro de un órgano de la persona jurídica, que ejerce un poder de dirección en su seno, cuyo origen se encuentre en:
   a. un poder de representación de la persona jurídica;
   b. una autorización para tomar decisiones en nombre de la persona jurídica;
   c. una autorización para ejercer control en el seno de la persona jurídica.
2) Fuera de los casos previstos en el párrafo 1, las Partes adoptarán las medidas necesarias para asegurar que una persona jurídica puede ser tenida por responsable cuando la

ran esta responsabilidad en los distintos países, no hay conflicto con los requerimientos del Convenio.

En relación con lo anterior, Silva Sánchez comenta que un texto como éste no resulta una verdadera novedad en el ámbito de los documentos internacionales, donde pueden encontrarse otros que se refieren con mayor amplitud a los entes ideales y con mayor restricción en cuanto consagran exclusivamente responsabilidad a título penal —artículo 14 del "*Corpus Juris*", año 1997, o artículo 13, año 2000 —. En este sentido, califica a la previsión del Convenio —en cuanto no "impone" una "naturaleza jurídica"—como consagratoria de un modelo relativamente abierto de responsabilidad directa y acumulativa —no subsidiaria y alternativa—, de las personas jurídicas.(183)

---

ausencia de vigilancia o de control por parte de cualquier persona física mencionada en el párrafo 1 haya permitido la comisión de las infracciones descritas en el párrafo 1 a través de una persona física que actúa bajo autorización de la persona jurídica.

3) La responsabilidad de la persona jurídica podrá resolverse en sede penal, civil o administrativa, dependiendo de los principios jurídicos propios del Estado.

4) Esta responsabilidad se establecerá sin perjuicio de la responsabilidad penal de las personas físicas que hayan cometido la infracción".

La propuesta fue reafirmada mediante la DM 2005/222/JAI del Consejo, de 24 de febrero de 2005, relativa a los ataques contra los sistemas de información, con esta redacción: "Artículo 8. Responsabilidad de las personas jurídicas. 1) Cada Estado miembro adoptará las medidas necesarias para que a las personas jurídicas se les puedan exigir responsabilidades por las infracciones mencionadas en los arts. 2, 3, 4 y 5, cuando dichas infracciones sean cometidas en su beneficio por cualquier persona, actuando a título particular o como parte de un órgano de la persona jurídica, que ostente un cargo directivo en el seno de dicha persona jurídica basado en: a) un poder de representación de dicha persona jurídica, o b) una autoridad para tomar decisiones en nombre de dicha persona jurídica, o c) una autoridad para ejercer un control en el seno de dicha persona jurídica. 2) Sin perjuicio de los casos previstos en el apartado 1, los Estados miembros garantizarán que a las personas jurídicas se les puedan exigir responsabilidades cuando la falta de vigilancia o control por parte de alguna de las personas a que se refiere el apart. 1 haya hecho posible que una persona sometida a su autoridad cometa las infracciones mencionadas en los arts. 2, 3, 4 y 5 en beneficio de esa persona jurídica. 3) La responsabilidad de las personas jurídicas en virtud de los aparts. 1 y 2 se entenderá sin perjuicio de la incoación de acciones penales contra las personas físicas que sean autores, incitadores o cómplices en la comisión de las infracciones mencionadas en los arts. 2, 3, 4 y 5". Fue sustituido por el art. 10 de la Directiva 2013/40/UE del Parlamento Europeo y del Consejo de 12 de agosto de 2013 relativa a los ataques contra los sistemas de información, con similar redacción y remisión a sus propios arts. 3 a 8.

(183) Silva Sánchez, Jesús-María, "La responsabilidad penal de las personas jurídicas en el Convenio del Consejo de Europa sobre cibercriminalidad", en Morales García (dir.), *Delincuencia Informática. Problemas de responsabilidad*, *Cuadernos de Derecho Judicial IX-2002*, Madrid, Consejo General del Poder Judicial, 2002, pp. 116/117 y 120/121.

Puede anotarse que la ley especial venezolana del año 2001 —sin dudas, la más extensa en la región— incorporó una previsión expresa relativa a la responsabilidad de las personas jurídicas: su art. 5.[184] En la base se encontraría el reconocimiento de la singular importancia que tienen las diferentes clases de prestadores de servicio en la estructura y configuración de la red telemática. No son otra cosa que grandes empresas que se benefician y, a la vez, tienen una cierta cuota de responsabilidad —co-responsabilidad— en el control de asuntos, objetos o servicios ofrecidos cotidianamente por Internet. Esto obliga, al decir de Aboso y Zapata, a replantearse la responsabilidad penal de las personas de existencia ideal, en muchos países sistemáticamente negada al calor del aforismo romano *societas delinquere non potest.*[185]

6.3. Sanciones y medidas (art. 13)

Finalmente, el artículo 13[186], "Sanciones y medidas", tal como se enfatizó en la introducción, brinda pautas genéricas acerca del tipo de sanciones

(184) Dice: "Responsabilidad de las personas jurídicas. Cuando los delitos previstos en esta Ley fuesen cometidos por los gerentes, administradores, directores o dependientes de una persona jurídica, actuando en su nombre o representación, éstos responderán de acuerdo con su participación culpable. La persona jurídica será sancionada en los términos previstos en esta Ley, en los casos en que el hecho punible haya sido cometido por decisión de sus órganos, en el ámbito de su actividad, con sus recursos sociales o en su interés exclusivo o preferente".

(185) Aboso, Gustavo E.; Zapata, María F., *Cibercriminalidad y derecho penal*, Bs. As., BdeF, 2006, p. 211.

(186) Su texto: "Artículo 13 – Sanciones y medidas.

1) Las Partes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias para permitir que las infracciones penales establecidas en los arts. 2 a 11 sean castigadas con sanciones efectivas, proporcionadas y disuasorias, incluidas las penas privativas de libertad.
2) Las Partes velarán para que las personas jurídicas que hayan sido declaradas responsables según lo dispuesto en el art. 12 sean objeto de sanciones o medidas penales o no penales efectivas, proporcionadas y disuasorias, incluidas las sanciones pecuniarias".

Con mayor detalle tanto respecto de personas físicas como jurídicas y endureciendo las penas, la propuesta fue reafirmada mediante la DM 2005/222/JAI del Consejo, de 24 de febrero de 2005, a través de sus arts. 6, 7 y 9, que llega a incluir escalas de sanciones de privación de libertad y circunstancias agravantes en algunos casos. Fueron sustituidos por los arts. 9 (que fusiona y amplía los mencionados 6 y 7 de la DM) y 11 de la Directiva 2013/40/UE del Parlamento Europeo y del Consejo de 12 de agosto de 2013 relativa a los ataques contra los sistemas de información.

Limito la transcripción a los ahora vigentes: "Artículo 9. Sanciones. 1) Los Estados miembros adoptarán las medidas necesarias para garantizar que las infracciones mencionadas en los arts. 3 a 8 se castiguen con penas efectivas, proporcionadas y disuasorias. 2) Los Estados miembros adoptarán las medidas necesarias para garantizar que las infracciones mencionadas en los arts. 3 a 7 se castiguen con sanción máxima de privación de libertad

que los Estados deben adoptar para punir las infracciones penales descriptas en los artículos 2° a 11. Éstas deben ser efectivas, proporcionadas y disuasorias. Se admiten las penas privativas de libertad con relación a las personas físicas (primer párrafo), así como las pecuniarias respecto de las personas jurídicas (segundo párrafo).

En cuanto a las últimas como sujeto de sanción, Silva Sánchez destaca que la utilización de este término sugiere que se prescribe un modelo de responsabilidad más allá de lo estrictamente reparatorio. Por lo que concluye que un modelo de exclusiva responsabilidad civil compensatoria no cumpliría las exigencias del Convenio. Así, estima que dicho Convenio situaría el mínimo de lo "proporcionado, efectivo y disuasorio" en el empleo, al menos, de una indemnización sancionatoria —*punitive damages*—.(187)

Un rápido repaso de la cuantiosa normativa a la que nos referimos en este trabajo revela que, lejos de ser una excepción, la pena privativa de libertad

---

igual o superior a dos años, al menos en los casos que no sean de menor gravedad. 3) Los Estados miembros adoptarán las medidas necesarias para garantizar que, cuando se hayan afectado a un número significativo de sistemas de información o cuando para cometerlas se haya utilizado uno de los instrumentos a que se refiere el art. 7, las infracciones mencionadas en los arts. 4 y 5, se castiguen con una sanción máxima de privación de libertad de al menos tres años. 4) Los Estados miembros adoptarán las medidas necesarias para garantizar que las infracciones mencionadas en los arts. 4 y 5 se castiguen con una sanción máxima de privación de libertad de al menos cinco años cuando: a) se cometan en el contexto de una organización delictiva con arreglo a la Decisión marco 2008/841/JAI, con independencia del nivel de la sanción que se establezca en la misma; b) causen daños graves, o c) se cometan contra el sistema de información de una infraestructura crítica. 5) Los Estados miembros tomarán las medidas necesarias para garantizar que, cuando las infracciones a que se refieren los arts. 4 y 5 sean cometidas utilizando ilícitamente datos de carácter personal de otra persona con la finalidad de ganar la confianza de un tercero, causando así daños al propietario legítimo de la identidad, ello pueda ser considerado, de conformidad con el Derecho nacional, como circunstancia agravante, a menos que tal circunstancia ya esté contemplada con otra infracción que sea sancionable con arreglo al Derecho nacional"; y "Art. 11. Sanciones contra las personas jurídicas. 1) Los Estados miembros adoptarán las medidas necesarias para garantizar que a la persona jurídica considerada responsable en virtud de lo dispuesto en el art. 10, apart. 1, le sean impuestas sanciones efectivas, proporcionadas y disuasorias, que incluirán multas de carácter penal o de otro tipo, y entre las que podrán incluir otras sanciones como: a) exclusión del disfrute de ventajas o ayudas públicas; b) inhabilitación temporal o permanente para el ejercicio de actividades comerciales; c) vigilancia judicial; d) medida judicial de liquidación; e) cierre temporal o definitivo de los establecimientos utilizados para cometer la infracción. 2) Los Estados miembros adoptarán las medidas necesarias para garantizar que a la persona jurídica considerada responsable en virtud de lo dispuesto en el art. 10, apart. 2, le sean impuestas sanciones o medidas efectivas, proporcionadas y disuasorias".

(187) Sánchez, *op. cit.*, p. 122.

—con distintas denominaciones y extensión; prisión, reclusión, detención, presidio— es la más asiduamente utilizada; ya sea sola o conjunta con la de multa o con la de inhabilitación especial, o alternativa con la de multa o la de prestación de servicios comunitarios. Salvo en el caso del CP de Paraguay, que responde con claridad al modelo alemán y, por lo tanto, sólo establece el tope máximo de privación de libertad posible; en los demás las escalas son fijadas con un mínimo y máximo determinados o mediante una regla de determinación derivada —así, el CP de Chile, de mayor semejanza con el sistema español—.

En muy pocos casos se prevé sólo multa. Esta pena a veces se expresa directamente en una cantidad variable de moneda de curso legal del país de que se trate y, en otras, remite a alguna otra unidad determinativa. Por ejemplo, "unidades tributarias", "unidades reajustables", "salarios mínimos legales mensuales" o "días-multa".

7. Recapitulación final

Sin perjuicio de insistir en todas las prevenciones formuladas al inicio, la tabla que seguidamente se incorpora permite visualizar de un modo claro y sencillo el resultado del ejercicio comparativo entre el Convenio de Budapest y las legislaciones de los países miembros plenos o asociados del MERCOSUR.

Los encasillamientos propuestos son tendenciales, basados particularmente en la adopción de reformas o modificaciones legales que incorporaron nuevas tipicidades o actualizaron otras anteriormente vigentes. Pero ello no descarta la posibilidad de que la carencia u omisión de normativa de moderna factura no se traduzca en forma directa en atipicidad ya que, en muchos casos, es factible que por vía interpretativa de la redacción de tipos previos a la irrupción de las TIC se dé solución a nivel local a eventuales lagunas de punición.

Esta última situación puede entonces operar como una suerte de efecto ralentizador de la actividad legislativa tendiente a armonizar el derecho interno a la propuesta convencional.

En principio, puede decirse que Argentina, Paraguay y Venezuela no ofrecerían déficit de tipificación alguno en confronte con las demandas de Budapest. En el otro extremo, Bolivia y Uruguay serían los Estados que necesitarían una urgente actualización para entrar en sintónica armonía

con los restantes. En ambos hay proyectos de reforma en consideración en la actualidad.

a. No obstante, como primera observación, es dable concluir que, la región del MERCOSUR no ofrece mayores problemas para su integración con los restantes signatarios del Convenio europeo en materia de derecho penal material.

La síntesis gráfica de la comparación entre la Sección 1 del II del Convenio de Budapest y las legislaciones de la región queda expresada del siguiente modo:

CUADRO 1. CONVENIO DE BUDAPEST Y LEGISLACIONES COMPARADAS. SÍNTESIS DE COMPARACIÓN

Budapest	Art. 2	Art. 3	Art. 4	Art. 5	Art. 6	Art. 7	Art. 8	Art. 9	Art. 10
Argentina	sí	sí	sí	sí	sí	sí	sí	sí	sí
Bolivia	sí	no	sí	no	no	no	si	no	sí
Brasil	no	sí	sí	sí	si	sí	no	si	sí
Chile	no	sí	si	no	no	sí	sí	sí	sí
Colombia	sí	sí	sí	sí	sí	no	sí	sí	sí
Ecuador	sí	sí	sí	sí	no	no	sí	sí	sí
Paraguay	sí	sí	sí	sí	sí	sí	sí	sí	sí
Perú	sí	sí	sí	sí	sí	no	sí	sí	sí
Uruguay	no	sí	no	no	no	sí	no	sí	sí
Venezuela	sí	sí	sí	sí	sí	sí	sí	sí	sí

Referencias: Art. 2= Acceso ilícito; Art. 3= Interceptación ilícita; Art. 4= Atentados contra la integridad de los datos; Art. 5= Atentados contra la integridad del sistema; Art. 6= Abuso de equipos e instrumentos técnicos; Art. 7= Falsedad informática; Art. 8= Estafa informática; Art. 9= Infracciones relativas a la pornografía infantil; Art. 10= Infracciones vinculadas a los atentados a la propiedad intelectual y derechos afines.

b. Con relación a la forma en que se penan las infracciones contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas

informáticos —Título 1—, si bien resulta clara la uniformidad en cuanto al uso de la pena privativa de libertad como principal modo de respuesta; puede advertirse rápidamente la diversidad con que en general se recibe el genérico mandato del art. 13: las sanciones han de ser "efectivas, proporcionadas y disuasorias" habida cuenta las disímiles escalas conminadas en abstracto, así como las variantes en alternatividad o conjunción con otras modalidades de penas. Con la misma advertencia del punto anterior acerca de volcarse una respuesta tendencial por las razones allí expuestas, pueden destacarse las siguientes observaciones particulares:

b.1 Acceso ilícito (art. 2°): Bolivia es el único que no admite pena privativa de libertad. En cambio, prevé penas de prestación de trabajo o multa. Todos los demás contemplan pena privativa de libertad. Argentina es el único que la prevé en forma exclusiva. Paraguay admite la posibilidad alternativa de multa. Perú admitía la alternativa de prestación de servicios comunitarios, pero con la ley 30.096 de octubre de 2013 ahora mantiene la pena privativa de libertad y días multa como sanción conjunta. Finalmente; Colombia, Ecuador y Venezuela prevén aplicación conjunta de prisión y multa.

b.2 Interceptación ilícita (art. 3°): en este caso, todos contemplan pena privativa de libertad. Argentina, Chile, Colombia, Perú y Uruguay, de forma exclusiva. Paraguay admite la posibilidad alternativa de multa. En cambio, Brasil, Ecuador y Venezuela prevén aplicación conjunta de prisión y multa.

b.3 Atentados contra la integridad de los datos (art. 4°): nuevamente Bolivia es el único que no admite pena privativa de libertad sino que prevé las de prestación de trabajo o multa. Los demás contemplan pena privativa de libertad. Argentina y Chile, de forma exclusiva. Paraguay admite la posibilidad alternativa de multa. Brasil, en algunos tipos, admite la multa conjunta y, en otros, alternativa. Por último, Colombia, Ecuador, Perú y Venezuela prevén aplicación conjunta de prisión y multa.

b.4 Atentados contra la integridad del sistema (art. 5°): respecto de esta conducta, todos contemplan pena privativa de libertad. Argentina lo hace de forma exclusiva, mientras que Paraguay admite la posibilidad alternativa de multa. Por su lado, Brasil, Colombia, Ecuador, Perú y Venezuela prevén aplicación conjunta de prisión y multa.

b.5 Abuso de equipos e instrumentos técnicos (art. 6°): nuevamente todos prevén como sanción la pena privativa de libertad, Argentina es el único que lo hace en forma exclusiva y Paraguay admite la posibilidad alternativa de multa. Brasil, Colombia, Perú y Venezuela prevén aplicación conjunta de prisión y multa.

