Sección 3: Documento de reflexión y cuestionario

Johannes F. Nijboer

(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. Johannes F. Nijboer por email: J.F.Nijboer@law.leidenuniv.nl

(B) Cuestiones Generales

(1) ¿Existen definiciones (jurídicas o socio-jurídicas) para la aplicación de las TI y de las TIC en el contexto del procedimiento penal (incluida la práctica forense)? ¿Cómo están reflejadas estas definiciones conceptuales en la doctrina científica, la legislación, las decisiones judiciales, y las prácticas pertinentes en el contexto del proceso penal?
(2) ¿Existen instituciones específicas y / o grupos de trabajo involucrados en la aplicación de las TIC en el sistema penal?
(3) ¿Existen organizaciones (empresas) privadas (comerciales) que ofrecen servicios relacionados con las TIC en el sistema penal? Si es así, ¿puede dar ejemplos? ¿Qué límites tienen que ser observados?

(C) Información e inteligencia: construyendo posiciones de información[1] (information positions) para aplicación de la ley

(1) ¿Qué técnicas relacionadas con las TIC se utilizan para la construcción de posiciones de información por las agencias de aplicación de la ley?
(2) ¿A qué tipo de bases de datos públicas (por ejemplo, bases de datos de ADN) y privadas (por ejemplo, el Registro de Nombre de Pasajero o los datos financieros como los datos de SWIFT) tienen acceso las agencias de la aplicación de la ley?
(3) ¿Pueden aplicarse las técnicas consideradas como minería de datos y comparación de datos? Si es así, ¿pueden utilizarse estas técnicas para crear perfiles de posibles autores o grupos de riesgo? Si es así, ¿se han desarrollado herramientas especiales para las agencias de aplicación de la ley?
(4) ¿Pueden utilizarse medidas coercitivas (por ejemplo, la interceptación de las telecomunicaciones) para la construcción de posiciones de información?
(5) ¿Qué actores privados (por ejemplo, proveedores de internet o empresas de telecomunicaciones) conservan o están obligados a conservar información para las agencias de aplicación de la ley?
(6) ¿Qué actores privados pueden proporcionar o están obligados a proporcionar información a las agencias de aplicación de la ley?
(7) ¿Existe control judicial de la construcción de posiciones de información?

(D) Las TIC en la investigación penal

(1) ¿Pueden las agencias de aplicación de la ley llevar a cabo intervenciones en tiempo real a) de datos sobre el tráfico , b) sobre el contenido de los datos?

[1] La construcción de las posiciones de información es parte de la denominada actuación policial basada en la inteligencia. Se puede definir la actuación policial basada en la inteligencia como un marco conceptual de llevar a cabo la actividad policial como un proceso de organización de la información que se permite a las agencias de aplicación de la ley en sus tareas preventivas y represivas.

(2) ¿Pueden las agencias de aplicación de la ley tener acceso / congelar / investigar / secuestrar los sistemas de información sobre: a) datos sobre el tráfico, b) el contenido de los datos?
(3) ¿Se puede obligar a las empresas de telecomunicaciones o proveedores de servicios a compartir los datos con las agencias de aplicación de la ley? En caso de incumplimiento, ¿hay medidas coercitivas o sanciones?
(4) ¿Pueden las agencias de aplicación de la ley realizar videovigilancia? ¿Pueden obligar a las personas físicas o jurídicas a cooperar?
(5) ¿Pueden o deben aplicar las agencias de aplicación de la ley grabación audiovisual de los interrogatorios (sospechosos, testigos)?

(E) Las TIC y la prueba
(La cadena de etapas: recogida / almacenamiento / retención / producción / presentación / valoración de la prueba electrónica)

(1) ¿Existen reglas sobre la prueba específicas para la información relacionada con las TIC?
(2) ¿Existen reglas sobre la integridad (por ejemplo, manipulación o procesamiento incorrecto) y seguridad (por ejemplo, hacking) de la prueba relativa a las TIC?
(3) ¿Existen reglas sobre la admisibilidad (incluido el principio de legalidad procesal) de las pruebas que son específicas de la información relacionada con las TIC?
(4) ¿Existen reglas específicas sobre el descubrimiento y revelación de la prueba relacionada con las TIC?
(5) ¿Existen reglas especiales para la valoración (valor probatorio) de la prueba relacionada con las TIC?

(F) Las TIC en la etapa de juicio

(1) Cómo puede o debe introducirse en el juicio la prueba relacionada con las TIC?
(2) ¿Pueden realizarse interrogatorios a distancia (por ejemplo, conexiones vía satélite)?
(3) ¿Pueden utilizarse técnicas digitales y virtuales para la reconstrucción de los hechos (asesinatos, accidentes de tráfico)?
(4) ¿Pueden utilizarse técnicas audiovisuales para presentar pruebas en el juicio (en su forma más simple: imágenes y sonido)?
(5) ¿Pueden sustituirse los expedientes penales en "papel" por otros electrónicos? ¿Se ha avanzado hacia la digitalización de los documentos del juicio?

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.