Cuestionario Sección I – Parte General

Sociedad de la Información y Justicia Penal
AIDP-IAPL Congreso Internacional de Derecho Penal 2014

Prof. Dr. Thomas Weigend

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

(a) ataques contra sistemas TIC
(b) violación de la privacidad TI
(c) falsedad forgery y manipulación de los datos almacenados digitalmente
(d) distribución de virus de ordenadores
(e) delitos relativos a las identidades virtuales de los usuarios, e.g., forging, sustracción o daño de personalidades virtuales
(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.

(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)?
(4) ¿Se limita a determinados grupos de autores y/o víctimas la responsabilidad penal por ciertos ciberdelitos?
(5) ¿Se extiende la responsabilidad penal en el area de las TIC a las conductas meramente imprudentes o negligentes?
(6) ¿Hay diferencias específicas entre la definición de los ciberdelitos y los delitos "tradicionales"?

(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)?
(2) ¿Cómo evita la legislación los efectos chilling indebidos sobre el uso legítimo 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? E.g.,
- ¿cómo se tienen en cuenta los cambios en el uso de internet y las redes sociales?
- ¿cómo se adapta la legislación al progreso tecnológico (e.g., mediante la remisión a las normas administrativas)?

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

(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?
(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)?
(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?

(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?
(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?

(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?

(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?
(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)?

(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.