Lo expuesto se sintetiza gráficamente en el cuadro que sigue:

CUADRO 2. PENAS CONTRA LAS INFRACCIONES. SÍNTESÍS GRÁFICA. ARTS. 2 A 6

Budapest	Art. 2	Art. 3	Art. 4	Art. 5	Art. 6
Argentina	P 15D a 2A	P 15D a 1A	P 15D a 6A	P 6M a 2A	P 15D a 1A
Bolivia	pT hasta 1A o M hasta 200D	no	PT hasta 1A o M hasta 200D	no	no
Brasil	no	P 2 a 4A y M	P 1M a 12A y/o M	P 1M a 3A y M	P 3M a 1A y M
Chile	no	P menor grado mín. a medio	P menor grado mín. a máximo	no	no
Colombia	P 48 a 96M y M 100 a 1000S	P 36 a 72M	P 48 a 96M y M 100 a 1000S	P 48 a 96M y M 100 a 1000S	P 48 a 96M y M 100 a 1000S
Ecuador	P 1 a 3A y M 1000 a 1500 u$s	P 2M a 9A y M 1000 a 10000 u$s	P 6M a 6A y M 60 a 600 u$s	P 8M a 4A y M 200 a 600 u$s	no
Paraguay	P hasta 3A o M	P hasta 3A o M	P hasta 5A o M	P hasta 5A o M	P hasta 1A o M
Perú	P 1A a 4A y 30 a 90 DM	P 3A hasta 10A	P 3A a 6A y 80 a 120 DM	P 3A a 6A y 80 a 120 DM	P 1A a 4A y 20 a 60 DM
Uruguay	no	P 3M a 3A	no	no	no
Venezuela	P 1 a 5A y M 10 a 50 UT	P 3 a 6A y M 300 a 600 UT	P 2 a 10A y M 200 a 1000 UT	P 2 a 10A y M 200 a 1000 UT	P 3 a 6A y M 300 a 600 UT

Aclaración: en el caso de países en los que concurren varios tipos a cubrir el pertinente artículo del Convenio de Budapest, la escala se formó con el mínimo menor y el máximo mayor posibles; considerando tipos básicos y especiales, y sin incluir agravantes genéricos. Tampoco se incorporaron ni consideraron las muy comunes sanciones de inhabilitación cuando el hecho es cometido por funcionario o persona encargada de la custodia, o el decomiso de los elementos del delito.

Referencias: Art. 2= Acceso ilícito; Art. 3= Interceptación ilícita; Art. 4= Atentados contra la integridad de los datos; Art. 5= Atentados contra la integridad del sistema; Art. 6= Abuso de equipos e instrumentos técnicos.

Abreviaturas: P= privación de libertad (prisión, reclusión, detención, presidio, penitenciaría); "x" D= cantidad de días; "x" M= cantidad de meses; "x" A= cantidad de años; PT= prestación de trabajo; M= multa; DM= días-multa; "x" S= cantidad de salarios; "x" J= cantidad de jornadas; UT= unidades tributarias; UVC= unidad de valor constante.

c. Con relación a la forma en que se penan las infracciones informáticas, de contenido o contra la propiedad intelectual y derechos afines (Títulos 2, 3, y 4), reiterando la advertencia genérica, se mantiene idéntica observación en cuanto a la uniformidad en el uso de la pena privativa de libertad como principal modo de respuesta y diversidad para recibir el genérico mandato del art. 13 en orden a que las sanciones han de ser "efectivas, proporcionadas y disuasorias". Sentado ello, pueden destacarse las siguientes particularidades:

c.1 Falsedad informática (art. 7): todos los países contemplan penas con privación de libertad. Argentina,[188] Chile y Uruguay lo prevén en forma exclusiva. Paraguay admite la posibilidad alternativa de multa. Finalmente, Brasil y Venezuela prevén la aplicación conjunta de prisión y multa.

c.2 Estafa informática (art. 8): nuevamente todos contemplan la pena privativa de libertad. Argentina y Chile, de forma exclusiva; Paraguay admite la posibilidad alternativa de multa. Por último; Bolivia, Colombia, Ecuador y Venezuela prevén la aplicación conjunta de prisión y multa.

c.3 Infracciones relativas a la pornografía infantil (art. 9): se mantiene la nota de uso por todos de la pena privativa de libertad que, en este caso, es prevista en forma exclusiva por Argentina, Chile, Ecuador y Uruguay. Paraguay admite la posibilidad alternativa de multa. Brasil, Colombia, Perú y Venezuela prevén aplicar en conjunto prisión y multa.

c.4 Infracciones vinculadas a los atentados a la propiedad intelectual y derechos afines (art. 10): todos prevén la pena privativa de libertad. Argentina y Uruguay en forma exclusiva, en tanto Paraguay admite la posibilidad alternativa de multa. En cambio, la aplicación conjunta de prisión y multa es la opción de Bolivia, Brasil, Chile, Colombia, Ecuador y Venezuela.

CUADRO 3. PENAS CONTRA LAS INFRACCIONES. SINTESÍS GRÁFICA. ARTS. 7 A 10

Budapest	Art. 7	Art. 8	Art. 9	Art. 10
Argentina	P 1 a 6A	P 1M a 6A	P 1M a 4A	P 1M a 6ª
Bolivia	no	P 1 a 5A y M 60 a 200D	no	P 3M a 2A y M 30 a 60D
Brasil	P 1 a 5A y M	no	P 3 a 8A y M	P 6M a 4A y M

(188) Se tomó como referencia la escala del art. 292 del CP.

Budapest	Art. 7	Art. 8	Art. 9	Art. 10
Chile	P menor en cualquier grado	P menor en cualquier grado	P menor grado med. a máx.	P menor grado mín. y M 5 a 50 UT
Colombia	no	P 48 a 120M y M 200 a 1500S	P 10 a 20A y M 150 a 1500S	P 32 a 90M y M 26,66 a 300S
Ecuador	no	P 6M a 5A y M 500 a 2000 u$s	P de 6 a 9A	P 3M a 3A y M 500 a 5000 UVC
Paraguay	P hasta 5A o M	P hasta 5A o M	P hasta 5A o M	P h. 3A o M
Perú	no	P 3A a 10A y 60 a 140 DM	P 6A a 12A y 120 a 365DM	P hasta 6A y 10 a 120DM
Uruguay	P 3 meses a 10 años	no	P 6 meses a 12 años	P 3 meses a 3 años
Venezuela	P 3 a 6 años y M 300 a 600 UT	P 1 a 7 años y M 10 a 700 UT	P 2 a 8 años y M 200 a 800 UT	P 1 a 5 años y M 100 a 500 UT

Aclaración: en el caso de países en los que concurren varios tipos a cubrir el pertinente artículo del Convenio de Budapest, la escala se formó con el mínimo menor y el máximo mayor posibles, considerando tipos básicos y especiales y sin incluir agravantes genéricos. Tampoco se incorporaron ni consideraron las muy comunes sanciones de inhabilitación cuando el hecho es cometido por funcionario o persona encargada de la custodia, o el decomiso de los elementos del delito.

Referencias: Art. 7 = Falsedad informática; Art. 8 = Estafa informática; Art. 9° = Infracciones relativas a la pornografía infantil; Art. 10 = Infracciones vinculadas a los atentados a la propiedad intelectual y derechos afines;

Abreviaturas: "x" D= cantidad de días; "x" M= cantidad de meses; "x" A= cantidad de años; PT= prestación de trabajo; M= multa; DM= días-multa; "x" S= cantidad de salarios; "x" J= cantidad de jornadas; UT= unidades tributarias; UVC= unidad de valor constante.

c. Poco más de una década después del Convenio de Budapest, comienza a surgir el interés en que las legislaciones nacionales incorporen nuevas tipicidades o refuercen las anteriores. Por caso, en la Unión Europea la "Directiva 2013/40/UE del Parlamento y del Consejo de 12 de agosto de 2013 relativa a los ataques contra los sistemas de información", respecto del robo o suplantación de identidad digital.[189] También se propulsa

(189) En Argentina existe un proyecto con trámite parlamentario que fue presentado el 15 de mayo de 2012 por la senadora Higonet (Exp. S N° 1312/12). A partir de éste se incorporaría como artículo 138 *bis* del CP con el siguiente texto: "Será reprimido con prisión de 6 (seis) meses a 3 (tres) años o multa de pesos veinte mil a pesos doscientos mil, el que sin

la incorporación de figuras que capten con más precisión, entre otras conductas disvaliosas; el *grooming*, el *ciber*stalk*ing* o el *ciberbullying*. Serían temas para seguir pensando el fenómeno expansivo del derecho penal. Del otro lado queda sobre todo la necesidad de reflexionar acerca de la racionalidad de seguir usándolo para conductas que tienen un alto grado de aceptación y son muy extendidas socialmente, cuya dañosidad básicamente es de orden patrimonial y que, por lo tanto, bien pudieran ser devueltas al ámbito civil, comercial y, si se quiere mantener una cierta cuota de poder punitivo al derecho sancionador administrativo o contravencional. Me refiero a la actividad *cuasi bagatelar* de agentes como los "manteros" —como se les llama en Latinoamérica— o "top manta/top mochila" —en España—, así como la tan frecuente de intercambio de archivos *on line*.(190)

consentimiento, adquiriere, tuviere en posesión, transfiriere, creare o utilizare la identidad de una persona física o jurídica que no le pertenezca, a través de internet o cualquier otro medio electrónico, y con la intención de dañar, extorsionar, defraudar, injuriar o amenazar a otra persona u obtener beneficio para sí o para terceros".

(190) Este problema ha sido perfectamente captado por Javier A. De Luca, titular de la Fiscalía General N° 4 ante la Cámara Nacional de Casación Penal, en su dictamen N° 7868 en causa "Andrade, Luz María s/recurso de queja", causa N° 16.914 de la Sala I, al desistir del recurso incoado en la etapa previa. El supuesto de hecho comprometía el secuestro de un total de 33 CD de música y 102 películas y videojuegos identificados precariamente todos con fotocopias de los originales, que la imputada comerciaba en la vía pública. Al fundar el desistimiento apuntó que la conducta investigada no constituía delito infractorio a la Ley de Marcas (N° 22.362), por la insignificante lesión al bien jurídico protegida por ésta. Vale aclarar que la presunta infracción a la Ley de Propiedad Intelectual corresponde al fuero común, no al federal, por lo que no entró en consideración en el caso, según se precisa en el propio dictamen. No puedo dejar de señalar que este desdoblamiento es incorrecto y lo que hubiera correspondido es que el fuero de excepción, es decir el federal, se hubiera hecho cargo de toda la imputación y no mantener esta ficcionada separación de lo que no es más que el mismo hecho visto desde dos tipicidades que, a todo evento, no constituiría más que un supuesto de concursalidad aparente.
Por lo demás, criticó De Luca abiertamente la actividad policial diciendo: "La acción de las autoridades en casos como el presente, se limita a la detección y represión de los llamados 'manteros' o vendedores ambulantes de objetos falsificados, a sacarlos de circulación e incautarse de la mercadería, sin realizar el más mínimo esfuerzo pesquisitivo para proseguir hacia arriba en la línea o pirámide delictiva y, así, descubrir y desbaratar a las organizaciones que están detrás de la producción de estos productos imitados que, precisamente, emplean a personas de bajos recursos económicos, sociales y culturales para llevar adelante su comercialización ilegal. Todo se reduce a lo mismo que ha ocurrido con la llamada 'lucha contra las drogas', donde se ha teorizado inclusivo que debe perseguirse a los consumidores porque, al ser los últimos eslabones de la cadena delictiva, con su represión se 'atraerán' (tirando de esa cadena, valga la redundancia) hacia nosotros a los productores y comercializadores. Si esto no fuese un asunto muy serio, realmente asombra por su candidez".

La relación entre la persecución de delitos informáticos y el Derecho Penal Internacional

Delitos informáticos: aspectos de Derecho Penal Internacional[1]

MARCOS SALT[2]

Muchas gracias a los organizadores por la invitación.

A continuación, voy a referirme a la relación entre la persecución de delitos informáticos y el Derecho Penal Internacional. De manera más general, a los cambios que implica o genera la tecnología informática para el sistema de cooperación internacional en materia penal. Tomando en cuenta el escaso tiempo con el que contamos, mi idea es intentar resaltar solamente algunos temas fundamentales que hoy requieren especial atención como forma de dejar "disparadores" para la discusión futura y la preparación de trabajos para la reunión de la AIDP en Brasil. Intentaré enumerar aquellas cuestiones que, desde mi punto de vista, deben ser especialmente analizadas al mo-

(1) Versión corregida de la transcripción de la charla que tuvo lugar en la Facultad de Derecho (UBA). Se agregaron notas a pie sugiriendo lecturas específicas sobre los principales temas planteados.

(2) Abogado especialista en derecho penal, penal económico, derecho procesal penal, y delitos informáticos. Profesor Adjunto de Derecho Penal y Procesal Penal y de Posgrado en la Facultad de Derecho (UBA).

mento de definir una política de cooperación internacional en materia penal en lo que respecta a los delitos informáticos y, de manera más amplia, de cooperación internacional en la investigación de cualquier delito que involucre la necesidad de obtener evidencia digital en una jurisdicción diversa a la de la autoridad que tiene el poder jurisdiccional de llevar a delante la investigación.

1. La relación del tema con la política internacional

En primer lugar, no cabe duda de que la definición de una política de persecución internacional de los delitos informáticos —y más ampliamente, de los delitos cometidos por medios informáticos o de cualquier delito que requiera para su investigación la obtención de evidencia contenida en soportes digitales—, no es hoy solamente un tema jurídico, sino, antes bien, político y de política internacional. No discutimos solamente derecho penal, sino posicionamiento de política internacional.[3] Obviamente, no cabe duda que necesitaremos los instrumentos del derecho penal y procesal penal para su implementación. Pero la discusión y las definiciones están teñidas de aspectos claves para la política internacional del futuro y por importantes intereses económicos. Es por ello que el tema es central no solo en países desarrollados, sino también en ámbitos de organizaciones internacionales como Naciones Unidas, el Consejo de Europa, la Unión Europea y, en el ámbito regional, OEA, UNASUR, MERCOSUR.

Estamos hablando de política internacional en uno de los aspectos claves para las relaciones internacionales del futuro: la regulación de Internet. Un primer tema fundamental, entonces, es cómo se va a posicionar la Argentina en relación a estos movimientos y tensiones que tocan cuestiones tan trascendentales como la idea de soberanía y el principio de territorialidad, la cooperación eficiente e igualitaria entre Estados, la protección de garantías individuales en entornos digitales, la relación con las empresas multinacionales del sector de la informática y las telecomunicaciones, entre otros.

Si bien no resulta sorprendente, sí debemos estar prevenidos respecto del hecho de que la discusión que debería centrarse en la cooperación en materia de "delitos y justicia penal" se empiece a mezclar y "ensuciar" con temas ajenos como la denominada cyberseguridad y seguridad nacional, o el cyberterrorismo, que responden a lógicas distintas y pueden llevar a una extensión peligrosa de pérdida de garantías para el sistema penal de nuestra región.

(3) Salt, Marcos, *"International legal cooperation in cybercrime matters: Challenges for countries of Latin America"*, [en línea] www.coe.int/cybercrime

2. La vinculación con el proceso penal

En lo que tiene que ver con las normas de derecho procesal penal, lo que hay que tener en cuenta es que, cuando estamos hablando de investigaciones en el ámbito digital y de cooperación internacional para estas investigaciones, las normas necesarias para una cooperación internacional eficiente van a ser un "espejo" de las normas procesales.[4] Si yo necesito asegurar datos para obtener una investigación eficiente en el ámbito nacional, voy a necesitar de una norma de cooperación que prevea la misma posibilidad con datos alojados en servidores en el extranjero. Si necesito obtener datos de tráfico de comunicaciones para una investigación, cuando tengo un convenio de cooperación, voy a necesitar también de una norma que lo prevea. Con el registro y secuestro de datos sucede lo mismo. Por este motivo, un primer paso para contar con canales de cooperación internacional eficiente pasa por generar mecanismos procesales en el derecho interno que regulen de manera adecuada los mecanismos de obtención de evidencia en entornos digitales. Hoy se aplican por analogía las normas pensadas para la obtención de la evidencia física. Según entiendo, esta tendencia lleva a soluciones inadecuadas tanto en términos de eficiencia en la investigación como en protección de garantías, especialmente el derecho a la intimidad. El cambio generado por el avance de la informática y las telecomunicaciones fue tan grande entre lo que significa la evidencia física y la digital que si no se regula de manera adecuada es peligroso. Contrariamente a lo que se planteaba hace unos años, donde la regulación era presentada por organizaciones protectoras de la libertad en Internet como un peligro para las garantías individuales, hoy entiendo que la regulación procesal de la evidencia digital resulta imprescindible. La "no regulación" ha generado avasallamiento de garantías por vía de la jurisprudencia bajo el paraguas del principio de libertad probatoria.[5]

---

(4) Es por este motivo que las reglas de cooperación internacional de la Convención de Budapest (arts. 23 y ss.) están construidas acertadamente como espejo de las medidas procesales previendo su necesidad de obtención mediante cooperación internacional.

