Sección 4: Documento de reflexión y cuestionario

André Klip

(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. André Klip por email: andre.klip@maastrichtuniversity.nl

(B) Cuestiones sobre la jurisdicción

(1)(a) ¿Cómo localiza su país el lugar de comisión de un delito cometido en el ciberespacio?
(b) ¿Su legislación nacional considera necesario y posible localizar el lugar donde se encuentran la información y las pruebas? ¿Dónde está la información que se puede encontrar en la web? ¿Se encuentra donde el ordenador del usuario está físicamente presente? ¿Allí donde el proveedor de la red tiene su sede (jurídica o de hecho)? ¿Qué proveedor? ¿O es el lugar de la persona que posibilitó la disponibilidad de los datos? Si estas preguntas no se consideran jurídicamente relevantes, por favor, indique por qué.
(2) ¿En su sistema penal se puede prescindir de la determinación del *locus delicti* en caso de cometerse un ciberdelito? ¿Por qué (no)?
(3) ¿Qué normas de competencia jurisdiccional se aplican a los ciberdelitos tales como la incitación al odio a través de Internet, hacking, ataques contra los sistemas informáticos, etc? Si su Estado no tiene jurisdicción sobre estos delitos, ¿se considera es esto problemático?
(4) ¿Su legislación nacional contiene normas relativas a la prevención o a la solución de los conflictos de jurisdicción? ¿Hay alguna práctica sobre ello?
(5) ¿En su sistema penal se puede prescindir de los principios jurisdiccionales en caso de que se cometa un ciberdelito, lo que en esencia significa que el Derecho penal nacional es de aplicación universal? ¿Debería esto limitarse a ciertos delitos, o estar condicionada a la existencia de un tratado?

(C) Derecho penal sustantivo y sanciones

(1) ¿Qué ciberdelitos tipificados en su sistema penal nacional considera usted que tienen una dimensión transnacional?
(2) ¿En qué medida las definiciones de los ciberdelitos contienen elementos jurisdiccionales?
(3) ¿Hasta qué punto las reglas de la parte general sobre la comisión, conspiración o cualquier otra forma de participación contienen elementos jurisdiccionales?
(4) ¿Considera usted que los ciberdelitos constituyen un asunto que un Estado puede regular por sí mismo? Si es así, indique cómo puede hacerlo un Estado. Si no es así, indique por qué no puede hacerlo.
(5) ¿Su Derecho penal nacional prevé la responsabilidad penal de las empresas / proveedores (internacionales)? ¿Tiene la atribución de responsabilidad implicaciones jurisdiccionales?

(D) Cooperación en materia penal

(1) ¿Hasta qué punto las especificidades de la tecnología de la información cambian la naturaleza de la asistencia mutua?
(2)(a) ¿Se prevé en su país la interceptación de telecomunicaciones (inalámbricas)? ¿Bajo qué condiciones?
(b) ¿En qué medida es relevante que un proveedor o un satélite puedan estar ubicados fuera de las fronteras del país?

(c) ¿Su legislación nacional prevé la asistencia judicial mutua en relación a la interceptación de las telecomunicaciones? ¿Ha celebrado su país convenios internacionales al respecto?
(3) ¿En qué medida las causas generales de denegación se aplican en relación a las investigaciones en Internet y otros medios para acceder a los ordenadores y las redes ubicadas en otros lugares?
(4) ¿Se exige en su legislación nacional el requisito de la doble incriminación para la cooperación en aquellas situaciones en las que el autor haya causado los efectos desde un Estado en el que se permite la conducta en un Estado en el que se tipifica como delito la conducta?
(5) ¿Permite su legislación nacional las investigaciones extraterritoriales? ¿Bajo qué condiciones? Por favor, responda tanto a la situación en la que las autoridades nacionales de aplicación de la ley necesitan información, como cuando las autoridades extranjeras necesitan la información disponible en su Estado.
(6. ¿Se permite el autoservicio (*self service*) (obtención de pruebas en otro Estado sin pedir permiso)? ¿Qué condiciones deben cumplirse para permitir el autoservicio? Por favor, diferenciar la información pública y la protegida. ¿Cuál es la práctica (tanto activa como pasiva) en su país?
(7) Si es así, ¿se aplica esta legislación también a las búsquedas que se llevan a cabo en la web de acceso público, o en ordenadores que se encuentran fuera del país?
(8) ¿Es su país parte en acuerdos sobre el Registro de Nombre de Pasajero (PNR) (transacciones financieras, intercambio de ADN, cuestiones de visados o similares)? Por favor especificar y explicar cómo se lleva a cabo el intercambio de datos en la legislación nacional. ¿Tiene su país una llamada unidad que está disponible 24 horas al día y 7 días a la semana para el intercambio de datos? Limítese a las cuestiones relevantes sobre uso de la información para la investigación criminal.
(9) ¿Hasta qué punto los datos a que se refiere en su respuesta a la pregunta anterior se intercambian para la investigación criminal y cuál es el fundamento jurídico? ¿Hasta qué punto la persona concernida tiene la posibilidad de impedir / corregir / eliminar la información? ¿En qué medida puede esta información ser utilizada como prueba? ¿La ley de su país permite la detección y retirada de un sitio web que contiene información ilegal? ¿Existe alguna una práctica? ¿Desempeña algún papel el sitio del proveedor, propietario del sitio o cualquier otro elemento extranjero?
(10) ¿Cree usted que es posible un sistema de aplicación internacional para ejecutar las decisiones (por ejemplo, órdenes de suspensión de Internet o inhabilitaciones) en el área de la delincuencia cibernética? ¿Por qué (no)?
(11) ¿Su país permite la consulta directa de bases de datos nacionales o internacionales que contienen información relevante para las investigaciones criminales (sin solicitud)?
(12) ¿Participa su país en Interpol / Europol / Eurojust o cualquier otro organismo supranacional que aborde el intercambio de información? ¿Bajo qué condiciones?

(E) Aspectos relacionados con los derechos humanos

(1) ¿Qué normas de derechos humanos o constitucionales son aplicables en el contexto de las investigaciones penales con tecnología de la información? ¿Es relevante para la determinación de las normas aplicables de derechos humanos dónde se considera que se han realizado las investigaciones?
(2) ¿Cómo se regula la responsabilidad o rendición de cuentas (*accountability*) de su Estado involucrado en la cooperación internacional? Por ejemplo, ¿es su Estado responsable del uso de la información recolectada por otro Estado en violación de las normas internacionales de derechos humanos?

(F) Desarrollos futuros

(1) Las modernas telecomunicaciones ofrecen la posibilidad de contactar directamente con los acusados, víctimas y testigos a través de las fronteras. ¿Se debería permitir eso y, en caso afirmativo, en qué condiciones? Si no es así, ¿se deberían aplicar las reglas clásicas de asistencia mutua (solicitud y respuesta), y por qué?
(2) ¿Existe algún impedimento legal en su legislación para las audiencias a través de medios audiovisuales (a través de Skype o de otro medio) en casos transnacionales? Si es así ¿cuál? Si no es así, ¿hay alguna práctica?
(3) ¿Hay alguna otra cuestión relacionada con la sociedad de la información y el Derecho penal internacional que actualmente juega un papel en su país y no ha sido tratado en las preguntas anteriores?

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.