SECCIÓN I: DOCUMENTO DE REFLEXIÓN Y CUESTIONARIO
GRUPO NACIONAL ARGENTINO*

Contribuyeron en el presente trabajo:

Javier Augusto DE LUCA, Marcelo RIQUERT, Christián C. SUEIRO, María Ángeles RAMOS y Francisco FIGUEROA

Objeto del cuestionario (ver Anexos 1 2)

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. 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 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 (p.e. integridad de los sistemas procesadores de datos, privacidad de los datos almacenados)?

La legislación de la República Argentina en materia de criminalidad informática a través de la ley 26.388 no ha creado bienes jurídicos autónomos o específicos de los 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) Los delitos contra la propiedad (antes, también por Ley 25930/04), 4) Los delitos contra la Seguridad Pública, 5) Delitos contra la Administración Pública.

Es así que la ley 26.388 ha alcanzado con su reforma un número muy limitado y especifico de tipos penales como lo son: 1) El Ofrecimiento y distribución de imágenes relacionadas con pornografía infantil (Artículo 128 del Código Penal, en adelante C.P.), 2) Violación de correspondencia electrónica (Artículo 153 del C.P.), 3) Acceso ilegítimo a un sistema informático (Artículo 153 bis del C.P.), 4) Publicación abusiva de correspondencia (Artículo 155 del C.P.), 5) Revelación de secretos (Artículo 157 del C.P.), 6) Delitos relacionados con la protección de datos personales (Artículo 157 bis del C.P.), 7) Defraudación informática (artículo 173, inciso 16, C.P.), 8) Daño (artículo 183 y 184, C.P.), 9) Interrupción o entorpecimiento de las comunicaciones (artículo 197 C.P.), 10) El tipo penal de alteración,

* Atención: El texto que se publica constituye la última versión original del informe nacional enviado por el autor, sin revisión editorial por parte de la Revista.

sustracción, ocultación, destrucción e inutilización de medios de prueba (artículo 255 del C.P.), a lo cual debe agregarse las modificaciones terminológicas realizadas en el artículo 77 del Código Penal de la Nación.

Además, a través de modificaciones e inserciones en leyes especiales, se han considerado otros bienes jurídicos, a saber: a) secreto empresarial (por Ley 24766/97); b) hacienda pública (por Leyes 24769/97 y 26735/11); c) propiedad intelectual (por Ley 25036/98); d) servicios de comunicaciones móviles (por Ley 25891/04).

(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*) e intangibles (*Software*) en el tipo penal de daño simple y agravado (Arts. 183 y 184 C.P.)

En similar dirección, se contempla la alteración dolosa de registros fiscales y la adulteración de controladores fiscales (arts. 12 y 12bis de la Ley 24769); la alteración de número de línea, de serie electrónico o mecánico de equipo terminal o módulo de identificación removible de usuario de SCM; la alteración de componente de una tarjeta de telefonía, el acceso a los códigos informáticos de habilitación de créditos de servicio SMC o el aprovechamiento ilegítimo de estos últimos (arts. 10 y 11, Ley 25891).

(b) violación de la privacidad TIC.

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

Los arts. 2 y 12, Ley 24766/97, 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 Defraudación informática (artículo 173, inciso 16, C.P.), que es mas especifica que la Defraudación a sistemas automatizados o con tarjetas de crédito y débito (Artículo 173, inciso 15 C.P.)

(d) distribución de virus de ordenadores.

El tipo penal de daño previsto en el artículo 183 segundo párrafo, 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 del C.P.)

El 13/5/10, 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 explicitas o toda representación de sus partes genitales con fines predominantemente sexuales en el que participaren menores (Artículo 128 del C.P.)

La defraudación de derechos de propiedad intelectual está prevista en el art. 71 y ss. de la Ley 11723, cf. mod. por Ley 25036/98.

(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, 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 ningún 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[1]; 2) Cracker[2]; 3) Preaker o Phreaker[3]; 4) Phisher[4]; 5) Sniffer[5]; 6) Virucker[6]; 7) Propagandista informático[7], 8) Pirata Informático[8], o 9) Cyberbullyng o Ciber-Acosador.