(5) Para ver el tema planteado más extensamente, Salt, Marcos, "Tecnología informática: ¿un nuevo desafío para el proceso penal?", en *XXV Congreso Nacional de Derecho Procesal Penal*, Bs. As, Rubinzal-Culzoni, p. 856. En el ámbito del derecho anglosajón, Kerr, Orin, "Digital Evidence And The New Criminal Procedure", *Columbia Law Review*, vol 105, 279. En el ámbito del derecho continental europeo, un interesante estudio de derecho comparado, Insa, Fredesvinda, "La Admisibilidad de las Pruebas Electrónicas ante los Tribunales. Luchando contra los Delitos Tecnológicos", AEC 2006.

Asimismo, la resistencia mantenida durante años respecto al único instrumento de alcance internacional vigente hasta el momento —la convención sobre delitos informáticos del Consejo de Europa o Convención de Budapest, de 2001— en la medida que, supuestamente, otorga al estado poderes procesales desmedidos, también ha perdido cierta vigencia frente a la realidad de la regulación de algunos países, que van mucho más allá de lo que previeron o imaginaron los redactores la Convención de Budapest. Solo por poner ejemplos, basta ver la nueva legislación de Perú, la de Costa Rica y la de Venezuela, o la nueva jurisprudencia italiana en la cual el Tribunal Constitucional ya ha avalado los registros de datos informáticos hechos a distancia a través de software[6] aunque no esté regulado expresamente en el código procesal penal.

Legislar y generar nuevos marcos normativos sobre este tema no tiene por qué significa siempre ir contra las garantías. Por el contrario, una buena regulación de estas nuevas herramientas puede permitir un uso adecuado a las necesidades de una investigación moderna y respetuosa de las garantías individuales. Por el contrario, una mala utilización del principio de libertad probatoria permite violaciones a las garantías procesales tal como ha sucedido en los últimos tiempos en nuestra jurisprudencia y en el derecho comparado.

Para poner un ejemplo al que he hecho referencia en varias charlas, si en el registro y secuestro de evidencia en entornos digitales yo pretendo utilizar las normas del secuestro de evidencia física o la jurisprudencia de la CSJN, seguramente las soluciones a las que arribe no van a ser siempre las más adecuadas. Por ejemplo, pensemos el caso de los hallazgos casuales y toda la doctrina de la *plain view*. No podemos aplicar la doctrina de la Corte de la misma manera para un ámbito físico que para un ámbito digital. Si allano esta aula en la que estamos sentados para buscar un elemento físico, obviamente por más que busque y busque solo vamos a poder encontrar lo que está en el ámbito físico en este momento. Si el registro lo realizo sobre una computadora, voy a poder encontrar lo que está alojado digitalmente en este momento, lo que estaba hace un año, lo que estaba hace cinco años, lo que se trató de borrar, lo que introdujo un usuario anterior de la computadora, y voy a poder encontrar todo, de manera tal que el hecho

(6) Se trata de la utilización de programas troyanos por parte del Estado para registrar y secuestrar datos informáticos. Sobre este tema, Ortiz Pradillo, Juan Carlos, "Fighting against Cybercrime in Europe: The admissibility of Remote Searches in Spain", *European Journal of Crime, criminal Law and Criminal justice*, 19 (2011), pp. 363/395.

de la incorporación de datos accidentales encontrados en un sistema informático no puede ser regulado de la misma manera que en el caso de la evidencia física. Por eso creo que es importante una regulación del marco procesal que proteja las garantías, pero que también piense en términos de eficiencia. Y en este punto disiento con algunas de las posturas de quienes me precedieron en la palabra. El sistema penal moderno avanza hacia un estado en el que no será posible prescindir de los elementos tecnológicos y la evidencia digital. Dentro de cinco años no va a existir investigación alguna en donde no haya evidencia digital involucrada. Piensen en las últimas causas que hayan tenido cada uno en el ámbito en el que trabajen y traten de identificar un caso en el que no fuera necesario algún dato tráfico de teléfonos celulares, algún dato o archivo obtenido de una computadora, alguna investigación de lavado de dinero o de fraude bancario donde no hayan tenido que secuestrar datos informáticos. Si eso no está regulado —y nosotros nos ponemos en una postura donde decimos "yo no quiero ningún tipo investigación que se valga de la moderna tecnología o de los archivos de evidencia digital" porque esto resulta peligroso para la intimidad de los ciudadanos—, no tendremos eficiencia alguna en la investigación y persecución de los delitos. Lo que sí creo importante señalar es que estamos hablando del sistema penal, no del sistema de inteligencia o de hipótesis de ciberguerra o seguridad nacional. Una cosa es proponer regular al sistema penal y otra cosa es proponerlo respecto del sistema de inteligencia, mucho más en términos de cooperación internacional en esta materia. Obviamente, no es lo mismo el caso de los abusos denunciados recientemente por la prensa internacional que involucran afectaciones a la soberanía de diferentes Estados por parte de otros o violaciones masivas a la intimidad de los ciudadanos a nivel internacional realizado por grandes potencias bajo la excusa de la seguridad o el terrorismo que lo que estoy proponiendo. Aquí se trata de la utilización regulada de la tecnología en materia de investigación criminal sin avasallar ninguna de las garantías propias de nuestro sistema constitucional y de lo que prevén los pactos internacionales de derechos humanos sobre la materia.

Ahora bien, lo dicho requiere del trabajo académico, de un análisis serio por parte de los legisladores, y del trabajo de los operadores del sistema de justicia penal. Mientras tanto, yo les aseguro que se pueden poner ejemplos en los cuales la jurisprudencia ha ido mucho más allá de lo que permiten legislaciones modernas o propone en términos de poderes procesales la Convención de Budapest. Yo les puedo contar causas de nuestra

jurisprudencia en donde se inicia la investigación con dos imputados, se abre una computadora para su registro, y surgen ochenta extracciones de testimonios como consecuencia de datos obtenidos de manera extralimitada de ese registro original avalado por los tribunales superiores. Entonces, evidentemente, no es que las normas procesales propuestas tanto a nivel nacional como en tratados internacionales son peligrosas. Las normas pueden contener hoy el sistema en el que se conjuguen de manera adecuada las necesidades de persecución con la protección de las garantías: un traslado de la vieja disputa entre eficiencia y garantías al ámbito digital.

3. Especial referencia a algunos de los temas que generan controversia a nivel de la cooperación internacional

Me gustaría detenerme brevemente a analizar dónde estamos parados desde la perspectiva de la política internacional. El desarrollo de la informática y las telecomunicaciones ha planteado un desafío aún no resuelto a la cooperación internacional. La creciente necesidad de obtener evidencia digital para los procesos penales a través de la cooperación internacional requiere de mecanismos que aún no han sido regulados de manera uniforme y, por otra parte, ha puesto en crisis pilares básicos de la cooperación tradicional como son el principio de territorialidad y la idea de soberanía como límite al poder de un Estado para realizar medidas de prueba en otro Estado. Tanto los tratados multilaterales como los bilaterales de asistencia en materia penal no resuelven los problemas que plantea la evidencia digital, lo que genera innumerables problemas prácticos en las investigaciones.

Vamos a poner algún ejemplo para que ustedes entiendan cuáles son el sinnúmero de problemas que se pueden generar.[7] Hay un supuesto que alguno de ustedes me debe haber escuchado citar. Se trata de un allanamiento a un banco en la Ciudad de Buenos Aires, con orden de allanamiento para revisar el sistema informático. Ingresamos al sistema informático buscando información de los movimientos de la cuenta de un imputado "X", de quien sospechábamos que era autor de un hecho de corrupción o de lavado de dinero. No dirigimos al espacio físico donde están las computadoras cumpliendo con todas las exigencias procesales y comenzamos la búsqueda en el sistema informático con mucho rigor y

(7) Para un desarrollo más amplio y con análisis de casos prácticos, Salt, Marcos, "Nuevos desafíos de la evidencia digital. El acceso trasfronterizo de datos en los países de América Latina", en *Derecho Penal y Procesal Penal*, Bs. As., Abeledo Perrot, 2013.

cuidando especialmente no vulnerar garantía alguna, incluso con el Defensor Oficial presente en el acto. Durante las operaciones de registro encontramos los archivos y datos contenidos en la orden de allanamiento, y el perito informático nos advierte que ha logrado identificar todos los archivos que estábamos buscando. Sin embargo, también informa que los archivos a los que está accediendo están alojados en el servidor que tiene el banco en España. ¿Por qué? Porque el banco aloja su información en la nube, y aloja la información en un servidor que cree —ni siquiera lo puede afirmar con seguridad—, está ubicado físicamente en España, aunque es posible acceder de forma remota desde Argentina y otros países. El interrogante del caso es si es posible y válido seguir adelante con el registro y secuestro de los datos; y lo cierto es que Internet como fenómeno ha roto con los paradigmas clásicos de la cooperación internacional, nada menos que con el principio de territorialidad y con el principio de soberanía nacional. Hoy uno de los participantes nombró el caso de Dropbox. Dropbox es solamente una de las aplicaciones que esta funcionando en la nube. La gran mayoría de las empresas importantes en este momento alojan la información en la nube. También nosotros, cuando utilizamos una cuenta de mail internacional como Gmail o Hotmail, estamos alojando la información en la nube. Es más, si esta tendencia se acentúa, es posible predecir que un futuro cercano nadie guarde los datos en sus computadoras sino en diferentes sistemas de almacenamientos en la nube. Cuando digo que la información se aloja en la nube, puede ser que se sepa o no en qué país está el servidor, y también puede suceder que la información, por cuestiones económicas y estratégicas, esté alojada en servidores ubicados en cinco países al mismo tiempo y solamente sea llamada a mi computadora cuando yo pongo un código específico que me permite traerla. Si aplicamos de manera acrítica y con los alcances tradicionales los principios de soberanía y territorialidad, no se puede acceder a estos datos. Entonces, uno de los temas más importantes que se está discutiendo en el mundo es precisamente el acceso transfronterizo de datos.[8] Este es uno de los ejes que mayor controversia genera en todos los foros internacionales y que repercutirá en las investigaciones penales del futuro, tanto en términos de eficiencia como en lo que respecta a la protección de las garantías, fundamentalmente los datos personales. Y no es una discusión sencilla ni inocente. En esta discusión hay involucrados tanto intereses de política y

(8) Véase el trabajo pionero de Seitz, Nicolai, "*Transborder Search: A new Perspective in Law Enforcement?*", en *Yale Journal of Law and Technology*, vol. 7, 2005.

estrategia internacional como intereses económicos, que incluyen a las grandes empresas de Internet y al desarrollo económico de los países en los que el manejo de la información es cada vez más importante.

En este contexto es que la Argentina analiza la posibilidad de adherir a la Convención de Budapest, aunque dicen que es una convención europea. Aclaro de entrada que en mis primeras presentaciones sobre este tema, me oponía a la idea de que Argentina adhiriera a la Convención de Budapest y prefería la idea de una unión regional para poder negociar con más fuerza con los países centrales. Hoy puedo decir que soy un "arrepentido" ya que apoyo el ingreso de Argentina la COC. He trabajado en diferentes comisiones del gobierno argentino para promoverlo. No es que me volví loco, lo que pasa es que el mundo fue cambiando y, según entiendo, la Convención de Budapest quedó como la opción más práctica y garantista de lo que hay en este momento a nivel de discusión internacional. Por otra parte, la Convención de Budapest no es una convención europea sino que pretende tener alcance universal y está abierta a la participación de los países no miembros del Consejo de Europa. Hoy, es una Convención surgida del Consejo de Europea, pero a la que han adherido Estados Unidos, Canadá, Japón, Sudáfrica, República Dominicana, Panamá. La OEA, por su parte, a través del grupo de expertos de delitos informáticos, recientemente a ratificado la sugerencia a los países miembros para que adhieran a este pacto internacional. De manera que es posible advertir que países con los que Argentina ha tenido tradicionalmente cooperación en materia penal ya son parte del sistema (EEUU, Italia, España, Alemania, Francia, Portugal, para poner ejemplos significativos de nuestro entorno cultural). Argentina ha sido formalmente invitada a adherir junto a otros países de la región como México, Colombia y Chile, y hay quienes se oponen diciendo que no les gusta porque nos van a utilizar. Claro que nos van a "utilizar". Ojalá nosotros hagamos los trabajos necesarios para permitirnos utilizar este sistema de cooperación al mismo tiempo. Acá tenemos que tomar una decisión que es de **política**. ¿Queremos estar de adentro del sistema de cooperación de la Convención para discutir y debatir lo que sea más conveniente para la Argentina y la región, o lo vamos a mirar desde afuera? Yo prefiero ir a discutir al seno del Consejo de Europea, unido con el resto de los países de la región, y dentro de los marcos que prevé la convención provocar los cambios que sean necesarios.

Hay otras opiniones que entienden que es mejor no adherir a la COC y promover una nueva convención en el seno de Naciones Unidas, idea sostenida

fuertemente por Rusia y en el ámbito regional por Brasil. Lo cierto que esta idea no prosperó y se bajó de la agenda. Pero supongamos que se vuelve a levantar como pretende Brasil (así lo propuso la semana pasada en la reunión del grupo de expertos en delitos informáticos de la OEA). ¿Cuánto tiempo va a llevar? ¿Diez años? ¿Qué se hace mientras tanto?

4. La cooperación internacional del sector privado

El tema de la cooperación del sector privado requiere también nuevas definiciones. Ya no es cooperación internacional entre países, sino cooperación internacional entre empresas privadas y los Estados. O sea, autoridades judiciales de un Estado que en vez de solicitar la obtención de evidencia digital alojada en servidores en el extranjero a través exhortos internacionales, lo solicitan de manera directa a las empresas del sector privado en las que los datos están alojados, como Microsoft, Google, Facebook, y otras. Estas empresas no tienen las mismas políticas de cooperación con los diferentes países. Así, a modo de ejemplo, hoy Microsoft responde a las requisitorias de datos de tráfico de comunicaciones solicitadas por autoridades judiciales argentinas, mientras Twitter no.

Supongamos, por ejemplo, que en una investigación en la Argentina es necesario acceder a la información contenida en una cuenta webmail de Hotmail. El exhorto internacional o la utilización de los acuerdos bilaterales de cooperación internacional en materia penal parecen no resultar eficientes para obtener esta información en lapsos de tiempo que tengan en cuenta la volatilidad de la evidencia digital. Los Estados hoy recurren a pedidos directos a las empresas, ya sea a sus oficinas centrales o a las dependencias comerciales que existen en sus países, siempre de acuerdo a protocolos de actuación impuestos por las empresas de manera unilateral y que difieren de país a país.

Hoy no existe regulación sobre este tema, y lo que tenemos en la práctica es que los que están regulando la cooperación sector público/sector privado en materia de obtención de evidencia con fines de utilización en investigaciones penales son las empresas del sector privado, que elaboran sus propias normas de acuerdo a cuándo puede pedirse la información, cómo hay que pedirla, de qué manera, y demás. Obviamente, esta situación está destinada a sufrir cambios en el futuro. No se trata tampoco de exigir abusivamente a las empresas que entreguen datos personales de sus clientes sin respetar las garantías del debido proceso y las leyes de protección de datos personales, sino de encontrar mecanismos que tengan en cuenta ambas necesidades.

Ese tipo de discusiones que se están dando con relación a Internet y derecho penal en el seno internacional, son las discusiones en las que tenemos que introducirnos como país, además de modificar nuestra legislación interna para poder hacer frente a estas investigaciones.

Ahora, dar vuelta a esto y decir de manera simplista "no quiero regular porque esto significa de alguna manera que va a haber una violación a garantías individuales", me parece que es esconder la cabeza y no darse cuenta de que las violaciones a las garantías individuales ya las tenemos presentes en este momento. Ya nos las están violando, y si van a entrar de alguna manera a nuestra computadora, a nuestros mails, yo prefiero que sea bajo una forma constitucionalmente admisible, respetando las garantías clásicas que requieren de adecuaciones a la realidad digital.

Entonces, sobre todas estas premisas es que yo creo que realmente hoy la mejor opción que tenemos es la Convención de Budapest. No porque me gusten absolutamente todas sus partes, sino porque muchas de las críticas que se le hacen al texto normativo no están presentes en la Convención.

Un tema importante es que la Convenio sobre la Ciberdelincuencia de Budapest tiene un fuerte contenido garantista, que surge de su art. 15, y que remite a los más importantes Pactos Internacionales de Derechos Humanos como límite a la actividad del Estado (en nuestro caso, de jerarquía constitucional). Por tal motivo, yo creo que es muy importante que en los ámbitos regionales que tienen que ver con protección de derechos humanos se empiecen a generar reglas que tengan que ver con las libertades y garantías en Internet, lo que hoy constituye un tema central en la materia. De la misma manera en que la Corte Suprema de Justicia de la Nación puso un coto a la obtención de datos de tráfico en 'Halabi' creo que la Comisión y los órganos internacionales de derechos humanos pueden ir fijando también criterios de cómo tiene que aplicarse un texto normativo como la Convención de Budapest.

Por último, insisto que personalmente entiendo que no estar dentro del sistema de cooperación internacional en la materia, aún con los riesgos que conlleve la relación asimétrica con países evidentemente más poderosos en términos tecnológicos, es más arriesgado que pretender aislarse en un mundo que, en este tema más que en cualquier otro, no solamente está globalizado sino que no reconoce fronteras. Gracias.

