Coloquio Preparatorio
24-27 abril 2013, Moscú (Rusia)
Sección II: Sociedad de la información y Derecho penal

GRUPO NACIONAL ARGENTINO*

Contribuyeron en el presente trabajo:
Javier Augusto DE LUCA, Marcelo RIQUERT, Christián C. SUEIRO, María Ángeles RAMOS y Francisco FIGUEROA

(A) 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 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, 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 C.P.) 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 concordada al Código Penal de la Nación.

Sin embargo, desde que sancionara la primera ley con disposiciones penales con referencias directas a expresiones de las TICs (Ley 24766, de 1997), se fueron sucediendo hasta 2008 una serie de reformas en leyes especiales o en el propio Código, 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 Código. Entre las primeras, 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.

* 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.

No obstante, decisiones judiciales que pusieron de manifiesto problemas de tipicidad (por ej., caso "Pinamonti" de 1991 para el "daño" informático; caso "Autodesk" de 1997 para la propiedad intelectual), operaron de disparador 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 reformas. 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 Código Penal 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 C.P. se ha caracterizado por abarcar la modificación en su mayoría tipos penales dolosos, no presentando el empleo de tipos penales culposos a excepción del delito de "alteración, sustracción, ocultación, destrucción e inutilización de medios de prueba" (artículo 255 del C.P.), 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[1].

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.

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)."

---

[1] Ver FILLIA LEONARDO CÉSAR – MONTELEONE ROMINA – NAGER HORACIO SANTIAGO – ROSENDE EDUARDO E. – SUEIRO CARLOS CHRISTIAN.*"Análisis a la reforma en materia de Criminalidad Informática al Código Penal de la Nación (ley 26.388)"*, Artículo publicado en el Suplemento de Derecho Penal y Procesal Penal de Editorial La Ley, publicado el Jueves, 28 de agosto de 2008, Pág 15/41.

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 C.P.

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 del C.P.

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 específicamente la introducción de terminología al Código Penal de la Nación.

En particular a través de la reforma al artículo 77 del C.P. se incorporan los términos documentos, firma, suscripción, instrumento privado en su modalidad digital.

En el artículo 77 del Código Penal se incorporaron 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."

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

El art. 183 C.P. 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 (Artículos 183 y 184 C.P.).

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. 157bis, inc. 3, del C.P., 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 (Artículo 183 y 184 C.P.).

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 (Artículo 155 del C.P.), Revelación de secretos (Artículo 157 del C.P.), Delitos relacionados con la protección de datos personales (Artículo 157 bis del C.P.),

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.

iv. ¿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?

v. ¿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. 157bis del C.P. pune en su inciso 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?

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 de Protección de Datos Personales 25286 del año 2000, entendida por gran parte de la doctrina como reglamentaria de la garantía constitucional del art. 43 de la Constitución Nacional (hábeas 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 (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 *website*s 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 del 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 (e.g. Cityville, Farmville, etc.)? Cite por favor las fuentes jurídicas relevantes.

No.

(c) Protección contra contenido ilegal relacionado con las TIC

1.

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, **SI**

2. hacer disponible, **SI**

3. exportar **SI.**

4. e intencionalmente accede a pornografía infantil en Internet; **SI**

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 (Art. 128 C.P.).

Art. 128 C.P.: ***"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."

Penaliza:

1. El acceso a sabiendas a pornografía infantil por internet

SI

2. La transmisión de pornografía infantil por internet

SI

3. Exportar pornografía infantil en internet

SI

4. Poseer pornografía infantil en internet con el fin de, e.g., transmitirla, exportarla…?

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

SI

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

SI.

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-stalking?

No posee una figura en particular.

4. ¿cyber-grooming?

Tampoco se contempla esta conducta como tipo penal especifico

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

Si a través del tipo penal del artículo 173, inciso 16, C.P.

2. Infracción de los derechos de la propiedad intelectual.

Si por medio de la ley 11.723.

3. Espionaje industrial

Si, mediante todos los tipos penales transcriptos.

(e) Criminalización de actos cometidos en el mundo virtual

(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 Univ. 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.

(8) Identifique, por favor, si las siguientes formas y medios de ciberdelincuencia (1) ocurren con frecuencia, (2) ocurren de manera infrecuente, o (3) no han tenido lugar en su país, colocando una "X" en la correspondiente casilla de la tabla siguiente: **Formas y medios de ciberdelincuencia**	**Ocurre frecuentemente**	**Ocurre infrecuentemente**	**No ha ocurrido**
Robo de identidad *online* (incluido el *phishing* y el tráfico *online* de información sobre falsa identidad)			
Hacking (intrusión ilegal en sistemas informáticos)			
Código malicioso (gusanos, virus, *malware* y *spyware*)			
Interceptación ilegal de datos informáticos			
Comisión *online* de delitos contra la propiedad intelectual			
Tráfico *online* de pornografía infantil			
Daño intencional de datos o sistemas informáticos			
Otros			

¿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.