---

[1] Ver CHIARAVALLOTI ALICIA Y RICARDO LEVENE (H), *"Delitos informáticos. Segunda Parte"*, La Ley 1998-F, 976; FILLIA LEONARDO CÉSAR – MONTELEONE ROMINA – NAGER HORACIO SANTIAGO – SUEIRO CARLOS CHRISTIAN. *"Análisis integrado de la Criminalidad Informática"*, Prólogo Carlos Alberto Elbert, Editorial Fabián J. Di Plácido, Buenos Aires, 2007, Pág 117. TOBARES CATALÁ GABRIEL H. – CASTRO ARGÜELLO MAXIMILIANO J. *"Delitos Informáticos"*, Prólogo de Marcelo J. Sayago, Editorial Advocatus, Córdoba 2010, Pág 97.

[2] Ver CHIARAVALLOTI ALICIA Y RICARDO LEVENE (H), *"Delitos informáticos. Segunda Parte"*, La Ley 1998-F, 976; FILLIA LEONARDO CÉSAR – MONTELEONE ROMINA – NAGER HORACIO SANTIAGO – SUEIRO CARLOS CHRISTIAN. *"Análisis integrado de la Criminalidad Informática"*, Prólogo Carlos Alberto Elbert, Editorial Fabián J. Di Plácido, Buenos Aires, 2007, Pág 118; TOBARES CATALÁ GABRIEL H. – CASTRO ARGÜELLO MAXIMILIANO J. *"Delitos Informáticos"*, Prólogo de Marcelo J. Sayago, Editorial Advocatus, Córdoba 2010, Pág 99.

[3] Ver CHIARAVALLOTI ALICIA Y RICARDO LEVENE (H), *"Delitos informáticos. Segunda Parte"*, La Ley 1998-F, 976; FILLIA LEONARDO CÉSAR – MONTELEONE ROMINA – NAGER HORACIO SANTIAGO – SUEIRO CARLOS CHRISTIAN. *"Análisis integrado de la Criminalidad Informática"*, Prólogo Carlos Alberto Elbert, Editorial Fabián J. Di Plácido, Buenos Aires, 2007, Pág 118.

[4] Ver FILLIA LEONARDO CÉSAR – MONTELEONE ROMINA – NAGER HORACIO SANTIAGO – SUEIRO CARLOS CHRISTIAN. *"Análisis integrado de la Criminalidad Informática"*, Prólogo Carlos Alberto Elbert, Editorial Fabián J. Di Plácido, Buenos Aires, 2007, Pág 119.

[5] ROSENDE EDUARDO E. *"El intrusismo informático. Reflexiones sobre su inclusión en el Código Penal".* Publicado en el Suplemento La Ley Penal y Procesal Penal, Editorial La Ley, Buenos Aires, Martes 27 de mayo de 2008, Pág 21.

[6] Ver RIQUERT MARCELO ALFREDO. *"Informática y Derecho Penal Argentino"*, Editorial Ad- Hoc, Buenos Aires, 1999, Pág 57; FILLIA LEONARDO CÉSAR – MONTELEONE ROMINA – NAGER HORACIO SANTIAGO – SUEIRO CARLOS CHRISTIAN. *"Análisis integrado de la Criminalidad Informática"*, Prólogo Carlos Alberto Elbert, Editorial Fabián J. Di Plácido, Buenos Aires, 2007, Pág 120; TOBARES CATALÁ GABRIEL H. – CASTRO ARGÜELLO MAXIMILIANO J. *"Delitos Informáticos"*, Prólogo de Marcelo J. Sayago, Editorial Advocatus, Córdoba 2010, Pág 101.

[7] RIQUERT MARCELO ALFREDO. *"Informática y Derecho Penal Argentino"*, Editorial Ad- Hoc, Buenos Aires, 1999, Pág 57; FILLIA LEONARDO CÉSAR – MONTELEONE ROMINA – NAGER HORACIO SANTIAGO – SUEIRO CARLOS CHRISTIAN.

La mayoría de los tipis 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 Ley 26388 estos tres últimos párrafos al art. 77 C.P.: *"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. 157bis C.P., cuando el autor sea funcionario público sufrirá, además, pena de inhabilitación especial. La Ley 25891 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.

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

En el art. 153bis C.P. 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 C.P., 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 es el tipo penal de alteración, sustracción, ocultación, destrucción e inutilización de medios de prueba. Esta figura prevé su modalidad imprudente:

Artículo 255 C.P.: *"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"?

"Análisis integrado de la Criminalidad Informática", Prólogo Carlos Alberto Elbert, Editorial Fabián J. Di Plácido, Buenos Aires, 2007, Pág 120.