Contribuciones a la Jornada

Modernidad y crisis del Estado-Nación en la sociedad del riesgo

Una especial referencia a la seguridad en las nuevas tecnologías

PATRICIO NICOLÁS SABADINI[1]

Buenas tardes a todos, es un honor poder compartir con ustedes estas Jornadas Preparatorias al Congreso de la AIDP, así como la antesala al Simposio de Jóvenes Penalistas, ambos a efectuarse en el segundo semestre del presente año. Vengo de muy lejos a intercambiar con ustedes perspectivas y visiones de lo que se conoce hace varios lustros como Sociedad de la Información, concretamente, lo vinculado al sector informático y a la delincuencia relacionada con este. Mi ponencia es una minúscula parte de un libro que acaba de salir a la luz hace unos meses en la Argentina, y en un par de semanas reeditado en Perú por ARA editores, donde destaco la crisis de modelos legales arquetípicos del Estado-Nación frente

(1) Doctorando en derecho por la Universidad Nacional del Nordeste; Especialista en Derecho Penal de la Universidad de la Cuenca del Plata; Investigador Visitante en la Universidad de Salamanca (España), realizó además estancia de investigación en el Instituto Max Planck de derecho penal extranjero e internacional en Friburgo (Alemania) y fue recomendado para becario de investigación; Disertante en paneles nacionales e internacionales (Brasil y Alemania), autor de traducciones al español del alemán y portugués; autor de artículos en libros, diarios y revistas jurídicas. Actualmente es Fiscal Federal de la ciudad de Resistencia, Chaco.

a nuevas realidades, no solo en lo que a globalización refiere, sino además, teniendo en cuenta la misma mecánica de las nuevas tecnologías. El presente es un enfoque sociológico, político y, si se desea, criminológico, con referencias a algunos puntos problemáticos que evidencia parte del sector informático, como es el caso de la seguridad; una problemática que al estar en consonancia con la crisis de la legalidad, juega un papel preponderante en materia de jurisdicción.

1. Los nuevos desafíos y las jerarquías cuestionadas

El tsunami en Japón y la emergencia nuclear en la central nipona de Fukushima no solo han demostrado lo latente que sigue la modernización de las sociedades y los peligros que ella entraña, sino que responde al hombre como un dios de la cosa que luego se vuelve cosificado por su invención, haciéndolo ineficaz para contener sus efectos devastadores. Solo Chernobyl ha sido capaz de alertar a su máximo punto el peligro para un sector de la humanidad, así como las secuelas dejadas por décadas para generaciones venideras. Luego del desastre, la lógica hubiese planteado un barajar y dar de nuevo en materia nuclear, pero la lógica en esta sociedad nihilista debe dejar de ser usada como programa marco para establecer parámetros de conductas futuras de los hombres, debiendo ser reservadas solo para matemáticos, filósofos o incluso programas para ordenadores, pudiendo dejar inmerso al hombre solo en la lógica que marca ser su propia condena, la de ser un animal capaz de tropezar dos veces con la misma piedra.

La única diferencia que estriba entre Chernobyl y Fukushima es que la primera pudo deberse a un error humano, dejando la segunda solo como producto de la naturaleza. Pero lo deja al hombre al descubierto el dato, y a la vez la incógnita, sobre la necesidad o relación costo-beneficio del manejo nuclear como medio alternativo de energía. Este no es solo un grano de arena en la playa de los peligros que vive la sociedad en la actualidad, sino que se suma, además, el cambio climático, la capa de ozono y su progresivo deterioro, acrecentado por nuevos factores, como el desmonte de bosques con fines de cultivo del "dios Soja", sobre todo en América Latina, donde empresas multinacionales sin control estatal hacen uso y abuso de herbicidas tóxicos prohibidos en sus países, herederos de un modelo feudal que no solo moderniza las técnicas de cultivo, sino que reactualiza uno de los métodos milenarios de trabajo que se denomina hoy en día **tráfico de personas con fines de explotación laboral**. No deben

olvidarse, además, los ejercicios militares, las manipulaciones genéticas y demás riesgos que bien describe Beck en su "Risikogesellschaft".(2) En la sociedad del riesgo global, el daño medioambiental, los peligros químicos y biológicos, la macrocriminalidad —que entró al mercado de finanzas gracias a los negocios ilícitos, convirtiéndose en un peligro supranacional—,(3) así como el narcotráfico y el terrorismo fundamentalista y político son áreas que escapan a las fronteras y a los controles democráticos y, por lo tanto, a un orden de jerarquía en la toma de decisiones.(4)

La sociedad moderna se caracteriza por una fuerte influencia de las instituciones vinculadas a la economía y a sus partícipes sobre los individuos, el Estado y las leyes. En ese marco, las necesidades del mercado experimentan sobre individuos independientes *in factum*, pero fuertemente condicionados por la satisfacción de bienes económicos a la que se deben un cuerpo o conjunto de leyes, y un poder común que organice las mismas. El término "organización" aquí debe ser entendido, además, como el control y sanción de las leyes. Como bien nos enseña el profesor italiano Pietro Barcellona, se produjo un cambio en la concepción de la sociedad tradicional o su folklore, que produjo una subversión o vaciamiento radical de su imaginario: se inaugura un modelo social donde la centralidad son los vínculos sociales y la relación jurídica inherente a ellos.(5)

El paradigma de la legalidad sufre una alteración con la nueva llegada del proceso de movilización y avance de la economía, los desarrollos de la tecnología, el surgimiento de capitales transnacionales ayudados por los procesos migratorios; en suma, un conjunto de elementos a los que se ha denominado "globalización".(6) La principal alteración evidente es

---

(2) Ver Beck, Ulrich, *La sociedad del riesgo. Hacia una nueva modernidad*, Barcelona, Paidós, 2006, p. 38 y ss.

(3) Ver Lozano, M. G., "La democracia, el crimen organizado y las leyes sobre la *privacy*", en *Doxa* 15/16, 1994, p. 452.

(4) *Ibid.*; también Prittwitz C., *Strafrecht und Risiko. Untersuchungen zur Krise von Strafrecht und Kriminalpolitik in der Risikogesellschaft*, Frankfurt am Main, V. Klostermann, 1993, p. 76 y ss.; Herzog, Félix, "Límites al control penal de los riesgos sociales (Una perspectiva crítica ante el derecho penal en peligro)", *ADPCP*, 1993, pp. 318/319.

(5) Ver Barcellona, Pietro, "La Teoría de los Sistemas y el paradigma de la sociedad moderna", trad. de M. Maresca, en Portilla Contreras, Guillermo (coord.), *Mutaciones de Leviatán. Legitimación de los nuevos modelos penales*, Madrid, AKAL, 2005, p. 13.

(6) Ver Günther, Klaus, "Pluralismo jurídico y Código Universal de la Legalidad: la globalización como problema de Teoría del Derecho", en *Anuario de Derechos Humanos*, Nueva Época, vol. 4, 2003, (225-257), p. 225.

la del orden normativo, modelo para una concepción de Estado Nación fuertemente arraigado, que se enfrenta a un orden planetario de características policéntricas o supranacionales. Modelo nacional que, en la mayoría de los países de Occidente, posee un sistema tripartito de división de poderes comandado por un Poder Ejecutivo. Este sistema se encuentra en medio de otros conjuntos de leyes ya sea de carácter otorgado por la comunidad internacional, como por ejemplo leyes internacionales y supranacionales, sobre todo en aquellos países cuyas leyes de libre mercado funcionan como estandarte, llámese Organización Mundial del Comercio (OMC), Banco Mundial (BM) o el Fondo Monetario Internacional (FMI); ya sea *de facto* o *de iure* o actuando como legislador.(7)

1.2. El Leviathan débil ante la revolución tecnológica. Sectores anárquicos

La revolución de las comunicaciones pareciera configurar una tercera revolución industrial o, al menos, en cuanto los efectos de las primera dos, ya que han condicionado y reescrito la costumbre y cultura de la sociedad global, pues la era postindustrial de la información preocupa a los gobiernos y al Estado en el conocimiento de las nuevas tecnologías.(8) La revolución digital, especialmente, ha condicionado modificaciones en el plano económico, convirtiéndose en un factor de competencia global ante el traspaso de información y la velocidad con que llega a los receptores. En este sentido, la sociedad de la información, en cuanto a delitos informáticos, no se ha superado respecto a lo que a vulnerabilidad refiere. Los negocios de empresas, las administraciones y la sociedad misma dependen de la eficacia y seguridad de la información con la moderna

(7) *Ibid*, p. 226, Mercado, P.; "El proceso de globalización, el Estado y el Derecho", en Portilla Contreras, Guillermo (coord.), *Mutaciones de Leviatán. Legitimación de los nuevos modelos penales, op. cit.*, p. 155. Sobre la problemática en el ámbito de una configuración de un "derecho penal global", teniendo como base una crisis de la legalidad y de la soberanía, ver Pawlik, Michael, "¿Pena o combate de peligros? Los principios del derecho internacional penal alemán ante el foro de la teoría de la pena", en *Teoría de la ciencia del derecho penal*, trad. de Eduardo Saad-Diniz y Cecilia Ugartemendía; además, Navarro Dolmetsch, Roberto, "'Reconfiguración' del sistema de fuentes del Derecho penal y 'amenaza de crisis' del principio de legalidad. La incorporación del Derecho internacional convencional y el fenómeno de la globalización", en Faraldo Cabana, Patricia; Puente Aba, Luz María y Brandariz García, José Ángel (coords.), *Nuevos retos del Derecho Penal en la era de la globalización*, Valencia, Tirant lo Blanch, 2004, p. 165 y ss.

(8) Ver Carney; P., "De Bentham a Beadle. La ciudad de la vigilancia", en AA.VV, *Criminología y Control social. Orden o Justicia. El falso dilema de los intolerantes*, v. II, Rosario, Juris, 2000, p. 26.

tecnología.[9] Este cambio altera las tradicionales concepciones y modalidades en la economía, ya que se acopla a ella utilizándola como campo de gestión de las transacciones financieras. La revolución tecnológica tiene su lugar de privilegio en la compleja sociedad global a punto de modificar no solo las costumbres de quienes conviven en el planeta, sino la cultura misma. Este achicamiento de los tiempos puja por lograr una única identidad en el mundo —aunque sea en el discurso—, pero donde el multiculturalismo opera como fuerte valla (*v. gr.* fundamentalismo religioso, guerras civiles en el norte de África, terrorismo político, movimientos independentistas, etc.).

Uno de los espacios pendientes de tratamiento y estudio es el gran mundo del ciberespacio, que no solo posee lagunas jurídicas, pues tampoco obedece a una centralidad,[10] e incluso se torna peligroso para la seguridad e intereses de las naciones de algunas potencias del planeta. Es tal la intensidad del crecimiento de las redes de características planetarias que van dejando zonas de penumbra o de anarquía global en determinados sectores del ciberespacio. Piénsese el fenómeno de repercusión mediática del fenómeno "Wikileaks" donde, más que un caso de espionaje, resultara ser un *ciberculebrón* de características similares a programas de televisión vinculados a la vida privada de la farándula. Ello no solo puede ser advertido respecto de delitos vinculados al sector de intranet, sino a la vulneración misma al acceso al ciberespacio:[11] por ejemplo, el efecto que produce el sistema de *host provider*.

---

(9) Ver Sieber, Ulrich, "*Legal Aspects of Computer-Related Crime in the Information Society*", *COMCRIME-Study, prepared for the European Commission, Section I.B.2.a, "Protection of Privacy*", Würzburg University, Jan 1, 1998. Para un análisis de la legislación holandesa véase el estudio de Zaitch, Damián, "Viejos conocidos, nuevos enemigos. Discursos y políticas sobre el delito organizado en la nueva Europa", en AA.VV, *Criminología y Control social. Orden o Justicia. El falso dilema de los intolerantes*, v. II, Rosario, Juris, 2000, p. 155 y ss.

(10) Ver Carcova C., "Complejidad y derecho", en *Doxa,* 21-11, 1998, p. 66.

(11) Ciberestafas con tarjetas de crédito, pornografía infantil, acceso a cuentas bancarias, etc. Respecto de la seguridad informática, la Comisión Europea en abril de 2002 elaboró una "Propuesta de decisión marco del Consejo sobre ataques a sistemas informáticos (COM 2002 - 173) donde los comportamientos que se procuraban prohibir iban del acceso ilegal a sistemas informáticos, a los fines de impedir piratería o *hacking*; ya sea para violentar medidas de protección especiales, causar un daño u obtener un beneficio patrimonial; o el acceso al solo efecto de obstaculizar la dinámica del sistema, ya sea interrumpiendo, infectándolo con virus, borrando datos u otra conducta lesiva para el mismo que ocasione un daño a intereses de personas físicas o jurídicas (arts. 3° y 4°). Esta normativa era obligatoria para los Estados miembro a los fines de tipificación en sus respectivos cuerpos punitivos, al que luego se sumó el traspaso de información que guarde relación con la pornografía infantil. Para un

A mediados de noviembre del año 2000, el Tribunal de *Grand Instance* parisino obligó al proveedor Yahoo! Inc. el bloqueo del acceso a los remates de objetos nazis. Esto fue originado por acciones judiciales contra un *host provider* por permitir la posibilidad de creación de páginas web, y dentro de ellas, ventilar sitios web de pornografía infantil y propaganda nacional-socialista. No contento con el bloqueo, se levantaron en contra grupos antiglobalización solicitando el acceso, motivándose en el derecho a la libertad de opinión. Un ejemplo de que sectores o corporaciones transnacionales no se independizan suficientemente de las regulaciones estatales es este. EEUU y la UE hace depender la responsabilidad del *provider* de la cooperación con los Estados. No obstante, cabría investigar si la independencia del *provider* es solo según el rostro del Estado o si cabe una aplicación del bloqueo respecto a países subdesarrollados o tercermundistas. No puede ocultarse lo conflictivo del caso y el sinnúmero de cuestiones fundamentales a debatir, como la censura, el derecho de acceso a Internet, el alcance de las normas nacionales y su influencia en el ciberespacio; y las normas fundamentales implicadas, según la constitución de un Estado-Nación y su posible no injerencia en el mundo web.[12]

En la sociedad de la información, se requiere reglas de tráfico para el ciberespacio, pero no la protección de cualquier dato de individualismo nómade que pueda significar la restricción a una libertad individual.[13] Internet ha modificado las condiciones de comunicación, las fronteras de formatos de comunicación individual y general, la tecnología de la comunicación. A ello cabe agregar que configura un reto para el sistema jurídico pues se halla fracturado o delimitado por las fronteras regionales. Ahora, visto hasta aquí, ¿cómo puede congeniarse la libertad de información con las restricciones en materia de pornografía infantil o la protección de datos sin caer en un acto de censura? El puntapié inicial lo dio en Alemania la nueva ley federal que otorga a la Oficina Federal de Investigación Criminal (BKA) la posibilidad de ordenar a los proveedores de servicios de Internet

---

detalle de los respectivos puntos, véase Puente Aba, L. M.; "Propuestas internacionales de criminalizar el acceso ilegal a sistemas informáticos: ¿Debe protegerse de forma autónoma la seguridad informática?", en Faraldo Cabana, Patricia; Puente Aba, Luz María y Brandariz García, José Ángel (coords.), *op. cit.*, p. 382 y ss.; Zaitch, Damián, *op. cit.*, p. 178 y ss.

(12) Para un debate profundo ver Teubner, Gunther, *El derecho como sistema autopoiético de la sociedad global*, Bogotá, *UEC*, 2005, p. 70 y ss.; Günther, Klaus, *op. cit.*, pp. 233/234.

(13) Ver Ladeur, Karl-Heinz, "T*oward a Network-Oriented Law of the Internet! The Necessity to Find A New Balance between Risk and Opportunity in Network Comunication*", *German Law Journal*, vol. 10, n° 9, 2009, p. 1214.

bloquear el acceso a sitios web que contengan pornografía infantil. Más allá de la posible ineficacia de estas medidas, cabe preguntarse si significan un avance global para el control de las comunicaciones en Internet, incluyendo las de contenido político. Es importante reconocer que garantizar al ciudadano el libre acceso a la información constituye uno de los pilares de un Estado democrático de derecho, cimentado en la mayoría de las constituciones de Occidente, pero que no por ello el legislador puede imponer límites a las libertades.

De esto no está exento el ciberespacio, pero lo que agrava la cuestión es que el control en este sector se vuelve un tanto más difuso, y en muchos casos, obsoleto. Luego de los atentados del "11-S", el sistema se hace más vulnerable y exige más control sobre la actividad financiera no solo en la comunicación en lo que a contribución a redes terroristas respecta. Sin embargo, tiene cabida un aprovechamiento de la situación de búsqueda de eficientismo como forma de control de la vida de los ciudadanos. En este sentido, el comercio electrónico depende del sistema de seguridad en lo que se refiere a transacciones de dinero en redes de computadores, así como el sostén de las empresas depende del sistema informático. Si bien conforman el nervio central de la economía, la comunidad aún no es consciente de la potencialidad de los ataques a los sistemas informáticos.[14]

Respecto de las intervenciones telefónicas y de correos electrónicos, las estrategias de control siguen avanzando en este sentido. El Tribunal Constitucional Federal Alemán (BVerfGE) se ha pronunciado sobre las intervenciones telefónicas.[15] Un individuo venía sufriendo llamadas telefónicas; cansado de ello solicitó y obtuvo de la Compañía Deutsche Bundespost Telekom datos sobre la fecha, hora y duración de las llamadas del apartamento de un conocido. Luego, los datos fueron utilizados para iniciar una demanda civil de daños y perjuicios. La condenada presentó un amparo argumentando que el Estado había intervenido en su derecho fundamental al secreto de las comunicaciones sin autorización legal. El Tribunal Constitucional, a pesar de no hallar un fundamento para la intervención, la consideró lícita y desestimó el recurso de amparo motivándose en que resultaba justificada para proteger los derechos fundamentales de quien sufría las llamadas, por ser "llamadas anónimas

(14) Ver Sieber, Ulrich, *op. cit.*, p. 2.

