Sección 2: Documento de reflexión y cuestionario

Prof. Dr. Emilio Viano

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

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

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

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

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.
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.

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

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

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?
iii. ¿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)?
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.)

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

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.

(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,
2. hacer disponible,
3. exportar
4. e intencionalmente accede a pornografía infantil en Internet;

- 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;
- Penaliza:

1. El acceso a sabiendas a pornografía infantil por internet
2. La transmisión de pornografía infantil por internet
3. Exportar pornografía infantil en internet
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?

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

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?

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.

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?

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?
2. ¿cyber-bullying?
3. ¿cyber-stalking?
4. ¿cyber-grooming?

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
2. Infracción de los derechos de la propiedad intelectual
3. Espionaje industrial

(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.

(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?
(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*.
(3) ¿Las encuestas de victimación de su país incluyen preguntas sobre ciberdelitos?
(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.
(7) ¿Es el tema del ciberdelito objeto de la formación inicial y/o continua de jueces, fiscales y policía?
(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			

(9) Adicionalmente a lo anterior, si hay otras formas y medios de ciberdelincuencia que han tenido lugar (tanto si de manera frecuente como infrecuente) en su país, identifíquelas por favor, indicando también la frecuencia de su producción, en la tabla siguiente:

Formas y medios de realización de la conducta	Ocurre frecuentemente	Ocurre de modo infrecuente

¡Gracias por su valiosa colaboración!

Anexo 1

John A.E. Vervaele

1. Definición de la Sociedad de la Información? Elementos esenciales de una definición

No existe un concepto único de sociedad de la información que predomine. La doctrina se esfuerza en la concreción de las definiciones y valores del concepto y se centran en cuestiones económicas, técnicas, sociológicas y culturales. La sociedad post moderna a menudo es caracterizada como una "sociedad de la información", debido a la amplia disponibilidad y uso de la Tecnologia de la Información y la Comunicación (TIC). La definición más común de la sociedad de la información pone el énfasis en la innovación tecnológica. El procesamiento, almacenamiento y transmisión de la información han dado lugar a la aplicación de las tecnologías de la información y la comunicación (TIC), y a las relacionadas con la biotecnología y la nanotecnología, en casi todos los rincones de la sociedad. La sociedad de la información es una sociedad postindustrial en la que la información y el conocimiento son los recursos clave y están jugando un papel fundamental (Bell, 1973 y 1979).

Sin embargo, la sociedad de la información no solamente se define por la infraestructura tecnológica, sino más bien como un fenómeno multidimensional. Bates (1984) señaló que cualquier sociedad de la información es una red compleja, no sólo de infraestructura tecnológica, sino también una estructura económica, un patrón de relaciones sociales, modelos de organización y otras facetas de la organización social. Por lo tanto, es importante no centrarse sólo en el aspecto tecnológico, sino también en los atributos sociales de la sociedad de la información, incluido el impacto social de la revolución de la información en las organizaciones sociales, comprendido el sistema de justicia penal.

Por otra parte, la era postmoderna de la tecnología de la información transforma el contenido, la accesibilidad y la utilización de la información y el conocimiento en las organizaciones sociales, incluido el sistema de justicia penal. La relación entre el conocimiento y el orden ha cambiado radicalmente. La transformación de las comunicaciones en tecnología instantánea de información ha cambiado la manera en la que la sociedad valora el conocimiento. En esta era de rápidos cambios, la estructura de la autoridad tradicional se está debilitando y está siendo sustituida por un método alternativo de control social. La aparición de un nuevo paradigma tecnológico basado en las TIC se ha traducido en una sociedad en red (network society) (Castells1996), en la que las principales estructuras y actividades sociales se organizan en torno a las redes de información procesada electrónicamente. Existe una transformación aún más profunda de las instituciones políticas en la sociedad en red: el surgimiento de una nueva forma de Estado (Estado en red) que gradualmente sustituye a los Estados-nación de la era industrial. En esta era de rápidos cambios, la estructura de la autoridad tradicional se está debilitando y está siendo sustituida por un método alternativo de control social (sociedad de la vigilancia). La transición del Estado-nación al Estado en red es un proceso organizativo y político impulsado por la transformación de la gestión, representación y dominación política en las condiciones de la sociedad en red. Todas estas transformaciones exigen la difusión de redes interactivas múltiples como la forma de organización del sector público.

La información y el conocimiento son recursos clave de la sociedad de la información, que afectan a la estructura social y política de la sociedad y al Estado y que afectan a la función, estructura y contenido del sistema de justicia penal.

2. La interrelación de los cuestionarios de las cuatro secciones

En primer lugar, deberíamos utilizar una definición de trabajo común. Está claro que la referencia a los delitos informáticos es demasiado restrictiva para nuestro tema y que la expresión "derecho penal de la información o delitos relacionados con la sociedad de la información" tampoco tiene un significado claramente fijado.

Por estas razones, tenemos que usar una definición común y un enfoque limitado.

En cuanto a la definición, propongo utilizar el concepto de ciberdelito, pero con una definición que incluye una amplia variedad de nuevos fenómenos y desarrollos.

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 nueve del ciberespacio y las bases datos cibernéticas.

En segundo lugar, ya que esta es un área muy amplia, debemos centrarnos en los ámbitos más interesantes en los que nuestras resoluciones puedan aportar valor añadido. El resultado de los debates con los cuatro relatores generales es que nos centremos en los siguientes bienes jurídicos en el ámbito del ciberdelito:

1. La integridad y funcionalidad del sistema de las ciber-TIC (delitos CID)
2. Protección de la privacidad
3. Protección de la personalidad digital
4. Protección frente a los contenidos ilícitos
5. Protección de la propiedad (incluidos los derechos de propiedad intelectual)
6. Protección contra los actos cometidos exclusivamente en el mundo virtual
7. Protección del sistema de cumplimiento de las normas (delitos de incumplimiento [non-compliance offences])

3. Bibliografía

Daniel Bell, The Coming of Post-Industrial Society, New York, Basic Books , 1976.

Manuel Castells, The Rise of the Network Society. The Information Age: Economy, Society and Culture Volume 1. Malden: Blackwell. 2d Edition, 2000

S. Sassen, The global city , New York-London, Princeton University Press, 2d edition, 2001.

U.Sieber, Mastering Complexity in the Global Cyberspace, in M. Delmas-Marty & M Pieth. Les chemins de l'harmonisation Pénale, Paris 2008, 127-202.