[8] Ver RIQUERT MARCELO ALFREDO. *"Informática y Derecho Penal Argentino"*, Editorial Ad- Hoc, Buenos Aires, 1999, Pág 57

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 el Código Penal, al producir una actualización integral del último por Ley 26388, 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 artículo 77 del Código Penal de la Nación 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 del 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, sino que a lo sumo son nuevas herramientas para realizar las acciones ya contempladas en los tipos penales previstos por la reforma.

En algún caso, como la regulación del SCM por Ley 25891, 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 nota distintiva sería la de falta de sistema, armonía y coherencia, aún cuando esto no seria 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, e.g., 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 si pena el mero intrusismo informático o Acceso ilegítimo a un sistema informático (Artículo 153 bis del C.P.).

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 luego de un largo reclamo de solución a problemas verificados jurisprudencialmente de lagunas de punición.

(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 por 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 que 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 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, Corte Suprema Justicia Nación, en el caso "Halabi", al declarar inconstitucional la Ley 25873 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 para 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 que con 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 (e.g., encriptación de mensajes, uso de passwords, uso de software de protección)? ¿Se prevén sanciones para la no protección del propio ordenador hasta cierto punto, e.g., 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[9].

En este sentido ha incorporado definiciones terminológicas en el artículo 77 C.P., teniendo en consideración las definiciones suministradas por el *"Convenio sobre la Ciberdelincuencia de Budapest",* en su artículo 1º 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 (Artículo 128 del C.P.), incorporando los verbos típicos establecidos su artículo 9º. En general, en lo referente a la modificación de los tipos penales alcanzados por la ley 26.388, ha

[9] Ver CONVENIO SOBRE LA CIBERDELINCUENCIA, Budapest, 23.XI.2001, Serie de Tratados Europeos nº 185, *Council of Europe* / *Conseil de L´Europe*.

tomado en consideración el Capítulo II *"Medidas que deberán adoptarse a nivel nacional"*, Sección 1, *"Derecho penal sustantivo"*, para delimitar que 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 nº 31/11 estipula la introducción gradual de la notificación electrónica.

Se ha presentado un proyecto[10] para tipificar en el C.P. la figura del robo de identidad digital, insertándola como art. 138bis 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[11], 2) El *Spamming* o correo basura o publicidad no solicitada[12]; 3) La captación ilegal y difusión de datos, imágenes y sonidos[13], 4) La posesión simple de material pornográfico infantil; 5) La responsabilidad de los proveedores[14].

---

[10] Por los senadores Marías de los Ángeles Higonet y Carlos Verna. Fuente: "Diario Judicial" del 28/5/12.

[11] Ver RIQUERT MARCELO A. *"Delincuencia Informática en Argentina y el MERCOSUR"*, Prólogo de David Baigún, Editorial Ediar, Buenos Aires, 2009, Págs 202/204.

[12] Ver RIQUERT MARCELO A. *"Delincuencia Informática en Argentina y el MERCOSUR"*, Prólogo de David Baigún, Editorial Ediar, Buenos Aires, 2009, Pags 204/206.

[13] Ver PALAZZI PABLO A. *"Los Delitos Informáticos en el Código Penal. Análisis de la ley 26.388"*, Editorial Abeledo Perrot, Buenos Aires, 2009, Págs 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*", Prólogo de David Baigún, Editorial Ediar, Buenos Aires, 2009, Pags 206/207, quien considera prudente y acertado postergar su punición hasta que exista un serio debate en torno a esta figura penal.

[14] Ver TOMEO FERNANDO. *"Responsabilidad penal de los administradores de sitios Web. El caso Taringa!"*, Editorial La Ley, Buenos Aires, 1 de junio de 2011. También se sugiere ver GRANERO HORACIO R. *"La naturaleza jurídica de la nube ("cloud computing")"*, Publicado en el Suplemento de Alta Tecnología de elDial.com, el 9 de septiembre de 2009, elDial.com DC11A9; VELAZCO SAN MARTÍN CRISTO. *"Aspectos jurisdiccionales de la computación de la nube"*, Publicado en el Suplemento de Alta Tecnología de elDial.com el 14 de abril de 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."* , Publicado en el Suplemento de Alta Tecnología de elDial.com, el 8 de junio de 2011, elDial.com DC15EE; TEIJEIRO NICOLÁS. *"La protección constitucional de la intimidad en internet con especial referencia a redes sociales",* Publicado en el Suplemento de Alta Tecnología de elDial.com, el 8 de junio de 2011, DC15EF.