(15) BVerfGE, 85, 386.

amenazantes o molestas". Pero, en cuanto a la confidencialidad y la integridad de los sistemas electrónicos, se agrava aún más la cuestión si se tiene en cuenta que en el fallo aludido se ve limitado el derecho a la intimidad y protección de datos. Ladeur demuestra que Internet, como red de redes,[16] no puede equipararse al teléfono como medio convencional de comunicación individual. Y, ello, ya que configura una herramienta de diferente formato, donde se abusa del anonimato de contactos electrónicos, lo cual y de la cual puede ser una forma más eficiente a la hora de cometer actos criminales, inimaginables con medios tradicionales.[17]

En el caso de la pornografía infantil, el bloqueo y ratificación de la censura dependerá de si lo que se advierte como sexo explícito de menores corresponde o queda abarcado por el concepto de opinión, dentro de lo que se conoce como libertad de expresión, o de información.[18] Esto, de perogrullo, podría responderse con una sola pregunta iracunda de Ladeur: "¿Qué tipo de opinión y qué tipo de información es la fotografía de un niño que ha sido degradado como un objeto de contenido sexual para adultos?".[19] Para evidenciar aún más la carencia de censura en caso de bloqueo, el contenido pornográfico de fotos donde se advierten involucrados a niños no puede basarse en una opinión con efecto intelectual, ya que lo que se comunica no da cabida a un debate público, dejando a un lado y en un pisapapeles las discusiones atinentes a su rechazo.[20]

Otro dato que arroja la mayor ineficacia de la política para ejercer el control directo es el sector del desarrollo planetario de Internet y los medios de pago a los que se ha optado. Las transacciones económicas efectuadas por medios electrónicos de pago son menos transparentes que las efectuadas por medio del dinero en efectivo estándar; esto demuestra, a su vez, cómo la delincuencia informática se halla en el campo de los delitos económicos.[21] Al ser menos visibles, se hacen menos controlables. Además del pago con tarjetas de crédito, se impone en las electro-transacciones la utilización de *smart cards* y el ciberdinero o *computer geld.*

(16) Ver Ladeur, Karl-Heinz, *op. cit.*, p. 1211 y ss.

(17) *Ibid.*

(18) Art. 5°, párr. 1°, *Grundgesetz*; art. 14 CN.

(19) Ver Ladeur, Karl-Heinz, *op. cit.*, p. 1203 y ss.

(20) *Ibid.*

(21) Ver Sieber, Ulrich, *op. cit.*, p. 3.

Las *smart cards* consisten en la utilización de tarjetas que operan con un chip, similares a las que se utilizan en la telefonía móvil. Estas tarjetas son recargadas con dinero electrónico, el cual es extraído directamente de la cuenta bancaria del usuario, y funcionan con la ayuda de un aparato lector que puede ser ubicado en terminales y en sectores de múltiple uso o consumo, como estaciones de trenes, snackbars, taxis, cines y comercios. Esto traería como consecuencia la estabilización y flexibilización de la actividad de los bancos centrales. Actualmente, está siendo implementado en la UE como parte de un Proyecto Marco.(22)

El ciberdinero o dinero informatizado opera de otra forma, y con computador de por medio. El usuario, o quien va a efectuar una transacción económica, almacena en su ordenador unidades o códigos electrónicos de valor que serán reconocidos por el banco o por quien efectuara la transacción con él, que puede ser un comercio. Esto arroja no solo problemas de control, sino de regulación, ya que es un terreno propicio para expertos encargados de desarticular códigos y extraer datos, así como para la introducción de virus, la destrucción de pruebas de las transacciones bancarias,(23) etc. Ninguno de los ejemplos anteriores quita la posibilidad de innovaciones en este marco de alejamiento del hombre de los medios de pago tradicionales; no hacen más que demostrar la ineficacia de una política y su función de control directo dentro de un límite en los términos de un Estado-Nación, ya que al poseer escalas globales, obliga a los Estados a tender lazos para trabajar sobre los problemas en este difícil y anárquico sector, lo que transforma una política unilateral, la que posee el Estado-Nación hacia adentro, en una política policéntrica, la que el Estado-Nación establecería hacia el exterior.

Es en este sentido que debe procurarse no caer en la vieja usanza de restricciones al libre flujo de la información, ya que estaría condenada al fracaso por la cantidad de datos transferidos en las redes internacionales, siendo imposible su control. Es por ello que también debe pensarse en medidas no legales, algo que vaya más allá de prohibiciones puramente criminales.(24)

---

(22) Ver Willke, Helmut, "La supervisión del Estado: el desafío a la política por parte de los sistemas mundiales adyacentes" en Gómez-Jara Díez, Carlos (coord.), *Teoría de sistemas y derecho penal : fundamentos y posibilidades de aplicación*, Bogotá, UEC, 2007, p. 167.

(23) *Ibid.*

(24) Ver Sieber, Ulrich, *op. cit.*, p. 5.

1.2. La era tecnológica y su influencia en la comunicación

Luhmann atribuye dos logros o características fundamentales de la sociedad actual, la diferenciación social y la revolución de los medios. Según Winthrop Young,[25] Luhmann es reacio a explicar estos procesos en forma causal ya que pueden distorsionar la complejidad de la evolución social. Esto, a su vez, puede venir inducido por la exclusión de las materialidades de la comunicación que efectúa Luhmann. Vaios Karavas, en un interesante artículo, analiza este segmento de la teoría de Luhmann y la yuxtapone a la teoría de Kittler sobre el determinismo tecnológico, con quien ha entablado discusiones al respecto.[26] Con esto Luhmann quiere decir que, más allá de los medios de comunicación, la *autopoiesis* social y los sistemas de diferenciación siguen siendo los mismos. Karavas lo trae a colación pues apuesta a la tesis de que, más allá de que Luhmann excluye la materialidad de la comunicación, ello desconoce como cálculo evolutivo los avances tecnológicos como puente entre la mente y la comunicación, entre ellos, las computadoras, como en su tiempo lo efectuó la imprenta, el telégrafo, la radio, el cine, etc.[27] En cierto modo, se demuestra una creciente desventaja entre el hombre y las nuevas tecnologías.

Kittler explica mejor esta situación, marcando una diferencia entre la manipulación del eje temporal en la era de la escritura y la manipulación del eje temporal en la era tecnológica. Kittler utiliza "Manipulación del tiempo" en el sentido de que las nuevas tecnologías son capaces de transformar el orden cronológico del evento en el espacio y manipularlo, como orden del espacio que puede cambiar de sitio.[28] La era de la escritura, históricamente, es la primera en manipular el tiempo, mediante signos (De Saussure) en un orden que puede ser modificado o sustituido por otro (Lacan), pero que no se acerca tanto al mundo real debido a las limitaciones que vienen

---

(25) Winthrop-Young, Geoffrey, "*Silicon Sociology, or Two Kings on Hegel's Throne? Kittler, Luhmann, and the Posthuman Merger of German Media Theory*", en *The Yale Journal of Criticism*, vol. 13, n° 2, otoño 2000, pp. 391/420.

(26) Ver Karavas, Vaios, "The Force of Code: Law's Transformation under Information-Technological Conditions", en *German Law Journal*, vol. 10, n° 4, 2009, p. 465 y ss. Incluso Karavas cita una anécdota de viaje en taxi de Luhmann con Kittler, que también puede hallarse en el artículo de Winthrop Young, respecto a la diferencia entre ambas teorías: "El Sr. Kittler, siempre ha sido así desde Babilonia. Cuando un mensajero pasa por la puerta, a la gente le gusta preguntarle por el caballo que está montando y a la gente como yo, sobre el mensaje que trae consigo", Winthrop-Young, Geoffrey, *op. cit.*, p. 391.

(27) Ver Karavas, Vaios, *op. cit.*, p. 467.

(28) *Ibid.*, p. 468.

de la propia configuración del esquema de símbolos y su campo de acción. En cambio, en la era de la tecnología, lo real ya no se aleja tanto, lo que no quiere decir que no sea controvertido, ya que los medios electrónicos permiten el procesamiento, en tiempo real, del evento temporal, no en signos, sino en procesos matemáticos con valores numéricos.

> "Si uno trata de almacenar con el auxilio de medios de comunicación escritos el temporal caso de una cadena de habla, solo se puede escribir sobre todo lo que se ha dicho. En la era de los medios tecnológicos, sin embargo, también se puede almacenar eventos singulares y los contingentes, tales como el tono de voz de la persona que habla por su transformación, por ejemplo, en el caso de la computadora, en series de 0 y 1 segundo".(29)

Este es un dato que Luhmann pareciera descartar y ello por su carácter de sociólogo que se satisface con la observación o descripción de superficies de la sociedad, cuestión que deja a un lado los códigos (informáticos) y circuitos para la técnica. Teniendo en cuenta este dato, la tecnología camina con ventaja respecto a las operaciones efectuadas por la ley y su limitado campo. Cabría preguntarse si no se halla, más bien, en presencia del paso hacia el ocaso, sobre todo, si uno se representa la expectativa normativa que debe asegurar.

Una de las obras pilares que reflejan este dilema es la de Lawrence Lessig *Code and other Laws of Cyberspace,* quien enfoca la implicancia de los nuevos medios y su impacto en la sociedad, así como su regulación en el ciberespacio. Lessig, consciente de la ineficacia de la regulación, opta por un sistema de encriptamiento o código, como en ámbitos que vinculan a la propiedad intelectual, donde el usuario para el acceso de determinada información debe relegar a aspectos atinentes a la privacidad o a su identidad y brindar dichos datos, abonando o no una tarifa, como sucede en el caso de tarjetas de crédito. Esto, si bien puede ayudar para la protección de determinados datos en distintas bases hace vulnerable al emisor de los mismos. Internet configura una red de un sinnúmero de computadoras interconectadas, donde establecen procedimientos de almacenamiento, procesamientos y manipulación de datos, como nuevo espacio donde la sociedad parece desenvolverse. Lo que demoraban los hombres en relacionarse ha quedado borrado de un plumazo con redes sociales como Facebook,

(29) *Ibid.*

Myspace o Twitter, lo que lo coloca como un nuevo espacio democrático de expresión ciudadana. Esto afecta a la ley, algo que Lessig logra explorar y unir con la tecnología, pero arroja un resultado de análisis negativo si se quiere que la ley logre regular la conducta de los usuarios del ciberespacio.

2. Seguridad informática. La *lex informatica*

El código dentro de Internet, si bien no logra paliar estas falencias, reemplaza y disminuye su poder, estableciéndose una fuente legal paralela que limita los flujos de la información.(30) Esta legislación paralela, a diferencia de las normas jurídicas que son definidas por el soberano en un lugar determinado, tiene su origen en la propia red y no deriva de un contenido sustantivo —así como su interpretación—, sino de las capacidades técnicas y las prácticas consuetudinarias. En cuanto a su origen, las normas jurídicas vienen de la mano de los procedimientos políticos para su creación dentro del Estado, mientras que *lex informatica* posee un desarrollo tecnológico y un proceso social de evolución, según la costumbre, adoptando su propia lógica interna. Además, opera ejecutando automáticamente sus condiciones, a diferencia de las normas jurídicas que precisan de la autoridad judicial para ser ejecutadas.

Reidenberg traza una didáctica diferencia entre la ley como tradicionalmente es conocida, y lo que denomina *lex informatica*. Los políticos asocian la elaboración a través del proceso político dentro del Estado por medio del Parlamento. Dentro de lo que se conoce como contexto de flujos de información se establece una nueva arquitectura ya que se prohíben accesos a la red en cuanto no se medie autorización de seguridad o se impongan ciertos flujos, como la dirección coercitiva de datos de enrutamiento de los mensajes electrónicos.(31) Atribuye un verdadero sistema de reglas a la sociedad de la información y la consibe como un sistema paralelo al legal, que abarca o es más efectivo en sectores donde las leyes comunes no puedan desplegar sus efectos. Por ejemplo, no solo reacciona automáticamente frente a quien intenta dar un código de acceso erróneo, no permitiendo ingresar a una fuente de datos, sino que configura un sistema que no posee jurisdicción, algo que en la ley tradicional viene impedido por el principio de territorialidad.

---

(30) *Lex informatica*; según Reidenberg, Joel R., *"Lex informatica: The Formulation of Information Policy Rules through Technology"*, en *Texas Law Review*, vol. 76, n° 3, febrero, 1998.

(31) *Ibid.*, p. 565.

La *lex informatica* posee una jurisdicción que es la red misma. En cuanto al contenido sustantivo o material, Reidenberg señala que la ley tradicional deriva del mismo texto legal, interpretación judicial, incluso lo que la propia dogmática extrae. En cambio, la *lex informatica* viene definida a través de las capacidades técnicas y prácticas de la costumbre.(32) Existe una estrecha relación entre el sistema legal y la *lex informatica*. Esta puede limitar la capacidad de acción de la ley y sustituirla en caso de mayor capacidad y campo de acción, por ejemplo, la filtración de contenidos pornográficos. Pero esto no quiere decir que haya una relación de preeminencia de la *lex informatica*, sobre todo a nivel de responsabilidad de los actores en juego, así como prerrogativas fundamentales, concretamente, lo que guarda relación con la protección de la privacidad, la libertad de información y expresión, frente a los abusos que se hacen de los datos privados por parte de las corporaciones, o limitaciones o bloqueos de la opinión. Obviamente, se abren abanicos de dilemas respecto de algunos puntos de discusión o *topoi* problemáticos como la difusión de imágenes pornográficas o la limitación a la expresión de ideología nazi, así como, ya en nuestro campo, las prerrogativas policiales a la hora de la intervención de las telecomunicaciones o del correo electrónico en regiones del globo con alto voltaje de sensibilidad a los riesgos terroristas, acrecentado por las noticias del polémico asesinato de Osama Bin Laden, donde el lema de que la historia se repite con diferentes personajes sigue en pie.

Karavas señala una posible preocupación para el esquema de Luhmann en el ámbito de la *lex informatica*, ya que dentro del mundo digital no se puede diferenciar entre expectativas normativas y cognitivas.(33)

3. *Mass media* y descentralización política

Una suposición que cabe a los medios de comunicación recae en tanto uno pueda elegir como consumidor, en forma libre y sin restricciones, entre los diferentes oferentes. El Tribunal Constitucional Federal Alemán (*BverfG*) ha tenido presente el rol que fueron cumpliendo los medios de comunicación en las últimas décadas, advirtiéndose algunos cambios según las manifestaciones del entorno y la época,(34) teniendo en cuenta que las decisiones sobre la ley de medios tienen un proceso de alto voltaje

(32) *Ibid.*, p. 567.

(33) Ver Karavas, Vaios, *op. cit.*, p. 477.

(34) BverfGE 31, 309 (312); 12, 205 (259); 31, 314 (325); 35, 202 (222); 73, 118; 44, 125 (145).

político en la formación de la opinión pública. Esto viene a justificar la introducción de derechos a la libertad de prensa como disposiciones generales de protección en el ámbito del proceso penal, la restricción de búsqueda en las oficinas de los periódicos, la legislación antimonopolio, etc.

La relación entre los medios de comunicación y el sistema político fue variando según el contexto. En los años 60 y 70 se observaba una armonía entre los grupos sociales y el medio ambiente, donde la solución y el balance podían hallarse en el sistema político y las decisiones del Gobierno, como decisión centralizada. Esto fue precedido por un consenso sobre los valores sociales y un proceso de prestructuración de los proponentes de las sendas alternativas en los partidos y asociaciones representativas. Los medios de comunicación, en última instancia, se hallaban políticamente funcionalizados. Esta tendencia va cayendo en la posmodernidad y con ella la centralización política, por los procesos de fragmentación en una nueva lógica de redes, intensificada por la multiplicación de posibilidades de, en términos de Ladeur, *media transmission*. Además, el debilitamiento de organizaciones representativas, tradicionalmente grandes, como sindicatos, iglesias, clubes, los cuales entran en declive.[35]

Estos datos *de lege ferenda* hablan de la necesidad de unificación global normativa como toque de queda para estos sectores anárquicos a los que puede sumarse lo relativo al medio ambiente. No obstante, un cuerpo global, hoy por hoy, resulta ser una utopía. Una de las principales cuestiones a resolver es el ámbito político diverso o heterogéneo a los que se ven sometidos los Estados. La actual crisis económica mundial y el rol de los bancos, de ahí en más, ha ocasionado un replanteo respecto al esquema neoliberal de libre mercado que con tanta magia y palabras dulces nos ha prometido un mundo de progreso y menor complejidad. Esto desde el punto de vista fáctico.

Uno de los retos de los organismos de control es que debe adaptarse a la volatilidad y la ubicuidad de la comunicación por Internet, debido a la flexibilidad de la autoorganización de las situaciones jurídicas involucradas en un procedimiento de permanente cambio.[36] Desde una perspectiva

(35) Ver Ladeur, Karl-Heinz; "*Guaranteeing the Programming Mandate of Public Broadcasters and Restrains on Private Broadcasters' Programmes in Multimedia Conditions*", en *German Law Journal*, vol. 5, n° 8, 2004, p. 910 y ss.

(36) Ladeur propone, en caso de la propiedad intelectual y la protección de datos en la financiación pública y privada, que las organizaciones encargadas de proteger datos, funcione como agentes de información de los usuarios, donde estos decida qué datos se pueden

normativa, las posibles normas que formen parte del paradigma legal se caracterizarán inevitablemente por la vaguedad de los términos abstractos empleados en la norma, dando apertura a diferentes conflictos de carácter jurídico, tal como surge en la mayoría de la normativa supranacional. A mayor cantidad de términos difusos, mayores serán los esquemas interpretativos, incluso desde el punto de vista teleológico, este puede considerarse el primer obstáculo.(37) Otro argumento que estanca es la progresiva obsoletización de las instituciones democráticas en el armado de un código universal, lo que deja en manos de unos pocos los destinos de los habitantes del globo, llámense economistas, científicos o juristas.

4. Colofón

1. El Estado-Nación, entre las tantas crisis, sufre aquella que puede ser ejemplificada por las redes tendidas desde la flexibilización de las fronteras, como producto de la globalización. Como efectos de tal flexibilización, se produjo el desarrollo de la tecnología y el surgimiento de capitales transnacionales. Especialmente, la que guarda relación con la delincuencia informática, sobre todo, la que repercute en diferentes sectores del globo. Esto trae serias implicancias en el proceso de toma de decisiones, así como en su ámbito espacial.

2. El trasfondo no solo posee el dato económico, sino que abre la discusión a otros ámbitos donde se plantean temas como la posibilidad de limitar la libertad de opinión, el derecho a la intimidad, el acceso a la información o la censura, el alcance de las normas nacionales y su influencia en el ciberespacio. Esto se advierte en la difusión de pornografía infantil y propaganda nacional-socialista en la mayoría de Occidente.

3. La *lex informatica*, como mecanismo de seguridad, difícilmente pueda ser considerada ley en sentido lato, pero no puede negarse su propia lógica interna en materia de seguridad y control.

utilizar por otras empresas, y cuáles en condiciones de privacidad. Ver Ladeur, Karl-Heinz, "T*oward a Network-Oriented Law of the Internet!...*", *op. cit.*, 1208.

(37) Sobre la indeterminación, ver Teubner, Gunther, "*Neo-Spontanes Recht und duale Sozialverfassungen in der Weltgesellschaft?*", en Simon/Weiss AAVV, *Zur Autonomie des Individuums – Liber amicorum für Spiros Simitis*, Baden-Baden, Nomos, 2000, p. 441.

El *grooming* en la legislación argentina

LUIS ÁNGEL NOCERA[1]

Para comenzar, debemos definir lo que se entiende por *grooming*.

Podría decirse que es el accionar deliberado que, mediante conductas que buscan generar una conexión emocional entre un adulto y un menor —sea de amistad o de otra índole—, deriva en prácticas abusivas de tipo sexual de las que es víctima el menor, y que pueden vincularlo incluso al mundo de la prostitución o la pornografía infantil.

En Argentina, del avance de las nuevas tecnologías en conjunto con el crecimiento del uso del ciberespacio y de las redes sociales, resultó la necesidad de crear un marco normativo de punibilidad penal para una nueva forma de acoso de parte de los pederastas, que han hecho de los medios de comunicación mencionados herramientas para lograr sus actos delictivos y lesivos. Dicha necesidad derivó en que, en el año 2013, se sancionara y promulgara la ley 26.904, que incorpora al Código Penal el artículo 131 de acuerdo a la siguiente redacción:

> "Será penado con prisión de seis (6) meses a cuatro (4) años el que, por medio de comunicaciones electrónicas, telecomunicaciones o cualquier otra tecnología de transmisión de datos, contactare a una persona menor de edad, con el propósito de cometer cualquier delito contra la integridad sexual de la misma".

(1) Asesor en Tecnología e Informática. Bachiller Universitario en Derecho.

La inclusión de esta modificación en el Código Penal generó discusiones debido a lo ambiguo que resultó para algunos, o a lo extorsivo e incompleto que resultó para otros. Unos repiten que al decir "mediante cualquier transmisión de datos" no se establece en que circunstancia específica puede aplicarse dicho artículo, o cómo se determina el propósito de "cometer un delito contra la integridad sexual", mientras que para otros lo que resulta extorsivo es su ambigüedad, debido a que un menor, o alguien que confunda su apariencia con la de un menor de edad, puede extorsionar a alguien diciendo que va a denunciarlo por *grooming* sino le da dinero o lo que le solicite a cambio de no realizar ninguna denuncia ante las autoridades.

Los que opinan que es incompleta tienen una mirada más técnica a nivel jurídico. Se enfocan en si se considera la aplicación de esta norma con el abuso consumado o con el mero hecho de establecer el contacto mediante actitudes de las que pueda sospechare —o que directamente tiendan— a dañar la integridad sexual del menor, es decir que la cuestión pasa por decidir si el acto preparatorio de la consumación del delito es punible o no.

La justicia, mientras tanto, se ha encargado de allanar el camino desde el momento mismo de la sanción de la ley a partir de un caso que se configuró de la siguiente manera:

Un hombre de 52 años, residente en el partido bonaerense de Coronel Suárez, fue acusado de tomar contacto con menores de 13 y 14 años, vía redes sociales, con la aparente intención de concretar algún acto de abuso sexual contra ellos.

En este caso, la madre de uno los adolescentes revisó el celular de su hijo preocupada por su comportamiento extraño. Allí descubrió un historial de conversaciones con un adulto desconocido que incluía una serie de ofrecimientos de aquel a cambio de favores sexuales, y que terminaban con una cita, ese mismo día a las 3 de la tarde, en un hotel alojamiento de la mencionada ciudad.

La mujer realizó la denuncia y el hombre fue aprehendido en la puerta de un hotel de Coronel Suárez, mientras esperaba al adolescente, por la presunta comisión del delito de *grooming* u hostigamiento sexual perpetrado a través de la web, en lo que constituye el primer caso de aplicación de esta figura incorporada hacía exactamente un mes al Código Penal. El acusado también había convocado a otro menor para el mismo encuentro.

El fiscal que entendió en la causa, titular de la UFIJ 14 especializada en delitos sexuales de la Fiscalía General de Bahía Blanca, Mauricio del Cero, dijo que debía tratarse del primer caso de *groomig* en todo el país, mientras explicaba que la pedofilia no se había consumado y por eso se trataba de *grooming*, que es como se denominan las maniobras para acercarse a un niño o adolescente con la finalidad de abusar o tener un encuentro sexual con él. Luego, el funcionario agregó que "la policía no tuvo más que ir a la hora pactada y aprehenderlo, porque además, en las conversaciones de *chat*, este señor pasó un teléfono celular, que es el mismo que tenía en su poder al momento de la interceptación policial, con lo cual pocas dudas hay sobre la identidad del autor". El acusado, luego, recuperó su libertad, por tratarse de un delito excarcelable, pero continuó siendo sometido al proceso judicial.

Aquí podemos observar que el mero intento de daño contra la integridad sexual del menor fue suficiente para el accionar de las autoridades, lo que aclara la cuestión acerca del momento a partir del cual el hecho configura el delito de *grooming*, sin que sea necesario que se concrete el abuso sexual. Esto ha significado un gran avance para la justicia en la medida que esta ley evita entrar en la figura de corrupción de menores, que lleva cuestiones técnicas más detalladas para que se le de curso a la denuncia.

En este caso también, la prueba documental fue fácil de determinar debido a que se utilizó un teléfono móvil para conectarse con el menor. En otros, en cambio, es más difícil el medio probatorio, y esto es algo por lo que puede criticarse el texto del artículo 131 del Código Penal, en razón de que no establece qué medios informáticos pueden ser determinados como prueba. No es lo mismo determinar prueba para un robo u homicidio que para el *grooming*. Tratándose de un mundo completamente abstracto y cibernético, la cuestión documental es muy compleja. El mero secuestro de elementos físicos puede no ser suficiente, y que muchas veces aparezcan involucradas empresas de servicios informáticos radicadas en el extranjero dificulta su recolección, ya que estas no siempre responden a las solicitudes emitidas por nuestra justicia o pueden demorarse demasiado.

Otro aspecto a discutir es cómo los fiscales y las autoridades piensan que actúa quien realiza *grooming*. De acuerdo a ciertos parámetros, se establece que un *groomer* es quien busca a quien acechar y prepara el acto del encuentro de consumación. Pero este esquema está obviando algo

sumamente importante: los actos preparatorios. Es decir, el uso de las redes sociales o Internet, la navegación, la búsqueda del perfil de la víctima, su vulnerabilidad psicológica, el lenguaje que va a utilizar de acuerdo a la edad del menor y en algunos casos la creación de un falso perfil de "menor" para, mediante ese engaño, intentar contactarse con aquel que va a resultar víctima del abuso —y todos los actos previos a intentar concretar el encuentro con el menor—, son sumamente importantes como prueba documental del delito.

A modo de síntesis, podemos establecer que la ley de *grooming* ha sido un avance aunque con muchas falencias en su redacción, por su ambigüedad, su poca claridad en lo que refiere a la prueba documental, y porque, en algunos casos, puede llegar a usarse de forma extorsiva. A su vez, no se establecen los mecanismos de prueba informática para este delito, y solamente encara el intento de concretar un delito contra la integridad sexual del menor, mientras que muchas veces el acosador no busca un encuentro, sino fotos o videos de índole erótica o pornográfica, lo que, en conjunto, hace que sea una ley y artículo con complicaciones de aplicación, con muchos vacíos acerca de como es la comisión del delito.

Estas ambigüedades van en contradicción de la claridad con la que se lo trata la Convención de Budapest, que define "sistema" o "dato informático" de la forma siguiente:

> "Artículo 1 – Definiciones
>
> A los efectos del presente Convenio, la expresión:
>
> a. 'sistema informático' designa todo dispositivo aislado o conjunto de dispositivos interconectados o unidos, que aseguran, en ejecución de un programa, el tratamiento automatizado de datos;
>
> b. 'datos informáticos' designa toda representación de hechos, informaciones o conceptos expresados bajo una forma que se preste a tratamiento informático, incluido un programa destinado a hacer que un sistema informático ejecute una función;
>
> c. 'prestador de servicio' (1) designa:
>
> i. toda entidad pública o privada que ofrece a los usuarios de sus servicios la posibilidad de comunicar a través de un sistema informático;

> ii. cualquier otra entidad que trate o almacene datos informáticos para ese servicio de comunicación o sus usuarios;
>
> d. 'datos de tráfico' (2) designa todos los datos que tienen relación con una comunicación por medio de un sistema informático, producidos por este último, en cuanto elemento de la cadena de comunicación, indicando el origen, el destino, el itinerario, la hora, la fecha, el tamaño y la duración de la comunicación o el tipo de servicio subyacente".

Esta claridad de términos fue apreciada en su momento por quienes impulsaron que Argentina sea parte de la dicha Convención, que en los fundamentos del proyecto de declaración dijeron lo siguiente:

> "Es responsabilidad de la clase dirigente que estos conceptos se globalicen en la misma medida que se globalizan los propios recursos y herramientas tecnológicas y éste es uno de objetivos fundamentales que se plantean y así lo explicitan claramente las Altas Partes al suscribir a la Convención de Budapest.
>
> En ese orden de ideas la Convención contempla los siguientes aspectos:
>
> Armonizar las leyes penales sustantivas aplicables a las conductas delictivas que tienen como escenario el entorno informático. Se plantea la necesidad que las legislaciones nacionales internas tipifiquen como delitos entre otros a los siguientes actos: acceso ilícito a redes o sistemas, interceptación deliberada e ilegitima de datos y sistemas informáticos, uso de dispositivos que permitan la comisión de tales ilícitos, falsificación y fraude informático, infracciones a la propiedad intelectual. En sus arts. 1 a 8 se definen los conceptos de "sistema informático", "datos informáticos", "prestador de servicios", "datos de tráfico" y diferentes delitos de naturaleza informática, de modo de establecer una terminología común que elimine de las legislaciones nacionales ambigüedades y falta de claridad en la terminología de uso en la materia" (Expediente 0890-D-2009, 18/03/2009, Firmantes: Pinedo, Federico - Bertol, Paula María).

A pesar de estos aspectos contradictorios, sigue siendo un paso más hacia adelante para empezar tipificar lo que refiere al *grooming*, debiéndose buscar algo a mayor escala, de fácil aplicación y claro en la determinación

de pruebas y respecto de la comisión del delito, así como esclarecedor en la cuestión de los actos preparatorios.

El artículo 131 del Código Penal no refleja el espíritu de la adhesión a la Convención de Budapest por parte de los firmantes del Proyecto de declaración, pues persiste la falta de claridad en las normas de nuestra legislación. Aun así, con el surgir de nuevos profesionales con una preparación no solo en lo jurídico sino en lo técnico/informático, se ve un haz de luz al final del camino para revertir esta situación.

La problemática del cibercrimen

DIEGO F. MIGLIORISI[1]

En principio, para analizar esta problemática, considero fundamental enfatizar la clasificación de los delitos informáticos.

En un primer grupo se hallan los llamados delitos típicamente informáticos, y son aquellos que nunca podrían existir sin la informática y/o Internet. Entre ellos encontramos el *hacking*, el *phishing* ,el *spamming*, los *hoax*, infecciones informáticas por medio de virus o troyanos (programas espías), programas maliciosos destinados a la denegación de servicio, y delitos relacionados con marcas y patentes y la identidad de las personas, como son los casos de *mettatanging* , *typosquatting* y *cyberquatting* (apropiación de dominios de Internet).

En un segundo grupo, que denominamos delitos configurados a través de Internet, aparecen los delitos establecidos históricamente en los códigos penales para los que la tecnología incorpora una nueva forma de comisión a través de Internet. Podemos destacar, entre estos, las calumnias, extorsiones, estafas, hurto informático, violación de correspondencia, instigación a cometer delitos, ejercicio ilegal de la medicina, delitos contra la propiedad intelectual, *grooming*, *cyberbullyng* (tipos de acoso), *spoofing* —para los países que lo tienen legislado—, incitación a la violencia, y

(1) Abogado especialista en delitos informáticos y derecho comparado e inmobiliario. Integra, entre otras, la Asociación Internacional de Derecho Penal (AIDP), la *Latin American Studies Association* y la *International Technology Law Association (ItechLaw)*. Asesor en seguridad pública en empresas nacionales e internacionales y colaborador en importantes fundaciones deportivas y sociales.

diferentes variantes de delitos sexuales como la pedofilia, pornografía infantil y corrupción de menores, por mencionar algunos .

Si bien debemos aclarar que no todos los delitos del Código Penal pueden configurarse a través de la *web,* muchos de ellos pueden utilizarla a los efectos de cometer ilícitos, de manera que quien delinque se sirve de esa tecnología como apoyo para la comisión de un delito —quien sustrae información de la *web* para luego cometer un robo o un secuestro, la interconexión de organizaciones terroristas o del crimen organizado, la venta de armas, o la comercialización de mercadería robada—, hechos estos en los que la *web* puede ser utilizada para canalizar diferentes acciones delictivas que se materializan fuera del ciberespacio.

Conforme a lo expuesto, no puedo dejar de mencionar otros canales de ciberespacio utilizados por delincuentes diferentes a la *wolrd wide web* que todos conocemos. Una de las vías preferidas del ciberdelincuente es la denominada *deep web,* que es una suerte de sub-red de redes que por su estructura informática no forma parte de la Internet superficial, ni las páginas que la integran —generalmente de contenidos ilegales— están indexadas por los motores de búsqueda.

En la también denominada *onion web,* el delincuente se siente más seguro ya que las posibilidad de determinar el origen de la conexión son francamente remotas y se ha transformado en un prioritario desafío para los investigadores.

El crecimiento de usuarios de Internet viene ascendiendo de modo vertiginoso, a una velocidad realmente sorprendente, y conforme a ello también asciende el número de delitos informáticos. Según la Organización Internacional de Telecomunicaciones, el número de habitantes en el mundo con acceso a Internet se ha incrementado de 700 millones en la década de los 90, a 2500 millones en la actualidad, proyectando esta tendencia para el futuro. Este avance comunicacional globalizado no ha llegado solo, ya que muchos delincuentes se comenzaron a inmiscuir en el ciberespacio a los efectos de cometer delitos a través de Internet o bien utilizar la red como apoyo para otros delitos, y esto sin descartar los nuevos delitos clasificados como típicamente informáticos.

Si bien esta escalada del avance de la ciberdelincuencia estaba prevista en el denominado "Proyecto Stanford", varias naciones lograron consensuar políticas para un avance estratégico contra este flagelo.

En el año 2001, en la Ciudad de Budapest, 29 Estados parte crearon el más importante instrumento internacional sobre el cibercrimen, popularmente conocido como el Convenio de Budapest. Luego, este convenio fue ratificado por otros 30 Estados. La República de Panamá fue el último en hacerlo en enero de 2014.

Si bien dicho Convenio contempla en forma genérica la problemática del cibercrimen, instando a colaborar y cooperar entre los estados miembros en materias procesal y probatoria, entre otras, los principios generales de asistencia mutua, información espontanea, conservación rápida de datos almacenados están entre los artículos más importantes.

Si bien el espíritu de esta convención es de extrema importancia para el control y el tratamiento de los ciberdelitos en los que el lugar de su ejecución es distinto del lugar de los efectos, debemos destacar que solo algunos de los Estados parte lograron incorporarla en su totalidad a su derecho interno. De este modo se obstaculiza, en cierta forma, la colaboración internacional en investigaciones de delitos configurados en determinado país con efectos en otro. Es decir, sin la obligatoriedad en las legislaciones internas de guardado de trafico de Internet, ni la coordinación y remisión expedita de información, se deberá remitir la cuestión probatoria mediante el proceso tradicional del exhorto, cuyo tiempo de implantación, en la mayoría de los casos, colisiona con la velocidad de Internet y puede dejar acéfala una investigación por la volatilidad de la prueba informática.

Sumado a ello, nos encontramos con la problemática de los llamados "paraísos informáticos", y con países que no suscribieron el convenio, quienes no tienen reglamentada en su derecho interno la forma de recolectar la prueba en tiempo y forma, o se niegan a colaborar con otros Estados, o tienen imposibilidad técnica de hacerlo.

A título de ejemplo podemos observar que la ley 34/2002 del Reino de España obliga a las ISP al guardado de tráfico de Internet de todos sus usuarios por el término de doce meses. Por lo tanto, cualquier delito informático cometido desde España cuyos efectos se materializaran en un país extranjero —por ejemplo, el daño informático a través del envió de virus informáticos— podrá ser investigado con mayor precisión y efectividad, a diferencia de otros países que no poseen legislación de guardado de tráfico como la Argentina o Uruguay.

Debo aclarar que el sistema de guardado de tráfico para recolectar la prueba no es infalible ya que existen métodos de elusión, como el proyecto Tor, programas de navegación anónima, conexiones de zonas Wifi, utilización fraudulenta de Wifi de terceros (Wifi sin clave o vulnerando su clave) o la misma utilización de la denominada "red zombi".

1. La ciberdelincuencia en el siglo XXI

La ciberdelincuencia se ha transformado en una de las mayores amenazas de la actualidad. Por estos medios se controlan desde armas letales de gran alcance hasta la honorabilidad de las personas, ya que el efecto viral de la información subida la *web* se trasmite al instante a todos los usuarios del mundo y quedara allí para siempre. Aunque mediante medidas judiciales se logre que buscadores des-indexen determinada URL con contenido impropio o se bloqueen por medio de los ISP locales, el alcance será solamente para la jurisdicción aplicable, y sobre ello siempre está latente la posibilidad de que se generen cientos de páginas clon o *mirrors* con la misma información objetada por su carácter delictivo.

Por lo expuesto, puedo afirmar que nos encontramos ante dos grandes desafíos. Por un lado el esclarecimiento de los delitos cometidos por ciberdelincuentes que obligan a dilucidar y consensuar un criterio universal en materia de la jurisdicción aplicable, la ley del lugar de comisión del hecho, la ley del lugar en donde se producen los efectos o la ley que corresponda a la plataforma virtual por la cual se cometió el delito.

El segundo desafío tiene que ver con del desarrollo de herramientas y políticas en materia de la protección de la privacidad de los usuarios, que hoy prácticamente dependen de políticas autorreguladas de grandes corporaciones internacionales que controlan Internet.

Es decir, en la Internet de hoy no solo no existe la infalibilidad, sino que tampoco existe la privacidad, ya que no existe posibilidad de saber quién accede a ella. Y ante la tendencia mundial del avance de la Internet satelital o del ya instalado fenómeno del *cloud computing*, estas empresas que hoy tienen hasta sus propios satélites para brindar un servicio hoy exclusivo, mañana popular, más poder tendrán cuando lleguen a poner en órbita esos satélites por sus propios medios, de modo que debemos tener en cuenta, y por supuesto estar alertados, sobre la posibilidad que los "gigantes de Internet" vayan sumando mayor autodeterminación y lleguen a tener más poder que las naciones en materia informática.

No es descabellado observar que dichas empresas buscan establecerse como micro-Estados todo poderosos en pequeñas islas, territorios, o plataformas de ultramar (cumplimentando los requisitos para ser reconocidas como Estados independientes: territorio, población y gobierno). Es decir, tendrán el poder de ofrecer, o no, gran parte de la prueba para el esclarecimiento de los diversos delitos informáticos como hoy ocurre con los delitos cometidos utilizando Twitter, en donde la remisión de la prueba dependerá de la justicia de California. Debo admitir, no obstante, que esta problemática es a mediano o largo plazo, aunque no deja de ser una posibilidad que nos ofrecerá el futuro cercano en esta materia.

2. La problemática actual

Como destacaba *ut supra*, la adaptación de los códigos penales del mundo a las nuevas formas comisión de delitos a través de Internet, como de los nuevos delitos informáticos, es un proceso activo que se viene dando, ya hace varios años en la mayoría de los regímenes jurídicos del mundo. La adaptación del derecho penal y procesal penal a la tecnología es una cuestión urgente e inevitable que en un futuro cercano incluirá a todas las naciones.(2) Esto es así porque a excepción de los países con ciberespacio cerrado a la conexión externa —generalmente dictaduras o gobiernos con regímenes especiales—, se lo considera como una problemática prioritaria en materia de seguridad interior y exterior, más allá de la disparidad de culturas, pensamientos filosóficos, religiosos o problemáticas históricas. En los ciberdelitos, el lugar de comisión y el de los efectos puede involucrar diferentes regímenes jurídicos, y por lo tanto, para esclarecer el hecho, será indispensable una extrema coordinación y cooperación internacional en materia probatoria, tal como lo menciona la Convención de Budapest. Para ello será imprescindible que las naciones cooperantes tengan en su administración interna herramientas que permitan aportar colaboración en forma precisa y expedita.

En cuanto a la situación interna presentamos la siguiente problemática:

- Delitos cometidos desde zonas Wi-fi cuyo y radio de alcance de la señal.
- Delitos cometidos desde locutorios o cibercafés sin control del usuario durante la sesión.

(2) Países distantes como Mongolia, Senegal, Timor Oriental, Unión de Myanmar, Kazajstán, Mozambique, y el Reino de Bhutan, entre otros, han adaptado sus regímenes penales a los delitos informáticos.

- Delitos cometidos desde Wi-fi abiertos.
- Delitos cometidos mediante sistemas informáticos de sub-redes de interconeccion anónima como por ejemplo el proyecto Tor, la *deep web* o proxis anónimos.

En materia internacional nos encontramos también con similares problemáticas que llevan en muchos casos para el esclarecimiento de delitos informáticos cometidos en determinado país se debe remitir a la colaboración de otra nación. Veamos:

- Los ciberdelitos cometidos desde conexiones alojadas en países extranjeros.
- Los ciberdelitos cometidos utilizando redes de conexión anónima o sistemas proxis con conexiones que involucran a diferentes países.

Es claro que en un futuro mediato sería apropiado establecer en los países signatarios de la Convención de Budapest —además de su adaptación a su derecho interno— tribunales especiales para el tratamiento de delitos informáticos a los efectos de optimizar la interconexión expedita entre diferentes dependencias internacionales para maximizar la investigación sobre este tipo de delitos y poder seguir el ritmo y la velocidad con la que se desarrolla en el universo informático.

3. Consideraciones finales

Los Estados, a corto o mediano plazo, llegarán a cumplimentar su legislación interna en materia de la comisión de delitos a través de Internet, como también de los delitos propiamente informáticos de hoy y los que surgirán con el avancen de la tecnología.

Lo fundamental estará enmarcado en la entidad probatoria y la cooperación y colaboración internacional precisa y expedita como así en la celeridad procesal. Mientras no exista esa coordinación, este tipo de delitos —en muchos casos implementado a la distancia y en el anonimato— tendrán difíciles posibilidades de resolución. Vale aclarar que, si bien la constatación del origen del delito o la titularidad de la conexión del servicio de Internet mediante en número de dirección de IP dinámica asignada y utilizada para realizar el ilícito no puede ser considerado prueba suficiente ni significa identidad de su titular, sí será un elemento indispensable para la investigación.

Para finalizar, quisiera destacar que, si bien la solución definitiva a la problemática de la ciberdelincuencia aun está muy lejos, la adaptación de

muchos regímenes penales del mundo han sido un significativo aporte. Pero más allá de la adaptación o tipificación de estos delitos, será determinante para avanzar en la lucha contra el cibercrimen que los Estados implementen los medios necesarios para recolectar la prueba informativa y presten colaboración entre sí.

Debemos tener en cuenta que el autor del ciberdelito tiene cada día más recursos para vulnerar jurisdicciones y esos recursos son cada vez más fáciles de utilizar por los usuarios comunes, como lo ya mencionados sistemas TOR, la utilización de proxys anónimos, o escritorios remotos alojados en otra jurisdicción.

Por lo tanto, pueden ser soluciones parciales en materia local, pero la solución definitiva recaerá en el esfuerzo conjunto de todas las naciones —salvaguardando siempre la libertad de expresión y los derechos de los ciudadanos— ya que Internet es un bloque que no reconoce fronteras.

ASISTENTES A LA JORNADA

Carla Caloni
Diego Ramón Encina
Christian Andrés Pérez Sasso
Bibiana Teresa Alonso
Martín Alejandro Mungai Bures
Antonio Fong Ruiz
Rosario Ianeri
Nicolás Michanie
Leandro Otero
María Eugenia Sagasta
Juan Ignacio Pascual
Lorena Laura Andrea Padován
Patricio Liali
Lucía Esquibel
Alejandro Grosso Grazioli
Elba Susana González
Federico Julián Lagorio
Eusebio de Jesús Maestre
María Sol Loredo
Mariana Serra Zamora
Hugo Américo Roson
Gabriel A Tula Gonzaga
María Lorena Cabrera
Viviana Mestres
Mariel Constantino

Arnoldo César Ceferino Lobbosco
Beatriz Sarahi Aguilera Gallegos
Luis Ángel Nocera
Diego Migliorisi
Virginia Guida
Héctor Fabiano Cortes
Marcelo Buigo
Alejandro Foster
Carlos María Raffetto
Juan Manuel Gomatti
David Sosa Dopazo
M. Florencia Romerstein
Juan Fernández Buzzi
Nicolás Bru
Graciela De Dios
Laura Carolina Casco
Agustín Ferreira
María Belén Masola
Gerónimo Vargas
María Soledad Gil
Agustín Sánchez
Lucas Valenzuela
Pablo Rambaldi
Francisco Santillán
Jorge Ignacio Moreno

Francina Spighi
Matías Martínez Núñez
María Florencia Pavese
Lautaro Pagani
Daniela Florencia Asato
Yesmin Abufager
Héctor Morales
Néstor Cerneaz
Natalia Aguiar
Jorge Frank
Cristian Cabral
Mariano Bibas
Danilo Deluca
Marta Inés Ruggeiro
Mariano Pinardi
Julieta Butler
Mariela Fernández
Ariel Pelegrino
Alfredo Ruiz Paz
Carlos Blanco
Guadalupe Piaggio
Florencia Canese
Soe Campora Iriart
Solange Capuya
Patricio Nicolás Sabadini
Julieta Martínez Becerra
Diego Sebastián Luque
Glenda De la Cruz
Julián Aristimuno
Laura Agüero
Carlos Caramuti
Sebastián Zanazzi
Jorge Luis Litvin
María Mercedes Gonzalez
Hernán Prepelitchi
Jonathan Gueler
Maria Doldan
Andrea Barberis
María Luján Bianchi
Lucía Souto Lazarre
Ines Abait
Cynthia Bonilla
Sofía Malarino
Jorge Moeremans
Daniela Mazzucco
Florentina Parisi
Emanoel Granger
Luciana Mendez
Juan Manuel Alcade
Mariano Scalercio
Carla Szep
Carla Lobelos
Blanca Nieves Marin
Sonia Cuesta
Mariana Altea
Justo José Bagnardi
Macarena Videla
Federico Jufaro
Adriana Bayonese
Sergio Fabián Comda
Nicolas Ciri
Silvana Noemí Vergatti
Natalia Cardozo

BIBLIOGRAFÍA

Aboso, Gustavo E.; Zapata, María F., *Cibercriminalidad y derecho penal*, Bs. As., B de F, 2006.

Acción para prevenir y Detener la Explotación Sexual de Niños, Niñas y Adolescentes, [en línea] http://resources.ecpat.net/EI/Updates/SPWCIIIOutcome.pdf

Anarte Borrallo, Enrique, "Incidencia de las nuevas tecnologías en el sistema penal. Aproximación al derecho penal en la sociedad de la información", en *Derecho y Conocimiento*, Servicio de Publicaciones de la Facultad de Derecho de la Universidad de Huelva, vol. 1.

Balardini, Sergio, "Hacia un entendimiento de la interacción de los adolescentes con los dispositivos de la Web 2.0. El caso de Facebook", en Barindelli y Gregorio (comps.), *Datos personales y libertad de expresión en las redes sociales digitales. Memorándum de Montevideo*, Bs. As., Ad-Hoc, 2010.

Barcellona, Pietro, "La Teoría de los Sistemas y el paradigma de la sociedad moderna", trad. de M. Maresca, en Portilla Contreras, Guillermo (coord.), *Mutaciones de Leviatán. Legitimación de los nuevos modelos penales*, Madrid, AKAL, 2005.

Beck, Ulrich, *La sociedad del riesgo. Hacia una nueva modernidad*, Barcelona, Paidós, 2006.

Candarle, Gisela, "Hacia la justicia digital en la Ciudad de Buenos Aires", [en línea] *elDial.com*, DC167D.

Carcova C., "Complejidad y derecho", en *Doxa*, 21-11, 1998.

Carnevale, Carlos A., "¿El acceso a internet es un Derecho Humano?", [en línea] *elDial.com.*, DC1746.

Carnevale, Carlos A., "¿Es posible ser condenado penalmente por descargar música de Internet? – Mp3, P2P y garantías constitucionales", en *el Suplemento de Derecho de la Alta Tecnología de la Biblioteca Jurídica Online* ", [en línea] www.elDial.com.ar, 12/3/08.

Carney, P., "De Bentham a Beadle. La ciudad de la vigilancia", en AA.VV, *Criminología y Control social. Orden o Justicia. El falso dilema de los intolerantes*, v. II, Rosario, Juris, 2000.

Cassin, Barbara, *Googléame. La segunda misión de los Estados Unidos*, 1ª ed., Bs. As., FCE, 2008.

Corte Suprema de Justicia de la Nación, *Justicia argentina* online, [en línea] http://www.fam.org.ar/media/img/paginas/Justicia%20Argentina%20On%20Line.pdf.

Cherñavsky, Nora A., "Fundamentación del castigo a las personas corporativas", en *Revista de Derecho Penal y Procesal Penal*, fasc. 7, Bs. As., 2008.

Cherñavsky, Nora A., "El delito informático", en De Luca, Javier A. (coord.), *XI Encuentro*

de Profesores de Derecho Penal de la República Argentina, Bs. As., La Ley/UBA/AAPDP, 2013.

Chiaravalloti Alicia y Ricardo Levene (h.), "Delitos informáticos. Segunda Parte", en *La Ley* 1998-F, 976

De Gavaldá y Castro, Rubén A., *Ceremonial. Un arte para comprender la vida*, Bs. As., Paidós, 2010.

De la Mata Barranco, Norberto J.; Hernández Díaz, Leyre, "El delito de daños informáticos: una tipificación defectuosa", en *Estudios Penales y Criminológicos*, Servicio de Publicaciones de la Universidad de Santiago de Compostela, vol. XXIX, 2009.

Díaz Gómez, Andrés, "El delito informático, su problemática y la cooperación internacional como paradigma de su solución: el Convenio de Budapest", en *Revista Electrónica de Derecho* de la *Universidad de La Rioja* (REDUR), n° 8, diciembre de 2010.

Domscheit-Berg, Daniel, *Dentro de WikiLeaks. Mi etapa en la web más peligrosa del mundo*, Ana Duque de Vega y Carles Andreu Saburit (trads.), Bs. As., Rocaeditorial, 2011.

Donna, Edgardo, "*¿Es posible un derecho penal liberal?*", en *Revista de Derecho Penal*, Rubinzal-Culzoni, Año 2003-1.

Doueihi, Milad, *La gran conversión digital*, Julia Bucci (trad.), Bs. As., FCE, 2010.

Elizalde Marín, Francisco, "La prueba en la *Cloud Computing: Cloud Computing & Service Level Agreements*. El modelo en los Estados Unidos de América y su proyección al ámbito local argentino", [en línea] *elDial.com*, DC15EE

Engisch, Karl, *Teoría de la libertad de la Voluntad*, Montevideo, BdeF, 2008.

Faerman, Juan, *Faceboom. El nuevo fenómeno de masas Facebook*, Bs. As., Ediciones B, 2009.

Falcone, Roberto y Capparelli, Facundo, *Tráfico de estupefacientes y derecho penal*, Bs. As., Ad-Hoc, 2002.

Faraldo Cabana, Patricia; Puente Aba, Luz María y Brandariz García, José Ángel (coords.), *Nuevos retos del Derecho Penal en la era de la globalización*, Valencia, Tirant lo Blanch, 2004.

Feijoó Sánchez, Bernardo, "Sobre el fundamento de las sanciones penales para Personas Jurídicas", en *La Responsabilidad Penal de las Personas Jurídicas, Órganos y Representantes*, Lima, Ara Editores, 2002.

Ferrajoli, Luigi, *Derecho y razón*, Madrid, Trotta, 2009.

Fillia Leonardo C.; Monteleone, Romina; Nager, Horacio S.; Sueiro Carlos C., *Análisis integrado de la Criminalidad Informática*, Prólogo Carlos Alberto Elbert, Bs. As., Fabián J. Di Plácido, 2007.

Freeman, Edward H., "*ISP Liability for Third-Party Defamation*", en *Legally speaking*, noviembre/diciembre, 2002.

Freeman, Edward H., "*Third-Party Liability: Who Pays for Computer Damages?*", en *Legally speaking*, marzo/abril, EBSCO Publishing, 2002.

Granero, Horacio R., "La naturaleza jurídica de la nube (*'cloud computing'*)", en el *elDial.com*, Suplemento de Alta Tecnología, 09/09/2009, elDial.com DC11A9

Granero, Horacio R., "La sanción de la Ley 26.685 de Expedientes Digitales. El principio de equivalencia funcional y la firma digital", [en línea] *elDial.com*, CC2736.

Günther, Klaus, "Pluralismo jurídico y Código Universal de la Legalidad: la globalización como problema de Teoría del Derecho", *Anuario de Derechos Humanos, Nueva Época*, vol. 4, 2003, (225-257).

Herzog, Félix, "Límites al control penal de los riesgos sociales (Una perspectiva crítica ante el derecho penal en peligro)", ADPCP, 1993.

Hirsh, Hans Joachim, "Cuestiones acerca de la armonización del derecho penal y procesal penal en la Unión Europea", en AAVV, *Estudios sobre Justicia Penal. Homenaje al Profesor Julio B. J. Maier*, Bs. As., Editores del Puerto, 2005Iellimo, Marcela, "El caso Wikileaks ¿un planteo de cambio para el orden jurídico internacional?", [en línea] *elDial.com*, DC1522.

Insa, Fredesvinda M., *La Admisibilidad de las Pruebas Electrónicas ante los Tribunales. Luchando contra los Delitos Tecnológicos*, AEC, 2006.

International Telecommunication Union (ITU), "Understanding Cybercrime: Phenomena, Challenges and Legal Response", [en línea] http://www.itu.int/ITU-D/cyb/cybersecurity/docs/Cybercrime%20legislation%20EV6.pdf

International Telecommunication Union (ITU), *El Ciberdelito. Guía para los países en desarrollo*, [en línea] http://www.itu.int/ITU-D/cyb/publications/2007/cgdc-2007-s.pdf ITU

Ivoskus, Daniel, *Obsesión digital. Usos y abusos en la red*, Bs. As., Norma, 2010.

Jaen Vallejos, Manuel, *Cuestiones Actuales del Derecho Penal Económico*, Capítulo II, Bs. As., Ad Hoc, 2004.

Karavas, Vaios, "The Force of Code: Law's Transformation under Information-Technological Conditions", en German Law Journal, vol. 10, n° 4, 2009.

Kerr, Orin, "Digital Evidence And The New Criminal Procedure", *Columbia Law Review*, vol 105:279.

Ladeur, Karl-Heinz, "Guaranteeing the Programming Mandate of Public Broadcasters and Restrains on Private Broadcasters' Programmes in Multimedia Conditions", en *German Law Journal*, vol. 5, n° 8, 2004.

Ladeur, Karl-Heinz, "Toward a Network-Oriented Law of the Internet! The Necessity to Find A New Balance between Risk and Opportunity in Network Comunication", en *German Law Journal*, vol. 10, n° 9, 2009.

Lampe, Ernst Joachim, "Sobre la estructura ontológica del injusto punible", en *Revista de Estudios Criminais*, n° 16, año IV, 2004.

Lezertua, Manuel, "El proyecto de Convenio sobre el Cybercrimen del Consejo de Europa", en López Ortega, Juan José (dir.), *Internet y Derecho Penal*, *Cuadernos de Derecho Judicial* X-2001, Madrid, Consejo General del Poder Judicial, 2001.

Lima Vianna, Túlio, "Dos crimes por computador", en *el Portal Jurídico Mundo Jurídico*, [en línea] www.mundojuridico.adv.br, en 16/04/2003.

Lo Giudice, María Eugenia, "Con motivo de la sanción de la ley que introduce el 'delito de *grooming*' en el Código Penal (año 2013)", en *elDial.com*, DC1C0B.

Lopes da Silva, "Direito Penal e Sistema Informático", en *Editora Revista dos Tribunais, Série Ciência do Direito Penal Contemporânea*, vol. 4, San Pablo, Brasil, 2003.

López Romero, Tatiana, "*Internet Service Providers' Liability. For Online Copyright Infringement: The Us Approach*", en *Vniversitas*, Pontificia Universidad Javeriana, Colombia, n° 112, julio-diciembre, 2006.

Lozano, M. G., "La democracia, el crimen organizado y las leyes sobre la privacy", en *Doxa* 15/16, 1994.

Mercado, P., "El proceso de globalización, el Estado y el Derecho", en Portilla Contreras, Guillermo (coord.), *Mutaciones de*

Leviatán. Legitimación de los nuevos modelos penales, Universidad Internacional de Andalucía-Akal, 2005.

Morales García, "Apuntes de política criminal en el contexto tecnológico. Una aproximación a la Convención del Consejo de Europa sobre Cyber-crime", en AAVV, *Delincuencia Informática. Problemas de responsabilidad*, *Cuadernos de Derecho Judicial IX-2002*, Madrid, Consejo General del Poder Judicial 2002.

O´Donnell, Santiago, *ArgenLeaks*, Bs. As., Sudamericana, 2011.

Ortiz Pradillo, Juan C., "*Fighting against Cybercrime in Europe: The admissibility of Remote Searches in Spain*", *European Journal of Crime, criminal Law and Criminal justice*, 19, 2011.

Palazzi Pablo A., *Los Delitos Informáticos en el Código Penal. Análisis de la ley 26.388*, Bs. As., Editorial Abeledo Perrot, Bs. As., 2009.

Pastor, Daniel, "La recodificación penal en marcha. Una iniciativa ideal para la racionalización legislativa", en *Pensar en Derecho*, Bs. As., Eudeba/Facultad de Derecho (UBA), 2012.

Pawlik, Michael, "¿Pena o combate de peligros? Los principios del derecho internacional penal alemán ante el foro de la teoría de la pena", en *Teoría de la ciencia del derecho penal*, Eduardo Saad-Diniz y Cecilia Ugartemendía (trads.).

Perron, Walter, "Perspectivas de la unificación del derecho penal y del derecho procesal en el marco de la Unión Europea", en AAVV, *Estudios sobre Justicia Penal. Homenaje al Profesor Julio B. J. Maier*, Bs. As., Editores del Puerto, 2005.

Piccone, V.; Mangini, M., "UNASUR en el contexto del regionalismo y los paradigmas de la integración latinoamericana", en *Revista Derecho Público*, año II, n° 5, Bs. As., Ediciones Infojus.

Prittwitz C., *Strafrecht und Risiko. Untersuchungen zur Krise von Strafrecht und Kriminalpolitik in der Risikogesellschaft*, Frankfurt am Main, V. Klostermann, 1993.

Radomir Jansky y Ruben Lombaert, "Hacia una estrategia europea unificada para combatir la ciberdelincuencia", en *E) NAC. E-newsletter. En la lucha contra el cibercrimen*, n° 4, octubre de 2009.

Reidenberg, Joel R., "*Lex informatica: The Formulation of Information Policy Rules through Technology*", en *Texas Law Review*, vol. 76, n° 3, febrero, 1998.

Reggiani, Carlos, *Delitos Informáticos*, Bs. As., *La Ley*, 2008-D.

Reischl, Gerald, *El engaño Google. Una potencia mundial sin control en Internet*, Héctor Piquer y Cristina Sánchez (trads.), 1ª ed., Bs. As., Sudamericana, 2009.

Riquert Marcelo A., *Delincuencia Informática en Argentina y el Mercosur*, Prólogo de David Baigún, Bs. As., Ediar, 2009.

Riquert Marcelo A., *Informática y Derecho Penal Argentino*, Bs. As., Ad-Hoc, 1999.

Riquert, Marcelo A., "Delincuencia informática y control social: ¿excusa y consecuencia?", en *Revista Jurídica Facultad de Derecho de la UNMDP*, n° 6, 2011, y [en línea] http://perso.unifr.ch/derechopenal/assets/files/articulos/a_20120208_01.pdf

Riquert, Marcelo A., "Informática y Derecho Penal", en De Luca, Javier (coord.), *XI Encuentro de Profesores de Derecho Penal de la República Argentina*, Bs. As., La Ley, 2013.

Romeo Malanda, Sergio, "Un nuevo modelo de derecho penal transnacional: el derecho penal de la Unión Europea tras el Tratado de Lisboa", en *Estudios Penales y Criminológicos*,

Servicio de Publicaciones de la Universidad de Santiago de Compostela, vol. XXXII, 2012.

Rosende Eduardo E., "El intrusismo informático. Reflexiones sobre su inclusión en el Código Penal", en *Suplemento La Ley Penal y Procesal Penal*, Bs. As., La Ley, 27/05/2008.

Rovira del Canto, Enrique, "Ciberdelincuencia intrusiva: hawking y grooming", conferencia brindada en Barcelona, noviembre de 2010, [en línea] http://www.iaitg.eu/mediapool/67/671026/data/Ciberdelincuencia_intrusiva_hacking_y_grooming_Enrique_Rovira.pdf

Sáenz, Ricardo y Ruiz, Maximiliano, "Hacia un nuevo modelo de investigación en materia de ciberdelincuencia", [en línea] *elDial.com*.

Sáenz, Ricardo, "Delincuencia Informática. Necesidad de adecuar normas y prácticas investigativas", [en línea] www.delitosinformáticos.fiscalias.gob.ar

Salt, Marcos, *Criminal procedure law provisions on cybercrime in Latin American regarding their compliance with the Budapest Convention (Argentina, Chile, Colombia, Costa Rica, México, Paraguay and Perú)*, Estrasburgo, council of Europe, 12/04/2011.

Salt, Marcos, "*International legal cooperation in cybercrime matters: Challenges for countries of Latin America*", [en línea] www.coe.int/cybercrime

Salt, Marcos, "Nuevos desafíos de la evidencia digital. El acceso trasfronterizo de datos en los países de América Latina", en *Derecho Penal y Procesal Penal*, Bs. As., Abeledo Perrot, 2013.

Salt, Marcos, "Tecnología informática: ¿un nuevo desafío para el proceso penal?", en *XXV Congreso Nacional de Derecho Procesal Penal*, Bs. As, Rubinzal-Culzoni.

Sarrabayrouse, Eugenio, *Responsabilidad Penal por el Producto*, Bs. As., Ad-Hoc, 2007.

Schopenhauer, Arthur, *Ensayo sobre el Libre Albedrío*, Colección Pensadores Universales, Bs. As., Gradifco.

Sieber, Ulrich, "Legal Aspects of Computer-Related Crime in the Information Society", [en línea] http://www.archividelnovecento.it/archivinovecento/CAPPATO/Cappato/Faldone6412Dirittiumanipaesiextracom/DonneAfghanistan/Desktop/sieber.pdf

Seitz, Nicolai, "*Transborder Search: A new Perspective in Law Enforcement?*", en *Yale Journal of Law and Technology*, vol. 7, 2005.

Sibilia, Paula, *El hombre postorgánico. Cuerpo, subjetividad y tecnologías digitales*, 2ª ed., Bs. As., FCE, 2009.

Sieber, Ulrich, "*Legal Aspects of Computer-Related Crime in the Information Society*", *COMCRIME-Study, prepared for the European Commission, Section I.B.2.a*, "*Protection of Privacy*", Würzburg University, Jan 1, 1998.

Silva Sánchez, Jesús M., *La expansión del derecho penal*, 3ª edición, Montevideo, BdeF, 2011.

Silva Sánchez, Jesús M., "La responsabilidad penal de las personas jurídicas en el Convenio del Consejo de Europa sobre cibercriminalidad", en Morales García (dir.), *Delincuencia Informática. Problemas de responsabilidad*, Cuadernos de Derecho Judicial IX-2002, Consejo General del Poder Judicial, Madrid, 2002.

Small, Gary y Vorgan, Gigi, *El cerebro digital. Cómo las nuevas tecnologías están cambiando nuestra mente*", Roc Filella Escolá (trad.), Barcelona, Urano, 2009.

Sueiro, Carlos C., "La eficiencia de la ley 26.388", en De Luca, Javier A. (coord.), *XI Encuentro de Profesores de Derecho Penal de la República Argentina*, Bs. As., La Ley, 2013.

Sueiro, Carlos C., "La eficiencia de la reforma en materia de criminalidad informática, en *La Ley*, Suplemento de Penal y Procesal Penal, 2011, pp. 11/22.

Teijeiro, Nicolás, "La protección constitucional de la intimidad en Internet con especial referencia a redes sociales", en el *elDial.com*, Suplemento de Alta Tecnología, 08/06/2011, DC15EF.

Terragni, Marco Antonio, "Conferencia",en De Luca Javier A. (coord.), *XI Encuentro de Profesores de Derecho Penal de la República Argentina*, Bs. As., La Ley, 2013.

Teubner, Günther, *El derecho como sistema autopoiético de la sociedad global*, Bogotá, UEC, 2005.

Teubner, Günther, "Neo-Spontanes Recht und duale Sozialverfassungen in der Weltgesellschaft?", en Simon/Weiss AAVV, *Zur Autonomie des Individuums - Liber amicorum für Spiros Simitis*, Baden-Baden, Nomos, 2000.

Tobares Catalá, Gabriel H.; Castro Argüello, Maximiliano J., *Delitos Informáticos*, Córdoba, Advocatus, 2010.

Tomeo, Fernando, "Responsabilidad penal de los administradores de sitios Web. El caso Taringa!", en *La Ley*, Bs. As., 1 de junio de 2011.

Vaninetti, Hugo A., "Inclusión del '*grooming*' en el Código Penal", Bs. As., La Ley, 2013, AR/DOC/4628/2013.

Vaninetti, Hugo A., "Media sanción del Senado al proyecto de '*grooming*'", en Revista Jurídica La Ley, Suplemento de Actualidad, Bs. As., 26/04/2012.

Velazco San Martín, Cristo, "Aspectos jurisdiccionales de la computación de la nube", en el *elDial.com*, Suplemento de Alta Tecnología Suplemento de Alta Tecnología, 14/04/2010, [en línea] elDial.com DC1304

Vianna, Túlio Lima, "Dos crimes por computador", [en línea] www.mundojuridico.adv.br, 160/4/2003.

Willke, Helmut, "La supervisión del Estado: el desafío a la política por parte de los sistemas mundiales adyacentes", en Gómez-Jara Díez, Carlos (coord.), *Teoría de sistemas y derecho penal: fundamentos y posibilidades de aplicación*, Bogotá, UEC, 2007.

Winthrop-Young, Geoffrey, "*Silicon Sociology, or, Two Kings on Hegel's Throne? Kittler, Luhmann, and the Posthuman Merger of German Media Theory*", en ***The Yale Journal of Criticism***, vol. 13, n° 2, otoño 2000.

Zaffaroni, E. Raúl; Alagia, Alejandro y Slokar, Alejandro, *Derecho Penal. Parte General*, Bs. As., Ediar, 2008.

Zaitch, Damián, "Viejos conocidos, nuevos enemigos. Discursos y políticas sobre el delito organizado en la nueva Europa", en AA.VV, ***Criminología y Control social. Orden o Justicia. El falso dilema de los intolerantes***, v. II, Rosario, Juris, 2000.

Zavrsnik, Ales "La intervención del sistema de justicia penal en las amenazas a la ciberseguridad: ¿panacea o caja de Pandora?", en *E-newsletter*, n° 44, diciembre de 2008.

Este libro con una tirada de 300 ejemplares, se terminó de imprimir en
los Talleres Gráficos de la Cooperativa Campichuelo Ltda. en agosto de 2014.

GRAFICA
CAMPICHUELO
Cooperativa Obrera Gráfica Campichuelo Ltda

Campichuelo 553 - C.A.B.A. - C1405BOG - Telefax: 4981-6500 / 2065-5202
campichuelo@cogcal.com.ar www.cogcal.com.ar